



Томский межвузовский центр  
дистанционного образования

**Н.В. Замятин**

**ЦИФРОВЫЕ СЕТИ ИНТЕГРАЛЬНОГО  
ОБСЛУЖИВАНИЯ**

Учебное пособие

Министерство образования Российской Федерации  
Томский государственный университет систем управления  
и радиоэлектроники (ТУСУР)

Кафедра автоматизации обработки информации (АОИ)

**Н.В. Замятин**

**ЦИФРОВЫЕ СЕТИ ИНТЕГРАЛЬНОГО ОБСЛУЖИВАНИЯ**

Учебное пособие для студентов специальности  
22.02.00 — «Автоматизированные системы обработки  
информации и управления»

**Томск 2002**

**Замятин Н.В.**

Цифровые сети интегрального обслуживания: Учебное пособие. — Томск: Томский межвузовский центр дистанционного образования, 2002. — ???? с.

В пособии рассматриваются

Учебное пособие предназначено для

© Замятин Н.В., 2002

© Томский межвузовский центр  
дистанционного образования, 2002

## ВВЕДЕНИЕ

Основой человеческого существования является три основополагающих вида деятельности: энергетика, технология, информатика. Сначала появилась энергетика в виде огня, затем топор как результат технологических приемов обработки камня, и в то же время информатика в виде цифровых коммуникаций, которые ограничивались поднятием двух пальцев и указанием на стадо мамонтов. Дальнейшее развитие этих видов деятельности человека происходит эволюционно, взаимно влияя друг на друга. В то же время тенденции развития общества свидетельствуют о том, что информационные технологии становятся доминирующими. Это объясняется тем, что более 60 % работающих связаны с необходимостью обработки информации, и более того уровень развития экономики определяется в настоящее время применением современных информационных технологий и, в частности, средств обмена информацией (информационных сетей).

Концепция информационных сетей является логическим результатом эволюции компьютерных технологий и систем электросвязи. Сначала необходимо было обеспечить доступ к компьютеру, удаленному на большие расстояния: терминалы соединялись с большими компьютерами через телефонные сети с помощью модемов. Затем появились системы, в которых осуществлялась связь компьютера с компьютером. Поскольку компьютеры были большими, и их было немного, и расположены они были на больших расстояниях, то хронологически первыми появились глобальные информационные сети или компьютеры, соединенные каналами связи. Это позволяло обмениваться данными в автоматическом режиме, реализовать службы обмена файлами, синхронизацию баз данных, электронную почту и другие сетевые службы.

В начале 70-х годов появились первые интегральные схемы, и, соответственно, размеры компьютеров стали резко уменьшаться, что привело к появлению большого количества миникомпьютеров. В дальнейшем у пользователей появилось желание пользоваться программными средствами и данными, расположенными на других компьютерах, и последние стали соединяться через последовательный порт. Таким образом, появились первые локальные сети.

Информационные сети по своему построению можно отнести как к частному случаю распределенных систем. На рис. 1. приведена структурная схема и показано место информационных сетей среди остальных видов информационных систем.

Если основным признаком распределенной системы является наличие нескольких центров обработки данных, то к распределенным системам также можно отнести как многопроцессорные системы, так и многомашинные комплексы. В многопроцессорных системах имеется много процессоров, каждый из которых может выполнять свою работу, независимо от остальных, имея общую операционную систему и общую память. В многомашинных комплексах имеется несколько компьютеров с общей памятью, но раздельными операционными системами. Связь между компьютерами осуществляется через программные и аппаратные средства связи.



Рис. 1. Структура информационных преобразователей информации

В информационных сетях программные, а аппаратные связи являются слабыми, а автономность отдельных блоков проявляется в большей степени. Основными элементами сети являются стандартные компьютеры (терминалы), не имеющие ни общих блоков памяти, ни общих периферийных устройств. Связь между терминалами осуществляется посредством сетевых адаптеров и протяженных каналов связи. Каждый компьютер функционирует под управлением локальной операционной системы, а взаимодействие между терминалами осуществляется через сетевые адаптеры и каналы связи. Посредством этих сообщений каждый терминал запрашивает доступ к локальным ресурсам другого терминала. Такими ресурсами могут быть как данные, хранящиеся на диске, так и различные периферийные устройства: принтеры, модемы, факс. Разделение локальных ресурсов между всеми пользователями сети основная цель создания локальной информационной сети. Основная цель создания глобальной информационной сети — это обмен информацией и предоставление пользователям различных сетевых услуг.

В середине 80-х годов положение в сетевых технологиях кардинальным образом начинает меняться. Основная причина — это расширение сферы информационных услуг, как по объему, так и по видам сервиса.

Понятие электронной информации возникло в связи с реформами в обществе. Появилась свобода слова, печати, складываются рыночные отношения, и этот процесс вызывает необходимость быстрого получения раз-

нородной информации. Свобода информации тесно связывается со свободой конкуренции и рассматривается как одно из базисных условий развития рыночной экономики.

Возник рынок информационных услуг, представляющих совокупность экономических, правовых и организационных отношений по продаже и покупке этих услуг, складывающийся между продавцом и покупателем.

Различают два вида сетевых услуг:

1) компьютеризованная межперсональная коммуникация (КМК) — это обмен сообщениями, бюллетени новостей, телеконференции и т.д.

Электронная почта (ЭП) — это наиболее распространенная служба КМК. Существуют две разновидности:

- простая ЭП, обеспечивающая отправку и получение сообщения по нужному адресу;

- почтовые списки, организация службы подписки, ведение списков рассылки, автоматическая рассылка.

Телеконференции — классификация сообщений по темам, предоставление диалогового интерфейса для оперативного общения пользователей, ведение архива сообщений и гибкий доступ к архиву;

2) услуги доступа к разделяемым ресурсам — это доступ к базам данных, управлению и передаче файлов.

Предоставление пользователю информационных сетей возможности передачи той или иной информации, выбора метода передачи и того или иного вида обслуживания его заявки принято называть сервисом сетевого обслуживания. Достижение микроэлектронных технологий повлекло за собой развитие высокопроизводительных микропроцессоров, позволяющих реализовывать сложные алгоритмы обработки информации. Это в свою очередь повлияло на сетевые технологии в появлении скоростных средств передачи информации. Необходимость в снижении стоимости телефонных разговоров и коммутаций привело к созданию цифровой среды передачи данных в интегрированной цифровой коммутации. Повышение производительности, снижение цен на компьютеры и периферийные устройства стимулировало распространение распределенных вычислений. Появление волоконно-оптических линий связи, развитие спутниковых технологий, новых алгоритмов преобразования сигналов для использования на старых линиях связи способствовало повышению скорости и объема транспорта данных.

Использование новых алгоритмов, протоколов и устройств маршрутизации и коммутации привело к возможности преодоления проблем разнородности сетей. Это предопределило появление «сети сетей» (интернета) и вызвало необходимость одновременной передачи по одним и тем же каналам информации, представленной в различной форме: данных, голоса, музыки, изображения, факса, телекса. Существует необходимость в примерно следующем распределении трафика:

- телефонные разговоры — 50 %;

- видеосвязь с низким качеством — 20 %;

- видеосвязь с высоким качеством — 5 %;

- передача данных — 25 %.

Причем речь идет о предоставлении гарантированного сервиса в реальном масштабе времени, потому что совершенно исключено запаздывание или потеря информации при передаче музыки или изображения, особенно в режиме телеконференций. Таким образом, появилась необходимость в интегрированном сетевом сервисе при обслуживании пользователей с гарантированным предоставлением услуг. Для передачи информации должна использоваться цифровая среда с различными каналами передачи интегрированной информации: от волоконно-оптических линий связи до двухпроводных телефонных линий на медных проводах. Такие сети получили название цифровых сетей с интегральным обслуживанием ЦСИО (ISDN — integrated ser-vice digital network). В последнее время появилось разделение таких сетей на узкополосные сети N-ISDN, предназначенные для интегральной передачи голоса и данных, и широкополосные сети B-ISDN, предназначенные для передачи изображения, речи, высококачественного звука, данных, факсов, телекса, проведение телеконференций. Аналогичные проблемы возникли и в Internet. Новые приложения типа аудио и видео в реальном времени, IP-телефония, видеоконференции нуждаются более высокой пропускной способности и обеспечении новой концепции обслуживания: гарантированном предоставлении качества обслуживания для приложений Internet реального времени. При этом необходимо для снижения стоимости обслуживания и быстрого внедрения новых технологий использовать имеющиеся развитые коммуникации в виде телефонных каналов связи.

За время развития человечества вычислительные и коммуникационные системы эволюционировали от простого к сложному. Наиболее наглядно это проявилось в объединении технологии цифровых коммуникаций с предоставлением комплексных услуг и технологией распределенных вычислений.

Технология коммуникаций (в основном телефонная связь) развивалась в ответ на необходимость общения между людьми на больших расстояниях. Создатели телефона разработали технологию телефонии, позволяющую передавать речь на большие расстояния и воспроизводить ее в точке приема. Первоначально связь разрабатывалась для передачи человеческой речи. Для этого достаточно полосы частот 3–4 КГц. Аналоговые речевые сигналы вызывают колебания мембраны и преобразования в аналоговый электрический сигнал. Так как электрические импульсы аналогичны генерирующим их звуковым волнам, говорят, что телефония основана на аналоговой передаче.

Изначально телефонная система состояла из одной передающей системы, одной приемной системы и одной линии, связывавшей их. Первым дополнением телефонной сети стали центральные телефонные узлы или центральные АТС, обеспечивающие коммутацию со всеми телефонными линиями в данном географическом районе. Все телефонные системы и конечные пользователи были связаны с АТС абонентскими линиями, а звон-

нок поступал на АТС, которая обеспечивала соединение с принимающим абонентом. На следующем этапе АТС были соединены друг с другом магистральными каналами связи, а несколько АТС связывались между собой промежуточными телефонными узлами. Такой узел содержал тандемный коммутатор, обслуживающий магистральные линии и маршрутизирующий по определенному маршруту звонки между АТС. Тандемные коммутаторы снизили стоимость телефонных разговоров, обеспечивая соединения между АРС, не требующие выделенной телефонной линии.

К тому времени, как телефонная сеть охватывала весь мир, начались разработки современных компьютерных систем. Все коммуникации между компьютерами и их периферийными устройствами осуществляются в цифровой форме. Если телефонная система развивалась на основе аналоговой передачи сигналов, то в компьютерной среде аналоговая передача не применялась. Компьютеры всегда использовали цифровое представление информации и команды.

Разработка локальных сетей породила более сложную форму цифровых коммуникаций – коммуникации между компьютерами. Локальные сети позволили реализовать новые мощные приложения и найти новые применения компьютерным технологиям. Распространение глобальных сетей привело к крупномасштабному использованию телефонных коммуникаций для соединений удаленных друг от друга терминалов в виде компьютеров, локальных сетей, факсов и другого пользовательского оборудования.

Обычно это требует применение преобразования цифровых сигналов терминалов в аналоговые сигналы, передаваемые телефонными системами, а затем обратного их преобразования в цифровую форму. Такое преобразование осуществляется модемами и это вызывает ощутимые задержки и непроизводительные потери. Поэтому появилась новая технология использования телефонных каналов и для коммутации и передачи цифровой информации, что стало ключевым фактором, стимулирующим переход на полностью цифровые системы с гарантированным предоставлением интегрированных услуг.

Основное назначение информационных сетей — обмен информацией и совместное использование аппаратных и программных ресурсов. Поэтому ИС – это сложный комплекс взаимосвязанных и согласованно функционирующих программных и аппаратных компонентов.

Весь комплекс программно-аппаратных средств сети представляется многослойной моделью. На нижнем уровне модели находится оконечное оборудование, представляющее терминалы, в качестве которых наиболее часто используются компьютеры или локальные сети.

Второй слой — это коммуникационное оборудование. Транспортные системы, повторители, коммутаторы, концентраторы и маршрутизаторы необходимые элементы для построения сети, реализующие функции сетевых протоколов.

Третьим слоем, образующим программную платформу сети, являются сетевые операционные системы (СОС). Концепции, положенные в основу управления локальными и распределенными ресурсами, определяют эффективность работы сети.

Верхним слоем сетевой системы являются приложения, представляющие многочисленные возможности для пользователей (электронная почта, сетевые базы данных, системы автоматизации коллективной работы, средства архивирования и др.)

Все сети имеют некоторые общие компоненты, функции и характеристики. В их числе:

- серверы;
- клиенты;
- транспортные среды;
- операционные системы;
- совместно используемые аппаратные ресурсы;
- совместно используемые программные ресурсы;
- сетевые приложения.

Несмотря на отмеченное сходство, сети разделяются на множество типов по различным признакам:

- по пространственному признаку: локальные, территориальные, глобальные;
- по виду представления сигнала: аналоговые и цифровые;
- по типу использования стека протоколов: в сетевых технологиях используется несколько стеков протоколов OSI/ISO, SNA, DECnet, SPX/IPX, NETBios, TCP/IP;
- по виду передаваемой информации: передача речи, передача данных, передача изображения, передача интегральной информации;
- по типу используемой сетевой операционной системы: NETWARE, WINDOWS NT, UNIX и LINUX, OS/2;
- по типу используемой транспортно-коммутационной системы: кабельные системы, медные провода, витая пара, волоконно-оптические системы, радиозфир, коаксиальный кабель;
- по типу способа коммутации: коммутация пакетов, коммутация каналов, коммутация сообщений;
- по особенностям топологии сети: общая шина, кольцо, иерархическая, комбинированная.

Обобщенная структурная схема классификации информационных сетей представлена на рис 2.

Данное пособие состоит из одиннадцати глав.

Глава 1 является вводной. В ней даны базовые понятия курса о сообщениях, информации, о ее кодировании и компрессии.

В главе 2 описываются каналы связи, способы передачи информации, виды представления сигналов.

Глава 3 полностью посвящена описанию модели OSI. Подробно описан каждый уровень. Также в этой главе раскрывается понятие стека протоколов и рассказывается о некоторых наиболее популярных. Все последующие главы посвящены сетям.

Глава 4 и глава 6 освещают локальные (Ethernet, Token Ring) и глобальные (X.25, Frame Relay) сети соответственно.

Построению больших сетей посвящена глава 5. В ней рассказывается об устройствах, предназначенных для расширения сети, о способах маршрутизации и подробно описывается протокол TCP/IP.

В главе 7 дается понятие о сетевых операционных системах.

В главах 8 и 9 рассказывается о цифровых (ISDN) и широкополосных (ATM) сетях интегрального обслуживания.

В главе 10 уделено внимание администрированию сетей.

Заключительная глава 11 освещает вопрос мониторинга, анализа и диагностики сетей.

## ГЛАВА 1

### СООБЩЕНИЯ И ИНТЕГРАЛЬНАЯ ИНФОРМАЦИЯ

Сообщением называется совокупность логически законченных сведений, снимающих неопределенность. Суть понятия «интегральная информация» заключается в том, что по каналам связи необходимо передавать информацию, носителями которой являются речь, высококачественный звук, изображение, как видео, так и факсимильное, телетекст, данные, графика, телеметрия. Причем эту информацию, особенно при организации видеоконференций необходимо передавать без задержек. Для того чтобы понять особенности речи и высококачественного звука, рассмотрим способы их образования и передачи, а также преобразования в электрический сигнал.

Человеческая речь формируется как излучения звуковых колебаний человеком. Так как губы человека способны делать не более 10 движений в секунду, человек может излучать звуковые колебания частоты 10 Гц, что соответствует длине волны 33 км. Размеры полости рта настолько малы по сравнению с излучаемой длиной волны, что движение губ человека никто бы не слышал. Природа придумала голосовые связки, излучающие гармоническую несущую, которая затем модулируется с помощью мышц полости рта. При разговоре грудная клетка сжимается и расширяется, поток воздуха проходит из легких через трахею и гортань в полости глотки, рта и носа. Голосовой тракт простирается от голосовой щели (отверстия между голосовыми складками в гортани) до губ.

Если произносятся звонкие звуки (гласные, носовые, звонкие согласные), голосовые складки в гортани смыкаются и размыкаются с той или иной частотой, которая называется частотой основного тона. Получается последовательность импульсов воздушного потока, которые возбуждают полости голосового тракта. Человек меняет геометрические размеры этих полостей, соответственно меняются и их резонансные частоты, которые называются формантами.

При произнесении глухих (невокализованных) звуков голосовые складки расслаблены. Проходя по суженному голосовому тракту, воздух создает турбулентный поток (завихрения). Когда человек говорит, он производит спектрально-временную модуляцию широкополосного сигнала, генерируемого голосовыми складками и представляющего своего рода несущую. Полезная информация в этой несущей есть только в интонации (изменении частоты основного тона) и в смене вида спектра с шумовой и наоборот. Частотный диапазон, формируемый голосом, лежит в пределах от 20 Гц до 4 кГц. Человеческая речь обладает большой избыточностью, которая может быть использована при сжатии информации.

Высококачественный звук включает певческий голос и звучание музыкальных инструментов. Звуковысотный диапазон певческого голоса определяется интервалом между наиболее низкой и высокой нотами, которые певец в состоянии воспроизвести. Певческие голоса делятся по высоте на мужские (бас, баритон и тенор) и женские (контральто, меццо-сопрано, сопрано и колоратурное сопрано). Диапазоны основных групп певческих голосов распределяются следующим образом: 82–349 Гц для баса, 110–392 Гц для баритона, 132–523 Гц для тенора, 165–698 Гц для контральто, 220–880 Гц для меццо-сопрано, 262–1046 Гц для сопрано и 330–1397 Гц для колоратурного сопрано.

Голоса певцов, несмотря на все их разнообразие, характеризуются общими закономерностями: сильной выраженностью высоких обертонов с частотами 2 500–3 000 Гц (верхняя певческая форманта) и наличием низкой певческой форманты в области 300–600 Гц. Верхняя певческая форманта придает голосу певца серебристый оттенок, нижняя — впечатление мягкости и массивности. Даже небольшой завал этих частот трактом звукозаписи приводит к значительному искажению тембра голоса. Пение отличается от обычной разговорной речи большей мощностью и громкостью. Динамический диапазон (максимальная разница в силе голоса между форте и пиано) у профессиональных певцов достигает 20–45 дБ. Динамический диапазон певцов-любителей не превышает 10 дБ. В отличие от разговорной речи, в которой содержится большая избыточность, высококачественный звук в виде пения наоборот требует введение дополнительных частот для повышения его качества.

Важнейшая характеристика любого музыкального инструмента — частотный диапазон звучания. Кроме спектра основных частот, каждый инструмент характеризуется дополнительными частотными составляющими — обертонами. Музыкальные инструменты отличаются и силой звучания. Пиковые мощности звучания инструментов составляют: 25 Вт для большого барабана, 12 Вт для малого барабана, 6 Вт для тромбона, 0,4 Вт для фортепиано, 0,3 Вт для саксофона, 0,05 Вт для кларнета. Учитывать различия в этих цифрах необходимо для того, чтобы при записи верно передать баланс уровней громкостей инструментов, а также для правильного выбора расстояния и чувствительности микрофона, исключающего нелинейные искажения, вызванные перегрузкой микрофона и усилительного тракта.

Музыкальные инструменты характеризуются также динамическим диапазоном звучания: отношением мощности звука, извлекаемого из инструмента при исполнении «фортиссимо» (максимальная громкость), к мощности звука при игре «пианиссимо» (минимальная громкость). Динамический диапазон D звукового сигнала принято измерять в децибелах:  $D = 20 \lg(P_{\max}/P_{\min})$ , где  $P_{\max}$  и  $P_{\min}$  — максимальное и минимальное звуковые давления. Если максимальный уровень звучания рояля составляет 80 дБ, а минимальный — 35 дБ, то говорят, что его динамический диапазон составляет  $80 - 35 = 45$  дБ. При этом 80 и 35 дБ — это уровни звукового давления относительно условного нулевого акустического уровня (порога слышимости).

Для преобразования колебаний воздуха, вызванных речью или высококачественной музыкой в электрический сигнал, обычно применяются микрофоны. Микрофоны отличаются по способу преобразования колебаний звукового давления в колебания электрические. С этой точки зрения различают электродинамические, электромагнитные, электростатические, пьезоэлектрические, угольные и полупроводниковые микрофоны.

Принципы действия микрофонов различных типов объединяет способ преобразования звуковых колебаний в электрические: мембрана (диафрагма) микрофона воспринимает и передает колебания звукового давления элементу, осуществляющему их преобразование в электрический сигнал.

К основным характеристикам и параметрам микрофонов, определяющим их качество, относятся следующие:

- чувствительность — отношение напряжения на выходе микрофона к воздействию на него звуковому давлению;
- динамический диапазон — разность между уровнями предельного звукового давления и собственных шумов человеческого голоса.

Когда человек говорит, он производит спектрально-временную модуляцию широкополосного сигнала, генерируемого голосовыми складками и представляющего своего рода несущую. Полезная информация в этой несущей есть только в интонации (изменении частоты основного тона) и в смене вида спектра с шумовой и наоборот.

При преобразовании звука микрофоны обычно искажают первоначальный сигнал за счет влияния шумов, нелинейности преобразования и ограниченности частотной характеристики.

#### 1.1. Сообщения в виде изображений и их преобразование в электрический сигнал

Изображения в качестве носителей информации, предназначенные для передачи по каналам связи, можно разделить на факсимильные изображения, телевизионные (бытовые и промышленные) и мультимедиа.

Источником цветových ощущений являются электромагнитные волны с частотой из светового диапазона. Ощущение цвета является психофизиологическим явлением и определяется спектральным составом света не вполне однозначно. В основном рассматриваются две цветовые модели.

- RGB, используемая в цветных электронно-лучевых трубках мониторов и телевизоров;
- YUV, используемая в каналах телевидения и для сжатия графики.

Цвета получаются смешением трёх основных цветов — красного, синего и зелёного — в пропорции, определяемой соотношением интенсивностей каждой составляющей. При смешении этих цветов в равной пропорции получается цвет, яркость которого может изменяться от чёрного до белого. Такая модель получения цвета называется цветовой моделью RGB (от англ. названий основных цветов red, green и blue). В модели RGB при смешении не основных цветов складываются яркости их одинаковых основных составляющих. Такая модель называется аддитивной. Она соответствует нашему восприятию источников освещения (монитор компьютера, телевизионный экран).

Для преобразования RGB-сигнал в один сигнал яркости изображения Y целесообразно его представлять в виде выражения

$$Y = 0,299 R + 0,587 G + 0,114 B,$$

где  $R$ ,  $G$  и  $B$  — яркости соответствующих цветových составляющих, а коэффициенты при них отражают физиологические особенности нашего зрения.

Вместе с сигналом яркости  $Y$  были введены ещё так называемые сигналы цветности  $U$  и  $V$ :

$$U = B - Y, V = R - Y.$$

В цветовой модели YUV эти величины рассматриваются как три составляющие цветového оттенка.

Изображения занимают намного больше места в памяти, чем текст. Иллюстрация на обложке книги размером  $500 \times 800$  точек занимает 1,2 Мб. Второй особенностью изображений является то, что человеческое зрение при анализе изображения оперирует контурами, общим переходом цветов и сравнительно нечувствительно к малым изменениям в изображении. Также в изображении соседние точки, как по горизонтали, так и по вертикали в изображении близки по цвету.

Поэтому можно создать эффективные алгоритмы компрессии изображений, в которых декомпрессированное изображение не будет совпадать с оригиналом.

Все изображения можно подразделить на две группы — с палитрой и без нее. У изображений с палитрой в пикселе хранится число — индекс в некотором одномерном векторе цветов, называемом палитрой. Чаще всего встречаются палитры из 16 и 256 цветов. Изображения без палитры бывают в какой-либо системе цветопредставления и в градациях серого (grayscale). Для последних, значение каждого пиксела интерпретируется как яркость соответствующей точки. Встречаются изображения с 2, 16 и 256 уровнями серого.

Изображения целесообразно делить на классы. Под классом понимается некая совокупность изображений, применение к которым алгоритма сжатия дает качественно одинаковые результаты. Например, для одного класса алгоритм дает очень высокую степень сжатия, для другого — почти не сжимает, для третьего — увеличивает файл в размере.

Класс 1. Изображения с небольшим количеством цветов (4–16) и большими областями, заполненными одним цветом. Плавные переходы цветов отсутствуют. Примеры: деловая графика — гистограммы, диаграммы, графики и т.п.

Класс 2. Изображения, с плавными переходами цветов, построенные на компьютере. Примеры: графика презентаций, эскизные модели в САПР, изображения, построенные по методу Гуро.

Класс 3. Фотореалистичные изображения. Пример: отсканированные фотографии.

Класс 4. Фотореалистичные изображения с наложением деловой графики. Пример: реклама.

Для представления изображения из двумерного (в зависимости от пространственных координат) в одномерное представление в виде электрического сигнала применяются сканирующие устройства с различными способами преобразований. Это могут быть вакуумные телевизионные трубки, называемые видиконы, полупроводниковые приборы типа приборов с зарядовой связью, а также развертывающие спиралеобразные преобразователи, используемые в факсимильных аппаратах. На выходе таких преобразователей формируется электрический сигнал в зависимости от времени.

Передача изображений представляет более сложную проблему, так как человеческий глаз с информационной точки зрения несравненно совершеннее уха.

Одним из видов сетевого трафика являются факсимильные сообщения. В 1902 году Артур Корн (Германия) запатентовал систему фотозлектрического сканирования изображения, а в 1910 году заработала первая международная факсимильная связь Берлин-Париж-Лондон. До 60-х годов этого века рынок факсимильной аппаратуры был ограничен. В 1968 году ССИТТ разработала рекомендации по факсимильному оборудованию, которое было способно передавать страницу за 6 минут при разрешении 3,85 линий на мм. Позднее в 1976 году аналоговая факсимильная техника была улучшена. Это позволило сократить время передачи страницы до 3 мин. В 1980 году разработан стандарт для цифровых факс-машин (группа 3), здесь уже предусматривается сжатие информации, что позволяет сократить время передачи страницы до 1 минуты при скорости передачи 4800 бит/с.

Факсимильное оборудование поделено на 4 группы. Первая группа практически совпадает с традиционным фототелеграфным оборудованием (6 минут на страницу при разрешении 3,85 линий на миллиметр). Динамической вариации кодовой таблицы не предусмотрено. При этом для кодирования очередной линии сканирования используются результаты, полученные для предшествующей линии.

Факс-оборудование группы 4 может поддерживать так называемый расширенный режим, когда часть рабочего поля кодируется без использования алгоритмов уплотнения информации (как правило, это участки, где попытка сжать либо ничего не дает, либо даже приводит к увеличению объема передаваемых данных). Оборудование этой группы использует на канальном уровне процедуры HDLC LAPB. Рекомендуемой полосой пропускания канала, к которому подключается такое оборудование, является 64 кбит/с.

Перед началом передачи терминалы должны обменяться своими идентификаторами (TID — Terminal Identification). В последнее время появились факс-аппараты, которые печатают изображение на обычную бумагу с разрешением 300–400 точек на дюйм. Такая схема имеет недостатки: аппараты дороги, печать может начаться не ранее, как будет передана вся страница; передающий аппарат может иметь более низкое разрешение, нужно уметь адаптироваться к любому разрешению, что приводит к тому, что скорость печати изображения при низком разрешении остается столь же низкой, как и при высокой.

В 1970 году в Бритиш Телеком были разработаны основные принципы телетекста. Каждому символу ставится в соответствие код длиной в 7–8 бит. На экране такой символ отображается с помощью специального знакового генератора, использующего таблицу. Полному экрану видеотекста, содержащему 24 строки по 40 символов, соответствует 960 байт, для передачи которых по коммутируемой телефонной сети требуется 6,4 секунды. Быстрые каналы могут пропустить эту информацию за 0,1 сек. Телетекст позволяет более эффективно использовать каналы связи и не налагает чрезмерных требований на устройства отображения.

Для корректной передачи цвета требуется 16 миллионов оттенков (8 бит на каждую из трех цветовых компонент). Таким образом, для описания картинки на экране, содержащей 575 линий по 720 пикселей, требуется 1,240 Мбайта. Для передачи такой информации, если не используется сжатие, потребуется около 2,5 минут.

Видеосигнал получается при потрочном сканировании прямоугольного цветного изображения «трёх-ствольной» электронной RGB-пушкой. Сканируемое изображение представляет собой растр, т.е. прямоугольную сетку пикселей, с отношением числа пикселей по горизонтали к числу пикселей по вертикали 4:3 (в системах телевидения высокой чёткости — HDTV — это отношение равно 16:9). В мониторах компьютеров и в телевидении этот обход происходит по-разному.

Для создания видимости непрерывного движения частота смены кадров должна превышать 24 кадра в секунду (к/сек). Для устранения мерцания экрана частота смены кадров должна происходить не менее 50 раз в секунду. Чтобы устранить мерцание и не увеличивать при этом скорость сканирования и, следовательно, объем передаваемой информации, в телевидении применяют так называемую чересстрочную развертку, при которой сначала сканируются нечётные строки (первый полукадр), а затем чётные (второй полукадр). При показе с частотой 25 к/сек смена полукадров происходит 50 раз в секунду и мерцание незаметно.

Таким образом, видеосигнал содержит последовательности полукадров (гасящих и синхронизирующих импульсов и аудиосигнала, синхронизированного с видеопотоком. При растре 800\*600 пикселей и частоте 25 к/сек получается поток 12000000 пикселей в секунду, а с учётом трёхкомпонентности цвета такой поток потре-

бует полосы пропускания шириной 36 МГц. Табл.1.1 показывает реальные характеристики, определённые действующими видеостандартами.

Характеристики некоторых видеостандартов

	NTSC (США, Япония)	PAL (Англия, Германия)	SECAM (Франция, Россия)	HDTV	VHS	S-VHS
Число строк в кадре	525	625	818	1150	250	400
Формат кадра	4:3	4:3	4:3	16:9	4:3	4:3
Частота полукадров	60	50	50	50		
Ширина полосы сигналов яркости/цветности в МГц	4,2/1,5/0,6	5/1,5/1,5	6/1,5/1,5	27	3-3,8	5
Скорость передачи цифровой информации в Мбит/сек	128,7	159,6	158,6		~90	

Сжать видео сигнал удается только использованием следующих приемов:

- переход от RGB к YUV;
  - фильтрация части высоких частот сигнала яркости Y, что приводит к едва заметной размытости в быстро меняющихся участках кадра;
  - фильтрация значительно большей части высоких частот сигналов цветности U и V, основанной на меньшей чувствительности глаза к изменению цвета, чем к изменению яркости.
- Оцифровка видеосигнала обычно происходит с 4-кратной частотой по отношению к наибольшей частоте сигнала, причём разрядность квантования может выбираться разной для сигналов яркости и цветности.

## 1.2 Методы компрессии информации

С точки зрения времени компрессии/декомпрессии различают симметричные и асимметричные методы. В симметричных методах время компрессии (по числу операций) примерно совпадает с временем декомпрессии. В асимметричных методах компрессия требует значительно больше операций (в десятки и сотни раз), чем декомпрессия. Асимметричные методы часто дают большую степень сжатия, чем симметричные при одинаковом качестве результата. Под качеством здесь обычно понимают степень сохранения информации, существенной для её восприятия.

С точки зрения сохранения информации различают методы кодирования:

- **без потери информации;**
- **с потерей информации.**

В первом методе уменьшается информационная избыточность, а во втором стараются потерять прежде всего ту информацию, к которой приёмник (например, человек) нечувствителен или мало чувствителен. Кодирование с потерей информации применяется тогда, когда полное сохранение информации не даёт нужной степени компрессии. Это относится и к мультимедиа-информации. При повторении кодирования с потерей остаётся всё меньше и меньше полезной информации, что приводит к сильному ухудшению качества. Современные алгоритмы сжатия применяют комбинации разных методов.

Аналоговые сигналы естественным образом передают речь, музыку и изображения. Для их преобразования в цифровой сигнал и использования в сетях осуществляется квантование и аналого-дискретное преобразование.

После того, как аналоговый сигнал преобразован в цифровую форму, к нему можно применять различные способы обработки, которые невозможно использовать при работе с чисто аналоговым сигналом. В частности, оцифрованный сигнал перед передачей можно сжать, уменьшив, таким образом, пропускную способность, необходимую для передачи одного голосового соединения.

Существующие алгоритмы сжатия информации также можно разделить на две большие группы:

- 1) алгоритмы сжатия без потерь:
  - алгоритм Лемпеля-Зива (Lempel-Ziv, LZ);
  - RLE (Run Length Encoding);
  - кодирование Хаффмана (Huffman Encoding);
- 2) алгоритмы сжатия с потерями:

Таблица 1.1

- JPEG (Joint Photographic Expert Group);
- M-JPEG;
- MPEG (Motion Picture Expert Group).

### 1.2.1 Кодирование без потерь

Алгоритм Лемпеля-Зива-Уэлча (LZW) отличается от алгоритма Хаффмана кодированием не отдельных элементов, а последовательностей. Используется в архиваторах LHARC, PKZIP, ARJ и т.п. Сжатие текстов — до 50 %. Алгоритм Лемпеля-Зива лежит в основе архиваторов (pkzip, arj, lha) и программ динамического сжатия дисков (Stacker, DoubleSpace). Суть алгоритма заключается в том, что второе и последующие вхождения некоторой строки символов в сообщение заменяются ссылкой на ее первое появление в сообщении. Применяются варианты LZ77, LZSS, LZW (файлы формата GIF, TIFF), BTLZ (рекомендация МККТТ V.42bis). Используется для сжатия текстов и графики.

RLE-алгоритм (Run Length Encoding) кодирует последовательности одинаковых элементов, указывая элемент и длину последовательности. Первоначально предназначался для сжатия рисованной графической информации. RLE применяется для сжатия графики (файлы формата PCX) и видео. Последовательность одинаковых символов заменяется 2 байтами. В первом байте — символ, во втором — счетчик, то есть число, которое показывает, сколько таких символов идет подряд. В PCX-файлах даёт сжатие до 2–3 раз (при 16 или 256 цветах). Сканированная графика, WAVE-звук и видео практически не сжимаются.

Кодирование Хаффмана состоит в замене информационных символов кодовыми последовательностями различной длины. Чем чаще используется символ, тем короче кодовая последовательность. Аналогично построена азбука Морзе. Алгоритм Хаффмана основан на статистике повторяемости. Чаще повторяющиеся элементы (символы, пиксели) кодируются более короткими последовательностями битов. Иногда используются готовые кодовые таблицы (симметричные алгоритмы), иногда они строятся в процессе сжатия на основе статистического анализа информации (асимметричные алгоритмы). Таблица строится в виде бинарного упорядоченного дерева. Кодирование последовательности включают биты, позволяющие отличить их друг от друга.

Применяют и другие алгоритмы сжатия без потери информации:

- сжатие за счет пауз в сигнале (паузы удаляются из исходного сигнала, а их длительность запоминается);
- при хранении и передаче музыки вместо оцифрованного звука - использование информации о том, какие ноты, когда и на каком инструменте нужно исполнять (интерфейс MIDI).

Все эти алгоритмы можно реализовать и аппаратно, и программно: ИКМ и ее ближайшие «родственники» — АИКМ, ДИКМ, АДМ, АДИКМ.

Компандирование для оцифровки телефонного сигнала описано в Рекомендациях МККТТ (Международный консультативный комитет по телефонии и телеграфии, ССГТТ) G.711 и G.712 для А- и мю-законов:

- частота дискретизации 8000 Гц;
- число двоичных разрядов на отсчет 8;
- скорость передачи 64000 бит/с.

### 1.2.2. Кодирование с потерями

Для сжатия речи в виде цифрового или аналогового сигнала применяют алгоритмы сжатия с потерями:

- логарифмическая импульсно-кодовая модуляция (ИКМ) (то есть с компандированием по А- и мю-закону), адаптивная ИКМ (АИКМ), дифференциальная ИКМ (ДИКМ), адаптивная дифференциальная ИКМ (АДИКМ), адаптивная дельта-модуляция (АДМ);

- клипширование речевого сигнала;
- статистическое уплотнение;
- применение вокодеров (устройство для сжатия, кодирования и передачи речи).

Алгоритм JPEG (Joint Photographic Experts Group) используется для цветных неподвижных изображений. Предложен в 1990 году. Сжатие в 10–12 раз практически без заметных потерь, а с потерями — в десятки и более раз.

JPEG ориентирован на сжатие неподвижных изображений. Он базируется на дискретном косинусном преобразовании (ДКП) неподвижного изображения, отбрасывании малых высокочастотных компонентов получаемого спектра и последующем энтропийном сжатии полученных данных. Прореживанием называют уменьшение частоты дискретизации сигналов цветности. Соотношение оставшихся сигналов условно показывают приведенной пропорцией (для JPEG это уменьшение вдвое). Прореживание может не выполняться по желанию пользователя. При прореживании файл сжимается, но возможно ухудшение качества.

ДКП — дискретное косинусное преобразование — вариант преобразования Фурье, позволяющее найти коэффициенты разложения в ряд Фурье по косинусам и получить спектр изображения. Применяется к блокам пикселов, на которые разбивается изображение.

Квантование спектра в блоках, более грубо по отношению к компонентам цветности, удаляет высокие частоты. Оно регулируется пользователем в широких пределах. Чем грубее квантование, тем сильнее сжатие и хуже качество. При плохом качестве видны блоки.

Линеаризация преобразует матрицу блока в последовательность, используя диагональный обход. Полученная числовая последовательность хорошо сжимается алгоритмом Хаффмана (тем лучше, чем грубее квантование).

Самый эффективный стандарт последнего времени — MPEG. Это стандарт сжатия аудио- и видеопотоков, а так же потоков их взаимной синхронизации и так называемых «вспомогательных» потоков. Под потоком понимается битовый файл. MPEG ориентирован на обработку видео. При формировании потока данных исходят из предположения о том, что два соседних кадра в видеопоследовательности мало отличаются. Опорные кадры сжимают по методу JPEG и передают относительно редко. В основном передаются изменения между соседними кадрами.

Всего в настоящее время существует пять видов (номеров) стандартов MPEG: MPEG1 — сжатие аудио и видео с общей скоростью до 150 Кбайт/сек (аудио 38,44.1, 48 кГц); MPEG2 — сжатие аудио и видео с общей скоростью до 300 Кбайт/сек (аудио 38,44.1, 48 кГц), сжатие аудио ИДЕНТИЧНО MPEG1; MPEG2.5 — сжатие аудио с пониженным разрешением (аудио 16,22.05,24 кГц).

MPEG3 — многоканальный MPEG1+MPEG2. Этот стандарт практически не используется. MPEG4 — принятый за рубежом стандарт (до 8-и каналов аудио). В табл. 1.2 приведен перечень стандартов MPEG.

Таблица стандартов

Стандарт	Видео	Аудио	Синхронизация
MPEG1	MPEG1	MPEG1	MPEG1 (150 Кб/сек) 352 X 240 38,44.1,48
MPEG2	MPEG2	MPEG1	MPEG2 (300 Кб/сек) 720 X 520 38,44.1,48
MPEG2.5	нет	MPEG2.5	нет MPEG2 LSF 16,22,05,24
MPEG3	нет	нет	нет
MPEG4	MPEG4	нет	MPEG4 (1200 Кб/сек)

Таблица 1.2

Каждый стандарт содержит несколько частей:

- формат сжатого потока видео;
- формат сжатого потока аудио;
- формат потока синхронизации;
- формат вспомогательного потока;
- неоптимальная программная реализация алгоритмов кодирования и декодирования всех предыдущих потоков (обычно на ANSI си).

Для части стандарта MPEG, относящаяся к аудио, определено несколько слоев качества (Layer - слой). Они так же нумеруются:

- Layer 1;
- Layer 2;
- Layer 3;
- Layer 4 (пока нет).

Layer 1. Позволяет сжимать аудио в 3..12 раз. Качество CD сохраняется при степени сжатия не более 4-х раз. Суть алгоритма сжатия:

1. берется несколько отсчетов левого и правого канала;
2. производится дискретное косинусное преобразование;
3. считается акустическая модель (модель уха);
4. по модели уха и степени сжатия происходит усечение коэффициентов косинусного преобразования;
5. эти усеченные коэффициенты вместе с информацией об их восстановлении пишутся в выходной поток.

Суть алгоритма декодирования:

1. берется заголовок и определяется размер блока коэффициентов;
2. читаются усеченные коэффициенты;
3. коэффициенты восстанавливаются;
4. производится обратное косинусное преобразование (синтезация);
5. полученный сигнал (восстановленное аудио) записывается в выходной поток.

Алгоритм сжатия — медленный (в основном за счет просчета акустической модели и итеративного усечения коэффициентов). Алгоритм декодирования — быстрый (может быть реализован в реальном времени).

Layer 2. Алгоритм строит гребенчатую цепочку аудиоданных в трех циклах, за счет чего общее качество увеличивается субъективно для быстрых скачков аудио-сигнала. Это позволяет сгруппировать коэффициенты для косинусного преобразования в три похожие подгруппы, степень сжатия увеличивается втрое по сравнению со слоем 1. Для улучшения модели уха, внесли в нее процедуры быстрого преобразования Фурье, что значительно замедляет просчет психоакустической модели при кодировании. Все процедуры при сжатии также усложняются в 3 раза, а значит увеличивается и время сжатия. По сравнению с Layer 1 процедура сжатия Layer 2 работает медленнее в 12 раз. При этом алгоритм восстановления потока практически не усложнился, хотя в него приходится внести тройные циклы для 3-х подгрупп коэффициентов обратного косинусного преобразования.

Характеристики сжатия для различных алгоритмов

Алгоритм	Особенности изображения, за счет которых происходит сжатие				
RLE	Подряд идущие одинаковые цвета: 2 2 2 2 2 2 15 15 15				
LZW	Одинаковые подцепочки: 2 3 15 40 2 3 15 40				
Хаффмана	Разная частота появления цвета: 2 2 3 2 2 4 3 2 2 4				
ССИТТ-3	Преобладание белого цвета в изображении, большие области, заполненные одним цветом				
Рекурсивный	Плавные переходы цветов и отсутствие резких границ				
JPEG	Отсутствие резких границ				
Фрактальный	Подобие между элементами изображения				
Алгоритм	Коэффициенты сжатия	Симметричность по времени	Ориентация	Потери	Размерность
RLE	32, 2, 0.5	1	3,4-х битные	Нет	1D
LZW	1000, 4, 5/7	1.2-3	1-8 битные	Нет	1D
Хаффмана	8, 1.5, 1	1-1.5	8 битные	Нет	1D
ССИТТ-3	213(3), 5, 0.25	~1	1-битные	Нет	1D
JBIG	2-30 раз	~1	1-битные	Нет	2D
Lossless JPEG	2 раза	~1	24-бит. сер.	Нет	2D
Рекурсивное сжатие	2-200 раз	1.5	24-битные, серые	Да	2D
JPEG	2-200 раз	~1	24-битные, сер.	Да	2D
Фрактальный	2-2000 раз	1000-10000	24-бит. сер.	Да	2.5D

В приведенной таблице видны следующие тенденции развития алгоритмов сжатия изображений:

- 1) ориентация на фотореалистичные изображения с 16 миллионами цветов (24 бита);
- 2) использование сжатия с потерями, возможность за счет потерь регулировать качество изображений;
- 3) использование избыточности изображений в двух измерениях;
- 4) появление существенно несимметричных алгоритмов;
- 5) увеличивающаяся степень сжатия изображений.

Алгоритмы сжатия и декодирования аналогичны алгоритмам слоя 1 с поправкой на утроенный цикл получения коэффициентов и усложненный психоакустический алгоритм. Субъективно алгоритм Layer 2 дает качество, неотличимое от CD при степени сжатия 4.6 раз. Файлы, упакованные этим слоем, имеют расширение MP2.

Layer 3. В этом слое применяется преобразование второй раз вдоль коэффициентов. Разделили коэффициенты на три связки (то есть первая связка - 1-й,4-й,7-й и т.д. коэффициент; вторая связка 2-й, 5-й, 8-й и т.д. коэффициент; третья связка 3-й, 6-й, 9-й коэффициент и т.д.). Пропускали еще одно дискретное косинусное преобразование по отдельности на этих связках, подкорректировали алгоритм декодирования. В результате улучшений при той же степени сжатия качество выросло в 4 раза!

В совокупности Layer 3 получился качественным и медленным. Мало того, необходимо было опять переделывать и усложнить психоакустические модели и добавить некоторые элементы архивации по фиксированной таблице Хаффмана.

Метод WIC (Wavelet Image Compression) — аналогичен JPEG, но вместо разложения по тригонометрическим функциям используется разложение по специальным волновым функциям — вэйвлетам, что увеличивает степень сжатия.

Фрактальное сжатие. Термин «фрактальный» ввел Б. Мандельброт. Практическое применение для сжатия изображений нашли фракталы на основе систем итеративных функций (IFS — Iterated Function System). IFS строится для каждого изображения (автоматически) с таким расчётом, чтобы при их повторяющемся выполнении изображение постепенно уточнялось. Чем больше выполняется итераций, тем лучше его качество. Коэффициент сжатия достигает 10000:1, но процесс сжатия (т.е. построение IFS) длится долго.

### 1.2.3. Сжатие движущихся изображений

Для видео необходимо сжатие в 100 и более раз. Для этого используется как внутрикадровое (intraframe), так и межкадровое (interframe) сжатие.

Внутрикадровое сжатие применяется к ключевым кадрам. Для этого применяются методы от RLE и JPEG до WIC и фрактальных преобразований.

Межкадровое сжатие осуществляется с помощью деления на ключевые и дельта-фреймы (последние получают как разности).

Невозможно составить универсальное сравнительное описание известных алгоритмов. Это можно сделать только для типовых классов приложений при условии использования типовых алгоритмов на типовых платформах. С распространением Internet, который характеризуется передачей изображений по сравнительно медленным каналам связи, использование Interlaced GIF (алгоритм LZW) и Progressive JPEG (вариант алгоритма JPEG), реализующих эту возможность, резко возросло.

В заключении рассмотрим таблицу, в которой сводятся воедино параметры различных алгоритмов сжатия изображений, рассмотренных выше.

## ГЛАВА 2 МЕТОДЫ ПЕРЕДАЧИ ИНТЕГРАЛЬНОЙ ИНФОРМАЦИИ

### 2.1. Каналы связи

Основное назначение коммуникаций — обмен сообщениями. Сообщение — это некоторая логически законченная совокупность сведений о состоянии какой-либо материальной системы. Сообщение должно содержать информацию, т.е. совокупность сведений, снимающих неопределенность. Для передачи сообщений необходим носитель, природа и характеристики которого определяются физической средой между источником и получателем информации — линией связи. Обычно носителем является электромагнитное поле. Для того чтобы носитель мог выполнять свою функцию — передачу информации, его характеристики должны иметь возможность меняться. Между характеристиками носителя и сообщением существует однозначная зависимость. Такой носитель называется сигналом. После того, как получатель принял информацию, он может извлечь ее, зная закон соответствия сигналов и сообщений.

Передача сообщения включает следующие процедуры:

- преобразование из незлектрической формы в электрическую;
- первичное кодирование;
- преобразование с целью согласования характеристик сигнала с характеристиками канала связи;
- передача сигнала;
- декодирование;
- обратное преобразование для восприятия сообщения.

Сигналы по своей природе можно разделить на аналоговые (с непрерывными значениями функции) и цифровые (с дискретными значениями). Канал связи, предназначенный для передачи аналоговых сигналов, соответственно, называется аналоговым, а для передачи цифровых сигналов — цифровым.

Аналоговые сигналы можно преобразовать в цифровые с помощью процесса квантования и дискретизации, при котором весь диапазон значений аналогового сигнала разбивается на определенное количество непересекающихся областей так, что все значения сигнала, попадающие в одну из этих областей, заменяются одним дискретным значением. Квантование при этом происходит только по какому-то параметру сигнала, например, по амплитуде, а дискретизация по времени.

Второй этап преобразования сообщения в сигнал — кодирование — заключается в преобразовании букв, чисел, знаков в символы некоторого другого алфавита. Правило этого преобразования называется кодом. Одним из главных параметров кода является его основание, равное основанию выбранной системы счисления, т.е. числу символов в коде. При передаче дискретной информации обычно используется код с основанием 2, при этом каждый символ кода может принимать только два значения: 0 или 1. Такие коды называют двоичными или бинарными. Каждому знаку исходного сообщения — элементарному сообщению — соответствует некоторая последовательность кодовых символов — кодовая комбинация. При этом знаком в исходном сообщении может являться буква или знак препинания. Таким образом, система кодирования сообщения задается в виде некоторой таблицы — словаря, где каждому элементарному сообщению в исходном алфавите сопоставлен некий набор символов другого — машинного — алфавита, у которого только два значения 0 или 1. В итоге исходное буквенно-цифровое сообщение, понятное человеку, оказывается преобразованным в цифровой форме в виде последовательности нулей и единиц.

Процесс преобразования сообщения включает также операцию модуляции, обычно имеющей отношение к преобразованию аналогового сигнала. Под цифровой модуляцией понимают процесс преобразования последовательности кодовых символов в последовательность элементов передаваемого сигнала. Модуляция состоит в изменении одного или нескольких параметров носителя. В аналоговых каналах в качестве носителя используются синусоидальные колебания или периодические последовательности импульсов. Последовательность импульсов можно модулировать по амплитуде, ширине импульсов, частоте их следования, что также можно назвать амплитудной, фазовой и частотной модуляцией. Устройства, осуществляющие оба эти преобразования и при их конструктивном совмещении, называются модемами.

Каждый элемент кода — кодовый символ — в процессе модуляции превращается в отрезок переносчика длительностью  $T$ , который называют единичным элементом. Число единичных элементов, передаваемых за 1 секунду, называется скоростью модуляции. За единицу скорости принят бод — скорость, соответствующая передаче одного единичного элемента в секунду. Информационная скорость передачи, под которой принято понимать количество информации, поступающее по системе передачи от источника к получателю за 1 секунду, измеряется в бит/с.

Важным параметром сигнала являются его частотные характеристики. Спектр сигнала — это набор значений частот его составляющих. На рис. 2.1. показан прямоугольный импульс и его частотный и фазовый спектры. Спектр сигнала, на выходе линии связи характеризует ее пропускную способность.

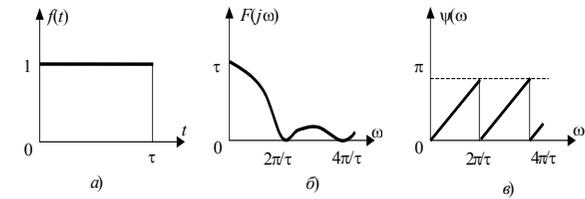


Рис. 2.1. Прямоугольный импульс (а) и его амплитудный (б) и фазовый (в) спектры

Сигнал, имеющий синусоидальную форму, называется гармоническим. Его параметры определяются частотой и амплитудой. Чем больше форма сигнала отличается от синусоиды, тем больше гармонических составляющих он несет. Частоты гармоник кратны частоте несущей. Стандарты электропитания, например, требуют оценки качества напряжения сигнала вплоть до тридцатой гармоники. Диапазон частот сложного сигнала называется спектральной шириной сигнала. Он включает основную составляющую, которая определяет несущую, и гармонические составляющие, которые задают форму импульсов. Восстановление формы импульсов производится на аппаратном уровне, поэтому гармонические составляющие убирают с помощью фильтров. Спектральная ширина сигнала зависит от тактовой частоты, метода кодирования и характеристик фильтра передатчика.

Рис. 2.2 иллюстрирует, как метод кодирования позволяет уменьшить частоту несущей. Для трех методов кодирования приведены ситуации, требующие максимальную частоту несущей. Один герц несущей передает один бит (1) при манчестерском кодировании, два бита (01) кода NRZ и четыре бита (1111) кода MLT-3. Фактор кодирования (передача) составляет соответственно один, два и четыре.

Другие комбинации битов требуют меньшей частоты. Например, при чередовании нулей и единиц частота несущей кода MLT-3 уменьшается еще в два раза, длительная последовательность нулей уменьшает частоту несущей до нуля.

Рис. 2.2. Альбомная

Спектральную ширину сигнала не следует путать с тактовой частотой. Тактовая частота — это метроном, задающий темп мелодии. На рис. 2.2 тактовой частоте соответствует скорость чередования битов. Спектральная ширина сигнала в данной аналогии это огибающая сигнала при условии, что она позволяет восстановить исходный импульсный сигнал.

В аналоговой передаче спектральная ширина — это мелодия, имеющая гораздо более широкий спектр. Если попытаться передать мелодию по телефону, придется пожертвовать спектром. Линия связи, имеющая узкую полосу пропускания, «обрежет» верхние гармоники. При этом качество звучания мелодии на выходе узкополосного канала связи ухудшится.

При цифровой передаче для восстановления исходного сигнала требуется меньше гармоник, чем для аналогового. Технология передачи и приема цифровых сигналов позволяет восстановить исходный сигнал по несущей спектра. Однако для уменьшения коэффициента ошибок необходимо присутствие первой гармоники, что удваивает ширину спектра или частотный диапазон.

Для повышения эффективности использования каналов связи широко применяется частотное разделение каналов. При этом для различных каналов отводятся не пересекающиеся полосы частот  $\Delta f_1, \Delta f_2, \dots, \Delta f_N$  на частотной шкале. Спектры сигналов соответствующих каналов должны укладываться в пределы  $\Delta f$ .

Для изучения каналов связи лучше всего применять спектральные методы, которые используют частотное представление функции в виде преобразования Фурье во временной или пространственной форме. При рассмотрении спектра сигнала главное внимание уделяется определению его ширины, поскольку в основном этот фактор используется для согласования сигнала с аппаратурой обработки информации, причем для исключения потерь информации ширина спектра сигнала не должна превышать полосы пропускания канала.

Для непериодического сигнала определяемого на бесконечном интервале времени, преобразование Фурье выглядит следующим образом:

$$W(\omega_T) = \int_{-\infty}^{\infty} U(t) \cdot e^{-j \cdot k \cdot \omega t} dt,$$

где  $W(\omega_T)$  — спектральная плотность,

$U(t)$  — функция сигнала,

$k$  — фактор кодирования (количество бит, шифруемое за 1 Гц, для максимальной частоты несущей).

Любой канал связи, как аналоговый, так и цифровой, влияет на форму передаваемых сигналов потому, что в процессе передачи на них накладываются всевозможные помехи, а также происходит затухание сигнала. Канал связи можно представить как полосовой фильтр, пропускающий на выход определенные частоты с некоторым ослаблением. Затухание тем больше, чем длиннее канал, и поэтому в любых системах передачи на трассе канала устанавливаются усилительные (на аналоговом канале) или регенерационные (на цифровом канале) пункты, с помощью которых сигнал возвращают к исходному с определенной погрешностью. Канал связи состоит аппаратуры передачи данных (DCE для аналоговых сигналов и CSU для цифровых сигналов) и линии связи. К основным характеристикам линии связи относятся:

- частотные характеристики;
- полоса пропускания;
- затухание;
- помехоустойчивость;
- перекрестные наводки на ближнем конце линии;
- пропускная способность.

Под полосой пропускания здесь понимается спектр частот затухания сигнала, который не выходит за разрешенные пределы. Для различных систем номинальные значения затухания разные, соответственно, на одном и том же канале для разных систем нужно по-разному оценивать пропускную способность. Из этого определения мы видим, что на возможную скорость передачи в канале влияют, помимо полосы пропускания, только мощности сигнала и помехи.

Стандартный телефонный канал имеет ширину полосы пропускания от 300 до 3400 Гц. При этом подавляющее большинство абонентских телефонных линий аналоговые. Пропускная способность аналогового канала с аддитивной помехой в виде белого шума определена Шенноном как

$$C_a = F \times \log_2(1 + P_c / P_{ш}) \quad (3)$$

где  $P_c$  и  $P_{ш}$  — соответственно средние мощности сигнала и помехи в полосе пропускания канала  $F$ .

Связь между полосой пропускания линии связи и ее максимально возможной пропускной способностью независимо от принятого способа кодирования можно представить в следующем виде. Пусть  $H'(x)$  — энтропия источника,  $C$  — пропускная способность канала связи. Из теоремы Шеннона известно, что при  $H'(x) < C$  сообщения дискретного источника могут быть закодированы сигналами на входе канала и восстановлены по сигналам на выходе канала со сколь угодно близкой к нулю вероятностью ошибки, а при  $H'(x) > C$  это невозможно. Поэтому пропускная способность канала должна быть выше производительности источника сообщений.

Существуют взаимные влияния между различными парами проводов в общем кабеле, количество которых может достигать нескольких десятков и даже сотен. Основной причиной переходных влияний между парал-

лельными цепями являются индуктивные и емкостные связи. Уровень таких влияний зависит от того, какого типа кабель используется в системе связи.

Наличие несогласованности в точках подключения абонентской установки к системе передачи приводит к возникновению так называемого электрического эха. Так как все линии связи вносят в передачу сигналов замедление вследствие конечной величины скорости распространения электромагнитной энергии, то говорящий абонент услышит свою речь сдвинутой во времени. Мешающее действие токов электрического эха тем больше, чем меньше затухание и больше время распространения на пути этих токов. Время распространения токов эха вдвое больше времени распространения полезного сигнала.

Помимо искажений, связанных с изменением формы сигналов, каналы связи вносят еще и временные искажения. Сигнал попадает в приемник только спустя какое-то время после выдачи его передатчиком. Это особенно важно для передачи данных. Задержка различна на различных частотах. В результате оказывается, что каждая составляющая полезного сигнала проходит по каналу за свое время. Это приводит к размытости передаваемых сигналов во времени, что мешает правильному приему.

Условием отсутствия искажений является идентичность спектров сигналов на выходе и входе канала связи. Спектр сигнала на выходе канала  $\bar{S}_{\text{вых}}(w)$  связан со спектром сигнала на его входе  $\bar{S}_{\text{вх}}(w)$  соотношением  $\bar{S}_{\text{вых}}(w) = \bar{K}(w) \times \bar{S}_{\text{вх}}(w)$ , где  $\bar{K}(w)$  — коэффициент передачи канала связи. Следовательно, условие отсутствия искажений сигналов с учетом того, что  $\bar{K}(w) = K(w) \times e^{j\phi(w)}$ , может быть записано так:

$$K(w) = \text{const}, \quad j(w) = wt,$$

где  $K(w)$  — АЧХ, а  $j(w)$  — ФЧХ канала связи. Таким образом, даже при полном отсутствии помех имеются два фактора, вызывающие искажения при передаче: ограничение спектра и неравномерность амплитудной и фазочастотной характеристик. Все современные модемы имеют средства, которые помогают существенно ослабить влияние этих факторов. Для устранения затухания сигнал усиливают по трассе канала или генерируют сигнал высокой мощности.

Амплитуда аналогового сигнала может принимать любые значения, следовательно, в оконечном или транзитном пункте невозможно точно восстановить исходное значение. Поэтому производится усиление входного сигнала для того, чтобы перекрыть внесенное каналом затухание. При этом вместе с полезным сигналом будет усилена и помеха. Это и есть основной критерий качества цифрового канала. Так, когда говорят, что уровень ошибок в цифровом канале равен  $10^{-8}$ , то это означает, что в среднем импульсы восстанавливаются на приеме неправильно с вероятностью  $10^{-8}$ .

Оценим максимальную скорость передачи информации. Скорость передачи ограничивается флуктуационным шумом, уровень которого зависит от длины канала и составляет 30–32 дБ. Отношение уровней мощностей двух величин задается формулой  $10 \lg P_c / P_{ш}$ . Если эта величина равна 30 дБ, то соотношение  $P_c / P_{ш} = 1000$ .

Таким образом, по формуле  $C_a = F \times \log_2(1 + P_c / P_{ш})$  при ширине полосы пропускания канала в 3000 Гц, получим  $C_a = 30\,000$  бит/с. Это и есть теоретический предел скорости.

Вся процедура частотного уплотнения сводится к тому, что каждый исходный канал с помощью перемножителей частоты переносится в другую частотную область (рис. 2.3). Например, стандартная 12-ти канальная группа занимает спектр частот от 60 до 108 кГц.

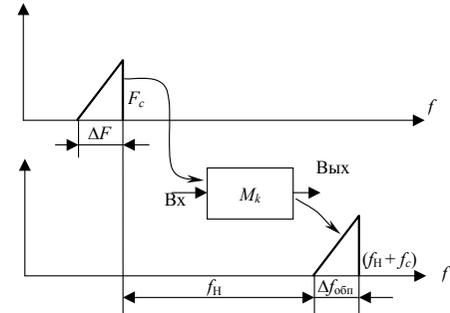


Рис. 2.3. Перенос спектра сигнала в другую частотную область

В групповом тракте каналы разносятся по частоте и поэтому не смешиваются друг с другом. Для работы таких систем нужна специальная аппаратура на концах линии, а по трассе кабеля должны стоять усилительные пункты. Каналообразующая аппаратура отводит под каждый телефонный канал полосу в 3100 Гц. Эта полоса называется тональным спектром, поскольку она предназначена для передачи тональных (слышимых ухом) сигналов, а сами эти каналы называются каналом тональной частоты.

Цифровые сигналы имеют более широкий спектр, чем ширина полосы пропускания аналогового канала. Для передачи цифровых сигналов по аналоговым каналам связи необходимо согласовать их по частоте с помощью цифровых модемов, в которых модулируемые параметры сигнала имеют только фиксированные значения из некоторого определенного набора. Это связано с тем, что исходный передаваемый сигнал является дискретным, принимающим только два значения: 0 или 1. На рис. 2.4 приведены примеры амплитудной, частотной и фазовой модуляций.

Прямоугольные импульсы заменились на отрезки синусоид, что и превратило цифровой сигнал в аналоговый, который можно передать по телефонному каналу.

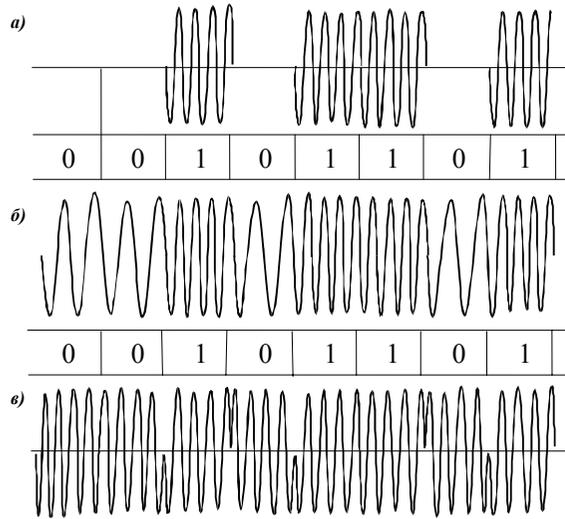


Рис. 2.4. Виды двухпозиционной модуляции: амплитудная (а), частотная (б), фазовая (в)

## 2.2. Асинхронная цифровая передача, ее особенности

Источники и приемники информации должны обмениваться между собой данными для оповещения о своей готовности к передаче или приему данных и информировании устройств о передаваемых сообщениях. Передатчик (ЭВМ или терминал) передает определенный сигнал, с тем, чтобы принимающее устройство знало, когда начать поиск и распознавание поступающих данных. Этот процесс является частью протокола связи и называется синхронизацией. Для обеспечения синхронизации используется одно из двух соглашений относительно форматирования сообщения. Первый подход называется асинхронным форматированием (рис. 2.5). Согласно этому подходу, каждый байт данных (каждый знак первичного кода) обрамляется сигналами «старт» и «стоп». Они, помещаются перед байтом и после него.

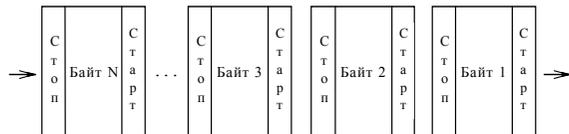


Рис. 2.5. Асинхронный формат

При асинхронной работе в периоды молчания канал заполняется двоичными единицами. В момент начала передачи перед каждым знаком передатчик вставляет ноль, который соответствует сигналу «старт», после него следуют информационные биты. После окончания передачи комбинации знака следует двоичная единица, означающая знак «стоп». После окончания передачи стопового сигнала за ним может следовать стартовый сигнал или же выдерживаться пауза, которая также заполняется единицами.

Необходимо заметить, что начало передачи знака производится асинхронно, но в составе этого знака все биты передаются синхронно. Таким образом, длительность каждого знака определена заранее. Между знаками не может быть пропусков, поскольку на приеме считывание бит производится через строго определенные промежутки времени, определяемые скоростью работы канала.

## 2.3. Синхронная цифровая передача

По синхронному каналу передачу можно вести с гораздо большей скоростью, чем по асинхронному, при этом избыточность синхронной системы намного ниже.

В синхронной системе ось времени разбита на последовательность моментов, причем начать передачу можно только в один из этих моментов. Когда канал проинициализирован и никаких данных по нему не передавалось, в линию постоянно передается одна и та же кодовая комбинация, которая называется флагом (также флаги называют синхробайтами). Длина флага один байт. Следуют они в канал друг за другом без пропусков. Когда у источника возникает необходимость передать в канал порцию данных, он обязан дожидаться окончания передачи флага. Таким образом, источник синхронизирован с каналом, поскольку скорость передачи флагов задает скорость работы канала и является общей для обоих устройств.

На рис. 2.6. приведен формат синхронной передачи. Как видим, в его составе между синхробайтами создано несколько полей, четыре из которых являются служебными и только одно содержит пользовательские данные.



Рис. 2.6. Синхронный формат (а) и типичная синхронная передача (б)

## 2.4. Взаимодействие компьютера с модемом. ООД и ООК

Перед тем как непосредственно перейти к рассмотрению взаимодействия компьютера с модемом, необходимо определить понятия оконечного оборудования данных — ООД (английский вариант DTE — Data Terminal Equipment) и оконечного оборудования канала — ООК (DCE — Data Circuit Equipment). ООД — это, как правило, источник информации, т.е. терминал или коммуникационный порт узла коммутации. ООК чаще всего бывает канальное оборудование (модем). Интерфейсный порт модема всегда определен как ООК.

ООД и ООК имеют разные функции. Логическое ООД может иметь доступ к каналу через физическое ООК и наоборот. Видно, что физический тип устройства и логическая процедура никак не связаны между собой. Функции логических устройств на канале также несколько различаются.

На сегодняшний день наиболее массовым способом подключения аппаратуры к каналам связи является интерфейс V.24. Наиболее популярные типы цифровых стыков — V.24 и V.35 (они отличаются лишь тем, что V.35 более высокоскоростной и позволяет передавать цифровой поток со скоростью до 2 Мбит/сек, тогда как стык V.24 работает на скоростях до 115 кбит/сек).

Модем — это сложное аналогово-цифровое устройство, обеспечивающее передачу цифровой информации по аналоговым коммутируемым и арендованным телефонным каналам. В соответствии с цифровой информацией, поступающей от ООД, в модемах производится модуляция параметров несущего синусоидального колебания с целью формирования спектра сигнала, пригодного для передачи по телефонному каналу с полосой пропускания 0,3–3,4 кГц. В модеме принятый из канала модулированный сигнал, подвергшийся воздействию помех и искажений, усиливается, корректируется и демодулируется для выделения исходной цифровой информации.

В настоящее время в набор функций, выполняемых модемом, введены защита от ошибок и сжатие данных, что позволило увеличить скорость передачи. Наиболее часто используемыми скоростями являются теперь 28800 и 33600 бит/с. Из-за сжатия фактическая скорость передачи цифровой информации может достигать 40–60 кбит/с. В последнее время начинают получать распространение совершенно новый класс модемов, работающих на скорости до 56000 бит/сек.

Технология DSL (Digital Subscriber Line) была разработана специально для работы по аналоговым неуплотненным парам. Максимальное расстояние, на котором может работать DSL, — 5.5 км.

DSL разбивается на подсистемы. Одной из таких подсистем является ADSL (Asymmetric Digital Subscriber Line). Она называется асимметричной потому, что большая часть полосы пропускания отведена для приема. Это особенно удобно для организации доступа в Internet, когда пользователи главным образом принимают данные из сети, а передают, как правило, только запросы на получение информации. При настройке канала ADSL нужно правильно установить, в каком направлении организовать широкий тракт, а в каком — узкий. Это позволяет иметь канал в одном направлении до 6.1 мбит/сек на расстояние до 3.5 км и до 640 кбит/сек — в другом. Подобная скорость позволяет передавать видео, аудио, трехмерную графику. Кроме того, процедура ADSL имеет возможность вырезать небольшую полосу частот для передачи по ней телефонных переговоров. Это особенно удобно в тех случаях, когда доступ к Internet и к телефонной сети осуществляется через одного оператора. Однако для реализации этого у пользователя должен находиться специальный «разделитель» — splitter, который разделяет спектры частот, предназначенные для телефонии и для передачи данных.

Вариантом реализации DSL, где такой разделитель не нужен, является CDSL (Consumer DSL). Такой вариант более удобен для пользователя при настройке и установке, однако, это удобство дается за счет уменьшения скорости работы до 1 Мбит/сек в одном направлении и до 640 кбит/сек — в другом. Самой ранней реализацией DSL является HDSL (High bit-rate DSL). Здесь нет асимметрии между направлениями передачи и приема и поэтому скорость меньше, чем в ADSL. Еще одной особенностью HDSL является то, что она работает по четырехпроводному каналу, тогда, как ADSL и CDSL — по двухпроводному. Максимальная скорость передачи в обоих направлениях — до 2 Мбит/сек. Есть, однако, усовершенствование этой системы, — SDSL (Single-Line DSL), — позволяющее работать на одной паре. Еще одной разновидностью DSL, пока не внедренной, является RADSL (Rate-Adaptive DSL). Устройства RADSL хороши тем, что встроенные протокольные средства позволяют этим модемам самостоятельно определять скорость, на которой они могут работать, в зависимости от качества линии и уровня затухания. Правда, максимальная скорость работы у них ниже — до 2.2 Мбит/сек в одном направлении и до 1 Мбит/сек — в другом.

## 2.5. Принципы организации цифровых каналов

### 2.5.1. Преимущества цифровых систем

В цифровых системах передача сигнала идет в виде двоичных данных, так как параметр сигнала может принимать только два значения. Цифровые сигналы так же, как и аналоговые, подвержены ослаблению и воздействию шумов. Поскольку цифровые сигналы дискретны, то при прохождении их через канал необходимо отмечать только отсутствие или наличие сигнального импульса. Цифровые сигналы можно полностью реконструировать прежде, чем они исказятся настолько, что их точное восстановление будет выполнено с большой вероятностью ошибки.

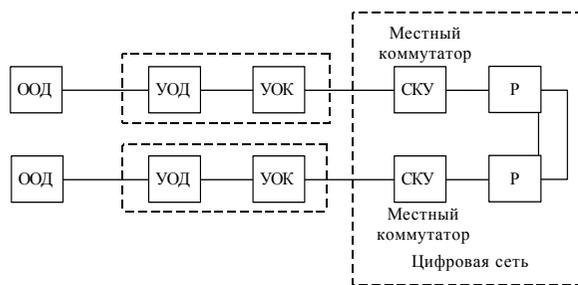


Рис. 2.7. Структура цифрового канала

На рис. 2.7: УОД — устройство обслуживания данных, УОК — устройство обслуживания каналов, СКУ — станционное канальное устройство, Р — регенератор.

Для восстановления параметров сигналов используются регенераторы, устанавливаемые через определенные промежутки цифрового тракта. Структуру цифрового тракта можно представить на рис. 2.7. Здесь передат-

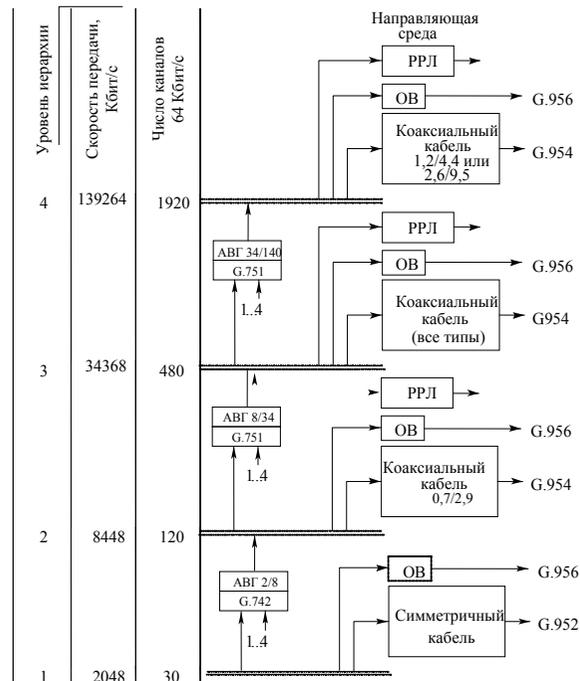
чик выполняет функции преобразования исходного сигнала в цифровую форму; приемник выполняет функции регенератора, а также производит преобразование двоичного цифрового сигнала в исходную форму.

### 2.5.2. Иерархия цифровых каналов

Для передачи интегральной информации целесообразно использовать цифровые телефонные каналы, где полоса пропускания и скорость передачи спроектированы для передачи речевых сообщений. Для передачи данных, видео, высококачественного звука необходимо пользоваться объединением выделенных полос, или цифровой иерархией. Основой для цифрового телефонного сигнала является канал 64кбит/сек, который возглавляет иерархию каналов передачи.

Существует две принципиально разных структуры иерархии — американская и европейская. На рисунке 2.8(a) представлена европейская иерархия с указанием типа физической среды, пригодной в использовании для передачи на таких скоростях, а на рисунке 2.8(б) — американская система иерархии. В европейской системе мультиплексирование производится всегда ступенями по четыре, в американской оно меняется. Так, система DS3 образуется объединением двадцати восьми систем DS1. Неподвижными точками в иерархии являются стыки, в которых могут соединяться любым образом друг с другом аппараты, рассчитанные на одну и ту же скорость передачи. Для этого в рекомендации G.703 устанавливаются формы импульсов и коды передачи сигналов на стыках.

Стандартные стыки (например, стык G.703) жестко указывает на форму сигналов. Если работать по такому стыку непосредственно через канал, то вследствие неизбежных искажений сигнал уже не будет иметь требуемую форму, и приемник, работающий по стандартному стыку, не сможет их декодировать. Поэтому совершенно необходимо выполнение некоторых преобразований на передаче и функции регенерации сигнала на приеме для того, чтобы на входе аппаратуры можно было работать стандартными сигналами. Без этого передавать сигналы можно только на очень короткое расстояние. Так, по стыку G.703 можно напрямую работать на расстоянии до 200 метров. Кроме того, выполняется дополнительное кодирование исходного сигнала с целью исключить постоянную составляющую и ввести в код систему синхронизации. Поэтому необходимо использовать дополнительные устройства для преобразования сигналов, цифровые модемы.



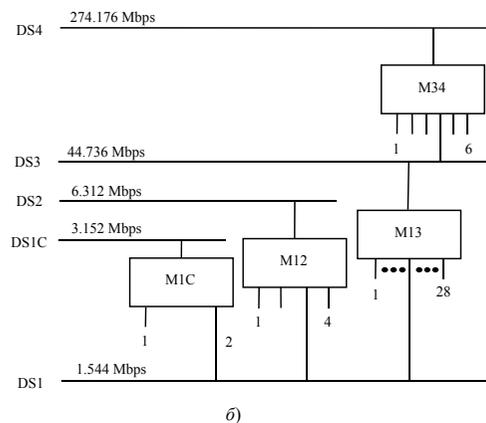


Рис. 2.8. Цифровые иерархии:

а) иерархия цифровых сигналов на основе 2048 Кбит/с, где АВГ — аппаратура временного группообразования, ОВ — оптическое волокно; G..., H..., Q... — обозначения соответствующих рекомендаций МККТГ; РРЛ — радиорелейная линия, прерывистая линия плоскость стыков (часто также точка переключений): стыки в соответствии с рекомендацией МККТГ G.703; б) система североамериканской цифровой иерархии

## 2.6. Организация цифрового телефонного канала 64 кбит/сек

Для превращения аналоговых сигналов в цифровые строки из двоичных значений используются различные методы. Первый широко используемый подход, называемый импульсно-кодовой модуляцией (ИКМ), разработан в 1938 году компанией Bell Labs. Основой этого метода является то, что между аналоговым сигналом и преобразованным цифровым существует взаимно однозначное соответствие, если аналоговый сигнал дискретизировать с частотой в два раза большей максимальной частоты его спектра. В промышленности принята стандартная частота дискретизации, равная 8000 Гц.

Общая структура передающего устройства ИКМ изображена на рисунке 2.9. В общем случае аналоговый сигнал проходит через устройство дискретизации, т.е. производятся мгновенные замеры амплитуды сигнала с частотой, большей, удвоенная максимальная частота спектра сигнала. Далее сигнал, соответствующий второму классу, проходит через устройство квантования, в котором произвольные значения амплитуды замеров дискретизируются по значениям конечного множества. Обычно бывает до 256 таких дискретных значений. Очевидно, чем больше число возможных дискретных значений, тем меньше искажений претерпит сигнал и, следовательно, тем точнее он будет соответствовать исходному аналоговому сигналу. После квантования получается сигнал четвертого класса. Последним этапом преобразования сигнала в устройстве передатчика является кодирование — разложение каждого квантованного значения на двоичные символы. По сути его можно представить как преобразование десятичного числа в двоичное. Длина этой двоичной комбинации определяется количеством возможных квантованных значений. Так, если это число равно 256, то необходимо для кодирования каждого значения использовать двоичную комбинацию длины 8. В этом случае каждый квантованный отсчет сигнала кодируется двоичной комбинацией длины 8 и затем передается по каналу связи.

Рис. 2.9. — альбомный

Цифровой сигнал может быть искажен различными способами. Так, помимо искажений в канале, ошибки возникают из-за процедуры квантования значений дискретных отсчетов аналогового сигнала. Ее можно было бы устранить путем поднятия частоты дискретизации и увеличения числа уровней квантования. Это, однако, потребует более дорогостоящих компонентов и более широкой полосы пропускания канала.

Другим широко применяемым и стандартизованным МККТГ методом цифровой передачи является метод дифференциальной импульсно-кодовой модуляции (ДИКМ). В канал передаются не фактические отображения аналогового сигнала, а только разница между соседними отсчетами. Это основано на структуре аналогового сигнала, чья амплитуда меняется сравнительно медленно и величина разницы между двумя отсчетами значительно меньше амплитуды самого сигнала. Следовательно, значения этой разницы можно кодировать не 8 битами, а меньше (например, четырьмя). Принцип работы одной из разновидностей ДИКМ, называемой дельта-модуляцией (ДМ), изображен на рисунке 2.10. Его суть состоит в том, что амплитуда разницы между двумя соседними отсчетами всегда принимается равной единице, а в канал передается только знак изменения (в сторону возрастания или в сторону убывания амплитуды). Более совершенным методом ДМ является адаптивная ДМ, при котором значение разницы может принимать не одно, а несколько значений.

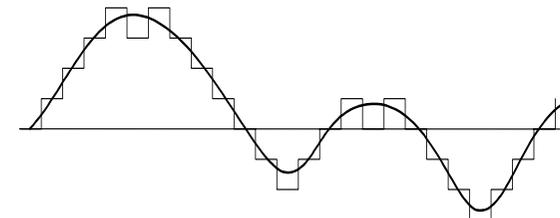


Рис. 2.10. Принцип дельта-модуляции

Важным преимуществом ИКМ является ее малая чувствительность к шумовым помехам, поскольку на промежуточных пунктах регенерации сигнала достаточно просто отличать ноль от единицы. При правильном различении все наложенные помехи сглаживаются.

## 2.7. Мультиплексирование цифровых сигналов

В цифровых трактах также производится уплотнение, но не частотное, а временное. В аппаратуре группообразования цифровые импульсы одного канала перемежаются импульсами другого в строго заданной последовательности. В результате получается, что суммарная частота следования импульсов в групповом тракте складывается из частот следования составляющих. Этот процесс проиллюстрирован на рис. 2.11. На вход аппаратуры группообразования подается четыре различных исходных канала, в каждом из которых импульсы следуют с частотой 64 кбит/сек. Аппаратура циклически осматривает каналы и последовательно соединяет с выходом каждый из входов. Получается, что каждому из входных каналов в групповом тракте соответствует закрепленный за ним временной интервал (time-slot), в котором будут передаваться его сигналы. Число таких интервалов определяется числом мультиплексируемых каналов. В этом состоит принцип временного уплотнения.

Рис. 2.11. - альбомная

Для того чтобы на приеме можно было из потока извлечь все исходные низкоскоростные сигналы, требуется точная система синхронизации и фазирования. Это означает, что момент подключения на вход канала какого-либо источника должен точно совпадать с моментом подключения к каналу соответствующего приемника. В этом состоит принцип фазирования. Синхронизация же обеспечивает равенство скоростей передачи и приема на обоих концах. Для этих целей в групповой высокоскоростной сигнал вставляются специальные тактовые сигналы, с помощью которых и задается синхронность и синфазность работы обоих устройств.

Второе отличие основано на том, что в Европе принято объединять в один групповой тракт 32 исходных канала, а в Америке — 24. Отсюда расхождение в скорости работы этих трактов, которая составляет 2048 кбит/сек и 1544 кбит/сек соответственно. Заметим, что в европейской системе произведение числа каналов на скорость каждого из них ( $32 \cdot 64$  кбит/сек) составляет 2048 кбит/сек, а в американской системе итоговое произведение дает результат 1536 кбит/сек. Разница в 8 кбит/сек используется для передачи управляющей информации. В европейской системе для этих целей были специально отведены два канала - первый (под синхронизацию) и шестнадцатый (под сигнализацию). Это также нашло отражение на рис. 2.11. В американской системе не выделяется отдельного временного интервала ни под сигнализацию, ни под синхронизацию. Эти сигналы как бы размазаны по информационным time-slot-ам, так как для передачи сигналов широкой полосы не требуется. Благодаря отсутствию специальных служебных каналов удается значительно понизить избыточность системы. Так, в европейской системе на эти цели отводилось  $2/32 = 7\%$  пропускной способности, тогда как в американской всего 1.5 %.

Заметим, что когда происходит временное уплотнение, то за одно подключение источника к каналу в канал выдается не один бит, а целый байт. То есть здесь имеет место коммутация байтов.

## 2.8. Синхронизация в цифровых сетях

Для обеспечения качественной работы цифровых сетей требуется битовая синхронизация, с помощью которой передатчик и приемник работают с импульсами одинаковой длительности. Другими словами, битовая синхронизация определяет, что каждый кадр передается на 125 мсек и каждый импульс имеет соответствующую длительность.

С битовой синхронизацией связаны два распространенных типа помех — вставки и выпадения. Они появляются за счет того, что тактовая частота, на которой работает передатчик, не точно совпадает с частотой работы приемника. Так, если приемник сканирует принимаемый сигнал несколько чаще, чем их выдает передатчик, то вскоре окажется, что на интервал одного бита попадет два синхроимпульса, и, таким образом, этот бит как бы удвоится, т.е. произойдет вставка бита, что и вызовет ошибку при приеме. Другой тип ошибки — выпадение - происходит, если частота приемника меньше частоты передатчика. В этом случае произойдет ситуация, когда на один из битов не придется ни одного синхроимпульса. Очевидно, что чем более совпадают частоты передатчика и приемника, тем меньше будет встречаться вставок и выпадений.

Чтобы предотвратить ошибки такого рода, необходимо обеспечить синхронную и синфазную работу передатчика и приемника. Это можно осуществить двумя способами. На верхнем уровне сети вводится высокостабильный главный тактовый генератор, на частоту и фазу которого настраиваются тактовые генераторы всех станций. Известен и другой метод, при котором синхронизация достигается за счет взаимной регулировки тактовых генераторов сети. При этом каждый тактовый генератор устанавливает свою частоту, усредняя фазы тактовых сигналов, поступающих от других генераторов. В этом случае для устранения различий в фазах на входах приемников также необходимы запоминающие устройства.

Таким образом, для точной работы цифровых каналов и сетей необходимо выполнять, во-первых, протокольные методы синхронизации (битовой или цикловой), и, во-вторых, осуществлять чисто физическую синхронизацию взаимодействующих устройств. Для этого на сети необходим очень точный тактовый генератор. Так, главный тактовый генератор имеет атомный эталон частоты, стабильность которого равна  $10^{-11}$  Гц. При такой стабильности ошибки, связанные с синхронностью и синфазностью, встречаются столь редко, что средний коэффициент ошибок остается в допустимых пределах.

### ГЛАВА 3 СТАНДАРТИЗАЦИЯ СЕТЕЙ И СТРУКТУРЫ ПРОТОКОЛОВ

Стандартизация в компьютерных сетях приобретает особое значение. Сети — это соединение разного оборудования, и проблема совместимости является одной из наиболее острых. Без принятия всеми производителями общепринятых правил построения оборудования функционирование сетей было бы невозможным. В компьютерных сетях основой стандартизации является многоуровневый подход (черный ящик) к разработке средств сетевого взаимодействия.

Разбиение на уровни, или уровневая архитектура, является формой функциональной модульности при проектировании информационных сетей. Модуль используется для обозначения как устройства, так и процесса, и выполняет некоторую выделенную функцию. Пользователя интересуют только входы, выходы и функциональная связь между входом и выходом. Модуль используется вместе с другими черными ящиками для построения более сложного модуля, который будет опять рассматриваться на более высоких уровнях как большой черный ящик.

Такой подход к проектированию приводит к иерархии вложенных модулей. Поэтому сложная система должна быть построена как взаимосвязанное множество модулей высокого уровня и, возможно, некоторых простых дополнительных модулей, необходимых для реализации взаимосвязей и выполнения дополнительных простых функций. Каждый модуль следующего более низкого уровня снова разбивается на модули еще более низкого уровня и так далее до самого низкого уровня иерархической цепи.

В простейшем случае черный ящик состоит из двух паритетных процессов (по одному на каждый из двух узлов) и черного ящика, который находится на более низком уровне и представляет систему связи, которая соединяет эти два паритетных процесса. Каждый процесс передает сообщение паритетному процессу в другом узле по нижнему уровню (рис. 3.1).

Процесс передачи информации между двумя паритетными модулями уровня  $n$ , принадлежащими разным узлам, имеет два совершенно различных аспекта. Первый — это уровневые протоколы (правила), с помощью которых паритетные модули обмениваются сообщениями для обеспечения требуемого обслуживания более верхних модулей. Второй — это описание точного интерфейса между модулем уровня  $n$  некоторого узла и модулем уровня  $n-1$  того же узла. Через этот интерфейс происходит фактический обмен указанными сообщениями между уровнем  $n$  и черным ящиком — системой связи более низкого уровня.

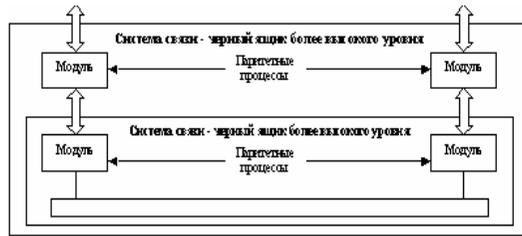


Рис. 3.1. Паритетные процессы в черном ящике, представляющем систему связи

Концепции уровневых (сетевых) протоколов развивались в течение последних 15 лет и были направлены на решение следующих задач:

- обеспечить логическую декомпозицию сложной сети на меньшие, более понятные части (уровни);
- обеспечить стандартные интерфейсы между сетевыми функциями, например стандартные интерфейсы между модулями программного обеспечения;
- обеспечить симметрию в отношении функций, реализуемых в каждом узле сети. Каждый уровень в некотором узле сети выполняет те же функции, какие выполняются аналогичным уровнем в другом узле;
- обеспечить средства предсказания изменений и управления изменениями, которые могут быть внесены в сетевую логику (программное обеспечение или микропрограммы);
- обеспечить простой стандартный язык коммуникации разработчиков сетей, администраторов, фирм-поставщиков и пользователей, используемый при обсуждении сетевых функций.

Формализованные правила, определяющие последовательность и формат сообщений, которыми обмениваются сетевые компоненты, лежащие на одном уровне, но в разных узлах, называется протоколом.

Модули, реализующие протоколы соседних уровней и находящиеся в одном узле, также взаимодействуют друг с другом в соответствии с четко определенными условиями и с помощью стандартизованных форматов сообщений. Эти условия принято называть интерфейсом. Интерфейс определяет набор сервисов, предоставляе-

мый данным уровнем соседнему уровню. Средства каждого уровня должны обрабатывать, во-первых, свой собственный протокол, во-вторых, интерфейсы с соседними уровнями.

Иерархически организованный набор протоколов, достаточный для организации взаимодействия узлов в сети, называется стеком коммуникационных протоколов.

Коммуникационные протоколы могут быть реализованы как программно, так и аппаратно. Протоколы нижних уровней часто реализуются комбинацией программных и аппаратных средств, а протоколы верхних уровней, как правило, только программными средствами.

Протоколы реализуются не только компьютерами, но и другими сетевыми устройствами-концентраторами, мостами, коммутаторами, маршрутизаторами и т.д. В общем случае связь компьютеров в сети осуществляется не на прямую, а через различные коммуникационные средства. В зависимости от типа устройства в нем должны быть встроенные средства, реализующие тот или иной набор протоколов.

#### 3.1. Модель взаимодействия открытых систем OSI

Модель взаимодействия открытых систем OSI сыграла значительную роль в развитии сетей. Модель OSI определяет различные уровни взаимодействия систем, дает им стандартные имена и указывает, какие функции должен выполнять каждый уровень. В модели OSI (рис. 3.2) средства взаимодействия делятся на семь уровней: прикладной, представительный, сеансовый, транспортный, сетевой, канальный и физический. Каждый уровень имеет дело с одним определенным аспектом взаимодействия сетевых устройств.

На прикладном (пользовательском) уровне формируется запрос. Программное сообщение состоит из заголовка и поля данных. Заголовок содержит служебную информацию, которую необходимо передать через сеть прикладному уровню машины-адресата, чтобы сообщить ему, какую работу выполнить. Поле данных сообщения может быть пустым или содержать какие-либо данные.

После формирования сообщения прикладной уровень направляет его вниз по стеку представителю уровню. Протокол представительного уровня на основании информации, полученной из заголовка прикладного уровня, выполняет требуемые действия и добавляет к сообщению собственную служебную информацию — заголовок представительного уровня, в котором содержатся сведения для протокола представительного уровня. Полученное в результате сообщение передается вниз сеансовому уровню, который в свою очередь добавляет свой заголовок и т.д. Наконец, сообщение достигает нижнего, физического уровня, который, собственно, и передает его по линиям связи машине-адресату. К этому времени сообщение «обрастает» заголовками всех уровней (рис. 3.2).

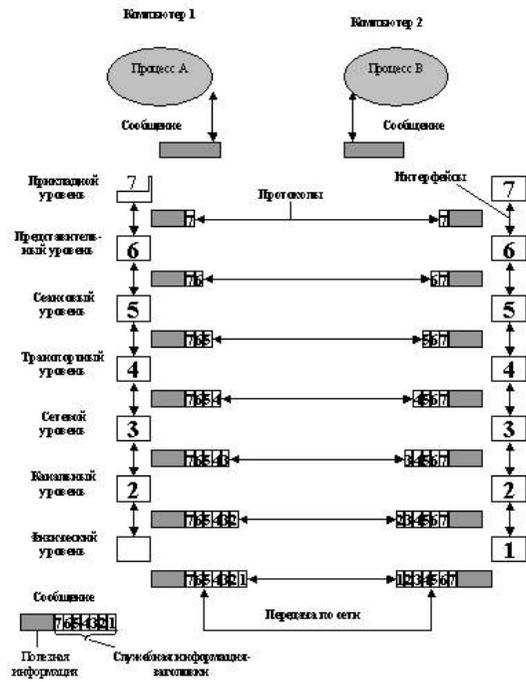


Рис. 3.2. Модель построения OSI/ISO

Когда сообщение по сети поступает на машину-адресат, оно принимается ее физическим уровнем и последовательно перемещается вверх с уровня на уровень. Каждый уровень анализирует и обрабатывает заголовок своего уровня, выполняя соответствующие данному уровню функции, а затем удаляет этот заголовок и передает его вышележащему уровню.

В модели OSI различаются два основных типа протоколов. В протоколах с установлением соединения перед обменом данными отправитель и получатель должны сначала установить соединение, и, возможно, выбрать некоторые параметры протокола, которые они будут использовать при обмене данными. После завершения диалога они должны разорвать соединение. Телефон может служить примером взаимодействия, основанного на установлении соединения.

Вторая группа протоколов — это протоколы предварительного установления соединения. Такие протоколы называются также дейтаграммными протоколами. Отправитель просто передает сообщение, когда оно готово. Опускание письма в почтовый ящик — это пример связи предварительного установления соединения. При взаимодействии компьютеров используются протоколы обоих типов.

### 3.1.1. Физический уровень

Физический уровень имеет дело с передачей битов по физическим линиям связи с такими характеристиками, как полоса пропускания, помехозащищенность, волновое сопротивление и др. На этом же уровне определяются характеристики электрических сигналов, передающих дискретную информацию, например, крутизна фронтов импульсов, уровни напряжения или тока передаваемого сигнала, тип кодирования, скорость передачи сигналов. Кроме этого, здесь стандартизируются типы разъемов и назначение каждого контакта.

Функции физического уровня реализуются во всех устройствах, подключенных к сети (сетевым адаптером или последовательным портом) и заключаются в обеспечении передачи последовательности битов между любой парой узлов. Для выполнения этой функции на каждой стороне канала связи находится модуль физического интерфейса (модем), функция которого состоит в преобразовании входящих битов, поступающих от следующего более высокого уровня (т.е. канального уровня или управление линией передачи данных (УЛПД)), в сигналы, предназначенные для передачи по каналу, и на приемном конце в обратном преобразовании сигналов в биты. Существует большое число таких стандартов, и наиболее известными являются RS-232-C и протокол X21.

### 3.1.2. Канальный уровень

Поэтому одной из задач канального уровня является проверка доступности среды передачи. Другой задачей канального уровня является реализация механизмов обнаружения и коррекции ошибок. Для этого на канальном уровне биты группируются в наборы, называемые кадрами. Канальный уровень обеспечивает корректность передачи каждого кадра, помещая специальную последовательность бит в начало и конец каждого кадра для его выделения, а также вычисляет контрольную сумму, обрабатывая все байты кадра определенным способом и добавляя определенную сумму к кадру. Когда кадр приходит по сети, получатель снова вычисляет контрольную сумму полученных данных и сравнивает с контрольной суммой из кадра. Если они совпадают, кадр считается правильным и принимается, иначе фиксируется ошибка. Канальный уровень может не только обнаруживать ошибки, но и исправлять их за счет повторной передачи поврежденных кадров. Функция исправления ошибок не является обязательной для канального уровня, поэтому в некоторых протоколах этого уровня она отсутствует.

В протоколах канального уровня, используемых в локальных сетях, заложена определенная структура связей между компьютерами и способы их адресации. Хотя канальный уровень и обеспечивает доставку кадра между любыми двумя узлами локальной сети, он это только делает в сети совершенно определенной топологией связей, именно той топологией, для которой он был разработан. К таким типовым топологиям, поддерживаемыми протоколами канального уровня локальных сетей, относятся общая шина, кольцо и звезда, а также структуры, полученные из них при помощи мостов и коммутаторов.

На канальном уровне каждая линия связи имеет на каждом своем конце модули управления линией передачи данных (паритетные процессы). Цель УЛПД — превратить ненадежный битовый тракт уровня 1 в виртуальную линию связи более высокого уровня, способную в обоих направлениях передавать пакеты асинхронно, но безошибочно.

По существу, передающий модуль УЛПД помещает некоторое количество управляющих битов в начале и конце каждого пакета, в результате чего получается более длинная последовательность битов, называемая кадром. Некоторые из этих управляющих битов обнаруживают возникновение ошибок в переданных кадрах, некоторые запрашивают повторные передачи, если возникли ошибки, а некоторые обозначают начало и конец кадра. Протоколы, выполняющие эти задачи, распределены между паритетными модулями УЛПД, находящимися на обоих концах линии связи, и довольно сложны, т.к. сами управляющие биты подвержены ошибкам передачи.

### 3.1.3. Сетевой уровень

Сетевой уровень служит для образования единой транспортной системы, объединяющей несколько сетей, причем эти сети могут использовать совершенно различные принципы передачи сообщений между конечными узлами и обладать произвольной структурой связей.

Внутри сети доставка данных обеспечивается соответствующим канальным уровнем, а вот доставкой данных между сетями занимается сетевой уровень, который и поддерживает возможность правильного выбора маршрута передачи сообщения даже в том случае, когда структура связей между составляющими сетями имеет характер, отличный от принятого в протоколах канального уровня.

Сети соединяются между собой специальными устройствами, называемыми маршрутизаторами. Чтобы передать сообщение от отправителя, находящегося в одной сети, получателю, находящемуся в другой сети, нужно совершить некоторое количество транзитных передач между сетями, каждый раз выбирая подходящий маршрут. Таким образом, маршрут представляет собой последовательность маршрутизаторов, через которые проходит пакет. Проблема выбора наилучшего пути называется маршрутизацией, и ее решение является одной из главных задач сетевого уровня.

Сообщения сетевого уровня принято называть пакетами. При организации доставки пакетов на сетевом уровне используется понятие «номер сети». В этом случае адрес получателя состоит из старшей части — номера сети и младшей — номера узла в этой сети. Все узлы одной и той же сети должны иметь одну и ту же старшую часть адреса.

На сетевом уровне определяются два вида протоколов. Первый вид — сетевые протоколы управляют движением пакетов через сеть. Второй вид протоколов — протоколы маршрутизации. С помощью этих протоколов маршрутизаторы собирают информацию о топологии межсетевых соединений. Протоколы сетевого уровня реализуются программными модулями операционной системы, а также программными и аппаратными средствами маршрутизаторов.

Паритетные процессы сетевого уровня должны обмениваться информацией, чтобы производить маршрутизацию и управление потоком. Часть этого обмена происходит через управляющие биты, которые добавляются к пакетам данных, перемещающимся от узла к узлу. Эти управляющие биты указывают источник пакета и пункт назначения, а также помогают управлять потоком пакетов определенного сеанса. Другая часть этого обмена происходит через пакеты, которые содержат только управляющие биты. Эти пакеты устанавливают новые сеансы и передают информацию, необходимую для образования маршрутных таблиц.

Когда сетевой уровень и все более низкие уровни во всех узлах и пунктах рассматриваются как один черный ящик, пакет, поступающий на сетевой уровень со следующего более высокого уровня в некотором пункте, через некоторое время появляется в интерфейсе сетевого уровня со следующим более высоким уровнем в пункте назначения. В зависимости от конструкции сетевого уровня эта виртуальная линия может быть надежной, доставляющей каждый пакет безошибочно один и только один раз, или ненадежной, не доставляющей некоторые пакеты или доставляющей их с ошибками. На более высоких уровнях в последнем случае эти ошибки должны исправляться. Сетевой уровень также может обеспечивать доставку всех пакетов каждого сеанса в порядке их следования или беспорядочно.

### **3.1.4. Транспортный уровень**

На пути от отправителя к получателю пакеты могут быть искажены или утеряны. Транспортный уровень обеспечивает приложениям или верхним уровням стека — прикладному и сеансовому — передачу данных с той степенью надежности, которая им требуется.

На транспортном уровне выполняется ряд функций. Во-первых, сообщение разбивается на пакеты на передающем конце, а на приемном конце пакеты собираются в сообщение. Эта функция сборки относительно проста, если процесс транспортного уровня имеет в распоряжении достаточное буферное пространство, но может быть довольно сложной, если буферное пространство ограничено и должно совместно использоваться многими виртуальными сквозными линиями. Если сетевой уровень нарушает порядок доставляемых пакетов, то проблема сборки становится еще более трудной.

Во-вторых, на транспортном уровне могут мультиплексироваться несколько низкоскоростных сеансов, имеющих один и тот же источник и пункт назначения, в один сеанс сетевого уровня. Поскольку подсеть связи в этом случае обслуживает только один сеанс, количество сеансов в подсети и соответствующая управляющая информация уменьшаются. До некоторой степени аналогичным образом на транспортном уровне один высокоскоростной канал может расщепляться на несколько сеансов сетевого уровня.

В-третьих, если на сетевом уровне возникают ошибки, на транспортный уровень может возлагаться функция обеспечения надежной сквозной связи для тех сеансов, которым это необходимо. Даже когда сетевой уровень проектируется так, чтобы обеспечить надежную связь, транспортный уровень должен принимать в этом участие в том случае, когда тот или иной конечный пункт выходит из строя или когда сеть становится разъединенной из-за повреждений линий связи.

Наконец, сети передачи данных часто соединяются, при этом коммуникационные пути проходят по нескольким подсетям (это известно как межсетевое соединение). Обычно сети соединяются посредством специальных узлов, называемых шлюзами. Соединяемые сети часто имеют несовместимые сетевые уровни и поэтому требуется, чтобы на транспортный уровень в шлюзе поступали пакеты от сетевого уровня одной сети и им придавалась такая форма, которая принята в другой сети. Если сети имеют различные максимальные размеры пакетов, то на транспортном уровне должны иногда разбиваться длинные пакеты на два или большее число пакетов меньшего размера.

Модель OSI определяет пять классов сервиса, предоставляемых транспортным уровнем. Эти виды сервиса отличаются качеством предоставляемых услуг: срочностью, возможностью восстановления прерванной связи, наличием средств мультиплексирования нескольких соединений между различными прикладными протоколами через общий транспортный протокол, и главное — способностью к обнаружению и исправлению ошибок передачи, таких как искажение, потеря и дублирование пакетов.

Выбор класса сервиса транспортного уровня определяется, с одной стороны, тем, в какой степени задача обеспечения надежности решается самими приложениями и протоколами более высоких уровней, чем транспортный, уровень, а с другой стороны, этот выбор зависит от того, насколько надежной является система транспортировки данных в сети, обеспечиваемая уровнями, расположенных ниже транспортного.

Все протоколы, начиная с транспортного уровня и выше, реализуются программными средствами конечных узлов в сети — компонентами их сетевых операционных систем. Протоколы нижних четырех уровней обобщенно называют сетевым транспортом или транспортной подсистемой, так как они полностью решают задачу транспортировки сообщений с заданным уровнем качества в составных сетях с произвольной топологией и различными технологиями.

### **3.1.5. Сеансовый уровень**

Сеансовый уровень обеспечивает управление диалогом: фиксирует, какая из сторон является активной в настоящей момент, предоставляет средства синхронизации. Последние позволяют вставлять контрольные точки в длинные передачи, чтобы в случае отказа можно было вернуться назад к последней контрольной точке, а не начинать все с начала. На практике немногие приложения используют сеансовый уровень, и он редко реализуется в виде отдельных протоколов, хотя функции этого уровня часто объединяют с функциями прикладного уровня и реализуют в одном протоколе.

Одна из функций сеансового уровня подобна справочной службе телефонных сетей (если пользователь хочет воспользоваться предоставляемым сетью видом обслуживания, но не знает, куда надо обратиться, чтобы

получить к нему доступ, то с этого уровня на транспортный уровень передается информация, необходимая для установления сеанса).

Сеансовый уровень также связан с правами доступа при иницировании сеансов. По существу, на сеансовом уровне осуществляется управление взаимодействием между двумя конечными точками при установлении сеанса, тогда как на сетевом уровне производится управление теми аспектами установления сеанса, которые связаны с подсетью связи.

### **3.1.6. Представительный уровень**

Представительный уровень имеет дело с формой представления передаваемой по сети информации, не меняя при этом ее содержания. За счет уровня представления информация, передаваемая прикладным уровнем одной системы, всегда понятна прикладному уровню другой системы. С помощью средств данного уровня протоколы прикладных уровней могут преодолеть синтаксические различия в представлении данных или же различия в кодах символов, например ASCII и EBCDIC.

Главными функциями уровня представления являются шифрование данных, их сжатие и кодовое преобразование. Например, шифрование для военных организаций. Сети передачи данных должны проектироваться так, чтобы предотвратить попадание сообщений к ошибочным получателям, однако возможны случайные сбои в работе как внешних пунктов, так и подсети связи. Это приводит к необходимости шифрования важных сообщений.

### **3.1.7. Прикладной уровень**

Прикладной уровень представляет набор разнообразных протоколов, с помощью которых пользователи сети получают доступ к разделенным ресурсам: файлам, принтерам или гипертекстовым WEB-страницам, электронной почте. Существует большое разнообразие служб прикладного уровня. Например, NCP в операционной системе Novell Net Ware, SMB в Microsoft Windows NT, NFS, FTP и TFTP, входящие в стек TCP/IP.

Для каждого приложения требуется свое собственное программное обеспечение (т.е. свои паритетные процессы). На более низких уровнях выполняются те части общей задачи, которые требуются для многих различных приложений, а на прикладном уровне выполняется та часть работы, которая специфична для конкретного приложения.

### **3.1.8. Сетезависимые и сетезависимые уровни**

Функции всех уровней модели OSI могут быть отнесены к одной из двух групп: либо к функциям, зависящим от конкретной технической реализации сети, либо к функциям, ориентированным на работу с приложением.

Три нижних уровня — физический, каналный и сетевой — являются сетезависимыми, т.е. протоколы этих уровней тесно связаны с технической реализацией сети и используемым коммуникационным оборудованием.

Три верхних уровня — прикладной, представительный и сеансовый — ориентированы на приложения и мало зависят от технических особенностей построения сети. На протоколы этих уровней не влияют какие бы то ни было изменения в топологии сети, замена оборудования или переход на другую сетевую технологию.

Транспортный уровень является промежуточным, он скрывает все детали функционирования нижних уровней от верхних. Это позволяет разрабатывать приложения, не зависящие от технических средств непосредственной транспортировки сообщений.

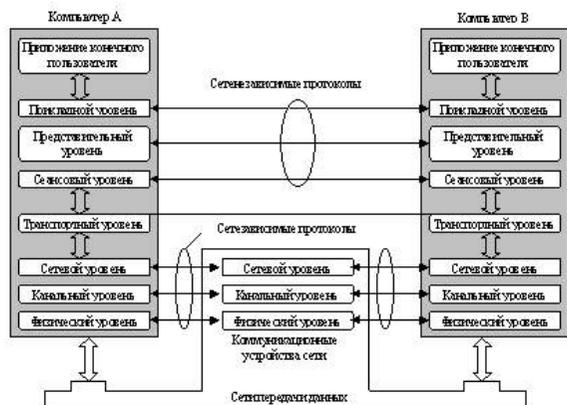


Рис. 3.3. Сетезависимые и сетезависимые уровни модели OSI

На рис. 3.3 показаны уровни модели OSI, на которых работают различные элементы сети. Компьютер с установленной на нем сетевой операционной системой (ОС) взаимодействуют с другим компьютером с помощью протоколов всех семи уровней. Это взаимодействие компьютеры осуществляют через различные коммуникационные устройства: модемы, концентраторы, мосты, коммутаторы, маршрутизаторы, мультиплексоры. В зависимости от типа коммуникационного устройства может работать либо только на физическом уровне (повторитель), либо на физическом и канальном (мост), либо на физическом, канальном и сетевом, иногда захватывая и транспортный уровень (маршрутизатор). На рис. 3.4 показано соответствие функций различных коммуникационных устройств уровням модели OSI.

Модель OSI представляет одну из многих моделей коммуникаций. Эти модели и связанные с ними стеки протоколов могут отличаться количеством уровней, их функциями, форматами сообщений, службами, поддерживаемыми на верхних уровнях, и прочими параметрами.

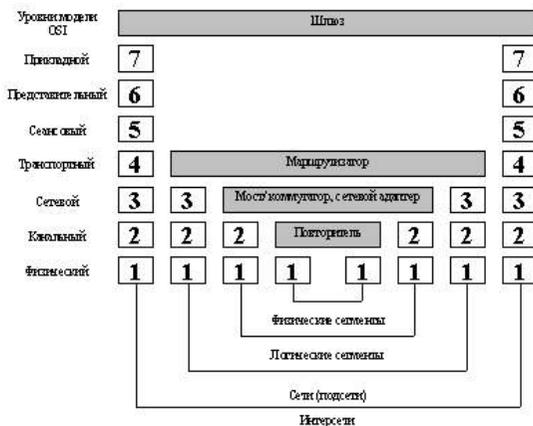


Рис. 3.4. Соответствие функций различных устройств сети уровням модели OSI

С одной стороны, имеется большая потребность в стандартизации интерфейсов и функции каждого уровня, даже если стандарт является в чем-то неподходящим. Эта потребность особенно велика для международных сетей и для производителей оборудования, которое должно правильно работать в сочетании с оборудованием других производителей. С другой стороны, стандартизация препятствует нововведениям и это особенно чувствительно в такой новой области, как сети передачи данных, которые еще не до конца поняты.

Один конкретный недостаток, связанный с семью уровнями, состоит в том, что каждое сообщение должно пройти через семь процессов только для того, чтобы войти в подсеть связи, и все это может привести к значительной задержке.

### 3.2. Понятие «открытая система»

В широком смысле открытой системой может быть названа любая система (компьютер, вычислительная сеть, ОС, программный пакет, другие аппаратные и программные продукты), которая построена в соответствии с открытыми спецификациями.

Под открытыми спецификациями понимается опубликованные, общедоступные спецификации, соответствующие стандартам и принятые в результате достижения согласия после всестороннего обсуждения всеми заинтересованными сторонами.

Использование при разработке систем открытых спецификаций позволяет разрабатывать для этих систем различные аппаратные или программные средства расширения и модификации, а также создавать программно-аппаратные комплексы из продуктов разных производителей.

Модель OSI касается открытости средств взаимодействия устройств, связанных в вычислительную сеть. Здесь под открытой системой понимается сетевое устройство, готовое взаимодействовать с другими сетевыми устройствами с использованием стандартных правил, определяющих формат, содержание и значение принимаемых и отправляемых сообщений.

Если две сети построены с соблюдением принципов открытости, то это дает следующие преимущества:

- возможность построения сети из аппаратных и программных средств различных производителей, придерживающихся одного и того же стандарта;
- возможность безболезненной замены отдельных компонентов сети другими, более совершенными, что позволяет сети развиваться с минимальными затратами;
- возможность легкого сопряжения одной сети с другой;
- простота освоения и обслуживания сети.

Структурная часть открытой системы, обеспечивающая обработку информации для обслуживания пользователя, называется прикладным процессом. Однако нельзя считать, что открытая система всегда имеет прикладные процессы. Последние отсутствуют, например, в открытой системе, предназначенной только для передачи данных.

### 3.3. Источники стандартов

Работы по стандартизации вычислительных сетей ведутся большим количеством организаций. В зависимости от статуса организаций различают следующие виды стандартов:

- Стандарты отдельных фирм (например, стек протоколов DECnet фирмы Digital Equipment или графический интерфейс OPEN LOOK для UNIX-систем фирмы Sun);
- Стандарты специальных комитетов и объединений, создаваемых несколькими фирмами, например, стандарты технологии ATM, разрабатываемые специально созданным объединением ATM Forum, насчитывающем около 100 коллективных участников, или стандарты союза Fast Ethernet Alliance по разработке стандартов 100 Мбит Ethernet;
- Национальные стандарты, например, стандарт FDDI, представляющий один из многочисленных стандартов, разработанных американским национальным институтом стандартов (ANSI), или стандарты безопасности информационных систем, разработанные Национальным центром компьютерной безопасности (NCSC) Министерства обороны США;
- Международные стандарты, например, модель и стек коммуникационных протоколов Международной организации по стандартам (ISO), многочисленные стандарты Международного союза электросвязи (ITU), в том числе стандарты на сети с коммутацией пакетов X.25, сети frame relay, ISDN, модемы и многие другие.

Более того, в виду широкого распространения некоторые фирменные стандарты становятся основой для национальных и международных стандартов. Стандарт Ethernet, первоначально разработанный компаниями Digital Equipment, Intel и Xerox, через некоторое время и в несколько измененном виде был принят как национальный стандарт IEEE 802.3, а затем организация ISO утвердила его в качестве международного стандарта ISO 8802.3.

### 3.4. Стандартные стеки коммуникационных протоколов

Важнейшим направлением стандартизации в области информационных сетей является стандартизация коммуникационных протоколов. В настоящее время в сетях используется большое количество стеков коммуникационных протоколов. Наиболее популярными являются стеки: TCP/IP, IPX/SPX, NetBios/SMB, DECnet, SNA и OSI. Все эти стеки, кроме SNA на нижних уровнях — физическом и канальном — используют одни и те же хорошо стандартизированные протоколы: Ethernet, Token Ring и FDDI и некоторые другие, которые позволяют использовать во всех сетях одну и ту же аппаратуру. На верхних уровнях все стеки работают по своим собственным протоколам. Эти протоколы часто не соответствуют рекомендуемому модели OSI разбиению на

уровни. Такое несоответствие связано с тем, что модель OSI появилась как результат обобщения уже существующих и реально используемых стеков, а не наоборот.

#### 3.4.1. Стек OSI

Существует различие между моделью OSI и стеком OSI. Модель OSI является концептуальной схемой взаимодействия открытых систем, а стек OSI представляет собой набор вполне конкретных спецификаций протоколов. В отличие от других стеков протоколов стек OSI полностью соответствует модели OSI, включая спецификации протоколов для всех семи уровней взаимодействия, определенных в этой модели. На нижних уровнях стек OSI поддерживает Ethernet, Token Ring, FDDI, протоколы глобальных сетей, X.25 и ISDN, то есть использует разработанные вне стека протоколы нижних уровней, как и все другие стеки. Протоколы сетевого, транспортного и сеансового уровней стека OSI специфицированы и реализованы различными производителями, но распространены пока мало. Наиболее популярными протоколами стека OSI являются прикладные протоколы. К ним относятся: протокол передачи файлов FTAM, протокол эмуляции терминала VTP, протоколы справочной службы X.500, электронной почты X.400 и ряд других.

Из-за своей сложности протоколы OSI требуют больших затрат вычислительной мощности центрального процессора, что делает их наиболее подходящими для мощных машин, а не для сетей персональных компьютеров.

Стек OSI — международный, независимый от производителей стандарт. Его поддерживает правительство США в своей программе GOSIP, в соответствии с которой все компьютерные сети, устанавливаемые в правительственных учреждениях США после 1990 года, должны или непосредственно поддерживать стек OSI, или обеспечивать средства для перехода на этот стек в будущем. Тем не менее стек OSI более популярен в Европе, чем в США.

#### 3.4.2. Стек TCP/IP

Стек TCP/IP был разработан для связи экспериментальной сети ARPAnet с другими сетями как набор общих протоколов для разнородной вычислительной среды. Популярность операционной системы UNIX привела к широкому распространению протоколов TCP, IP и других протоколов стека. Сегодня этот стек используют для связи компьютеров всемирной сети Internet, а также в огромном числе корпоративных сетей.

Стек TCP/IP на нижнем уровне поддерживает все популярные стандарты физического и канального уровней: для локальных сетей это Ethernet, Token Ring, FDDI, для глобальных — протоколы работы на аналоговых коммутируемых и выделенных линиях SLIP, PPP, протоколы территориальных сетей X.25 и ISDN.

Основными протоколами стека являются IP и TCP. Эти протоколы в терминологии модели OSI относятся к сетевому и транспортному уровням соответственно. IP обеспечивает продвижение пакета по составной сети, а TCP гарантирует надежность его доставки.

За долгие годы использования в сетях различных стран и организаций стек TCP/IP вобрал в себя большое количество протоколов прикладного уровня. К ним относятся такие популярные протоколы, как протокол пересылки файлов FTP, протокол эмуляции терминала telnet, гипертекстовые сервисы службы WWW, почтовый протокол SMTP, используемый в электронной почте сети Internet и многие другие.

Существует большое количество локальных, корпоративных и территориальных сетей, непосредственно не являющихся частями Internet, в которых также используют протоколы TCP/IP. Эти сети называют сетями TCP/IP или просто IP-сетями.

Поскольку стек TCP/IP изначально создавался для глобальной сети Internet, он имеет много особенностей, дающих ему преимущество перед другими протоколами, когда речь заходит о построении сетей, включающих глобальные связи. В частности, очень полезным свойством, делающим возможным применение этого протокола в больших сетях, является его способность фрагментировать пакеты. Действительно, большая составная сеть часто состоит из сетей, построенных на совершенно разных принципах. В каждой из этих сетей может быть установлена собственная величина максимальной длины единицы передаваемых данных (кадра). В таком случае при переходе из одной сети, имеющей большую максимальную длину, в сеть с меньшей максимальной длиной может возникнуть необходимость деления передаваемого кадра на несколько частей. Протокол IP стека TCP/IP эффективно решает эту задачу.

Другой особенностью технологии TCP/IP является гибкая система адресации, позволяющая более просто по сравнению с другими протоколами аналогичного назначения включать в интерес сети других технологий. Это свойство также способствует применению стека TCP/IP для построения больших гетерогенных сетей.

В стеке TCP/IP очень экономно используются возможности широкоэвентельных рассылок. Это свойство совершенно необходимо при работе на медленных каналах связи, характерных для территориальных сетей.

Однако все это осуществляется за счет высоких требований к ресурсам и сложности администрирования IP-сетей. Мощные функциональные возможности протоколов стека TCP/IP требуют для своей реализации высоких вычислительных затрат. Гибкая система адресации и отказ от широкоэвентельных рассылок приводят к наличию в IP-сети различных централизованных служб типа DNS, DHCP и т.п. Каждая из этих служб направлена на облегчение администрирования сети, в том числе и на облегчение конфигурирования оборудования, но в то же время сама требует пристального внимания со стороны администраторов.

Опишем подробнее протокол RTP, который также относится к стеку протоколов TCP/IP.

RTP (Real-Time Transport Protocol) базируется на идеях, предложенных Кларком и Тенненхаузом, и гарантирует доставку данных одному или более адресатам с задержкой в заданных пределах. Это означает, что данные могут быть воспроизведены в реальном времени. При этом определяется тип поля данных, производится нумерация посылок, присвоение временных меток и мониторинг доставки. Приложению обычно используется RTP поверх протокола UDP для того, чтобы использовать его возможности мультиплексирования и контрольного суммирования. Но RTP может использоваться и поверх любой другой сетевой транспортной среды. RTP поддерживает обновленную доставку по многим адресам, если мультикастинг поддерживается нижележащим сетевым уровнем.

Вчерашние методы работы с большими объемами трафика совершенно непригодны для современных систем. Удовлетворить растущим требованиям к передаче данных в связи с ростом их объема, распространением приложений реального времени и многоадресной рассылки без новых инструментов невозможно. RTP и RSVP (Resource Reservation Protocol) обеспечивают надежный фундамент для сетей следующего поколения.

Данное решение обещает решить проблему передачи чувствительных к задержкам данных по Internet.

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 воспроизведены с правильными интервалами 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 время от времени одновременно «говорят» несколько источников.

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

Более простое устройство создает 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. Транслятор конвертирует видео в формат более низкого качества, требующий не такой высокой скорости передачи данных.

RTP не поддерживает каких-либо механизмов доставки пакетов, обеспечения достоверности передачи или надежности соединения. Эти все функции возлагаются на транспортный протокол. RTP работает поверх UDP и может поддерживать передачу данных в реальном времени между несколькими участниками RTP-сеанса. Для каждого участника RTP сеанс определяется парой транспортных адресов назначения пакетов (один сетевой адрес — IP и пара портов: RTP и RTCP).

Пакеты RTP содержат следующие поля: идентификатор отправителя, указывающий, кто из участников генерирует данные, отметки о времени генерирования пакета, чтобы данные могли быть воспроизведены принимающей стороной с правильными интервалами, информация о порядке передачи, а также информация о характере содержимого пакета, например, о типе кодировки видеоданных (MPEG, Indeo и др.). Наличие такой информации позволяет оценить величину начальной задержки и объема буфера передачи.

В типичной среде реального времени отправитель генерирует пакеты с постоянной скоростью. Они отправляются через одинаковые интервалы времени, проходят через сеть и принимаются получателем, воспроизводящим данные в реальном времени по их получению. Однако ввиду изменения времени задержки при передаче пакетов по сети, они могут прибывать через нерегулярные интервалы времени. Для компенсации этого эффекта поступающие пакеты буферизуются, придерживаются на некоторое время и затем предоставляются с постоянной скоростью программному обеспечению, генерирующему вывод. Поэтому для функционирования протокола реального времени необходимо, чтобы каждый пакет содержал временную метку — таким образом получатель может воспроизвести поступающие данные с той же скоростью, что и отправитель.

Поскольку RTP определяет (и регулирует) формат полезной нагрузки передаваемых данных, с этим напрямую связана концепция синхронизации, за которую частично отвечает механизм трансляции RTP — микшер. Принимая потоки пакетов RTP от одного или более источников, микшер, комбинирует их и посылает новый поток пакетов RTP одному или более получателям. Микшер может просто комбинировать данные, а также изменять их формат, например, при комбинировании нескольких источников звука. Предположим, что новая система хочет принять участие в сеансе, но ее канал до сети не имеет достаточной емкости для поддержки всех

потоков RTP, тогда микшер получает все эти потоки, объединяет их в один и передает последний новому члену сеанса. При получении нескольких потоков микшер просто складывает значения импульсно-кодовой модуляции. Заголовок RTP, генерируемый микшером, включает идентификатор отправителя, чьи данные присутствуют в пакете.

На практике протокол RTP не отделим от протокола RTCP (RTP control protocol). Последний служит для мониторинга QoS и для передачи информации об участниках обмена в ходе сессии. RTP гибкий протокол, который может доставить приложению нужную информацию, его функциональные модули не образуют отдельный слой, а чаще встраиваются в прикладную программу. Протокол RTP не является жестко регламентированным. При организации аудио-конференции каждый участник должен иметь адрес и два порта, один для звуковых данных, другой для управляющих RTCP-пакетов. Эти параметры должны быть известны всем участникам конференции. При необходимости соблюдения конфиденциальности информация и пакеты управления могут быть зашифрованы. При аудио конференциях каждый из участников пересылает небольшие закодированные звуковые фрагменты длительностью порядка 20 мсек. Каждый из таких фрагментов помещается в поле данных RTP-пакета, который в свою очередь вкладывается в UDP-дейтограмму. Заголовок пакета RTP определяет, какой вид кодирования звука применен (PCM, ADPCM или LPC), что позволяет отправителю при необходимости сменить метод кодирования, если к конференции подключился новый потребитель с определенными ограничениями или сеть требует снижения скорости передачи.

При передаче звука весьма важным становится взаимное положение закодированных фрагментов во времени. Для решения задачи корректного воспроизведения заголовки пакетов RTP содержат временную информацию и порядковые номера. Порядковые номера позволяют не только восстановить правильный порядок фрагментов, но и определить число потерянных пакетов-фрагментов. Так как участники конференции могут появляться и исчезать по своему усмотрению, полезно знать, кто из них присутствует в сети в данный момент, и как до них доходят передаваемые данные. Для этой цели периодически каждый из участников транслирует через порт RTCP мультикастинг - сообщение, содержащее имя участника и диагностические данные. Узел участника конференции шлет пакет BUY (RTCP), если он покидает сессию.

Если в ходе конференции передается не только звук, но и изображение, они передаются как два независимых потока с использованием двух пар UDP-портов. RTCP-пакеты посылаются независимо для каждой из этих двух сессий. На уровне RTP не существует какой-либо взаимосвязи между аудио- и видеосессиями. Только RTCP-пакеты несут в себе одни и те же канонические имена участников.

В некоторых случаях можно столкнуться с ситуацией, когда один из участников конференции подключен к сети через узкополосный канал. Было бы не слишком хорошо требовать от всех участников перехода на кодировку, соответствующую этой малой полосе. Для того чтобы этого избежать, можно установить преобразователь, называемый смесителем, в непосредственной близости от узкополосной области. Смеситель преобразует поток аудио-пакетов в последовательность пакетов, которая соответствует возможностям узкополосного канала. Эти пакеты могут быть уникальными (адресованными одному получателю) или мультикастными.

Заголовок RTP включает в себя средства, которые позволяют мультиплексорам идентифицировать источники, внесшие вклад. Так что получатель может правильно идентифицировать источник звукового сигнала.

Некоторые участники конференции, использующие широкополосные каналы, не доступны для IP-мультикастинга. Для таких узлов смесители не нужны, здесь используется другой RTP-уровень передачи, называемый трансляцией. Устанавливается два транслятора по одному с каждой из сторон. Внешний транслятор передает мультикастинг-пакеты по безопасному каналу внутреннему транслятору. Внутренний же транслятор рассылает их подписчикам локальной сети обычным образом.

### 3.4.3. Стек IPX/SPX

Этот стек разработан для сетевой операционной системы NetWare. Протоколы сетевого и сеансового уровней Internetwork Packet Exchange (IPX) и Sequenced Packet Exchange (SPX) являются прямой адаптацией и протоколов XNS фирмы XEROX. Стек IPX/SPX непосредственно связан с операционной системой Novell NetWare, которая широко используется.

Стек IPX/SPX предназначен для работы в локальных сетях небольших размеров, состоящих из персональных компьютеров с небольшими ресурсами. Следовательно, на реализацию протоколов IPX/SPX требовалось минимальное количество оперативной памяти (ограниченной в IBM совместимых компьютерах под управлением MS-DOS объемом 640 кб и быстро работающей на процессорах большой вычислительной мощности). В результате протоколы стека IPX/SPX до недавнего времени хорошо работали в локальных сетях, но не очень хорошо в больших корпоративных сетях, т.к. слишком перегружали медленные глобальные связи широкополосными пакетами, которые интенсивно используются несколькими протоколами этого стека. Это обстоятельство ограничивало распространенность его только сетями NetWare.

Сейчас стек IPX/SPX реализован не только в NetWare, но и в нескольких других популярных сетевых ОС, например SCO UNIX, Sun Solaris, Microsoft Windows NT.

### 3.4.4. Стек NetBios/SMB

На физическом и канальном уровнях этого стека используются все наиболее распространенные протоколы: Ethernet, Token Ring, FDDI и другие. На верхних уровнях работают протоколы NetBEUI и SMB.

Протокол NetBios (Network Basic Input/output System) появился в 1984 году как сетевое расширение стандартных функций базовой системы ввода-вывода (BIOS), IBM PC для сетевой программы PCNetwork фирмы IBM. В дальнейшем этот протокол был заменен так называемым протоколом расширенного пользовательского интерфейса NetBEUI (NetBIOS Extended User Interface). Для обеспечения совместимости приложений в качестве интерфейса к протоколу NetBEUI был сохранен интерфейс NetBIOS. Протокол NetBEUI разрабатывался как эффективный протокол, потребляющий немного ресурсов и предназначенный для сетей, насчитывающих не более 200 рабочих станций. Этот протокол содержит много полезных сетевых функций, которые можно отнести к сетевому, транспортному и сеансовому уровням модели OSI, однако с его помощью невозможна маршрутизация пакетов. Это ограничивает применение протокола NetBEUI локальными сетями, не разделенными на подсети, и делает невозможным его использование в составных сетях. Некоторые ограничения NetBEUI снимаются реализацией этого протокола NBF (NetBEUI Frame), которая включена в операционную систему Microsoft Windows NT.

Протокол SMB (Server Message Block) выполняет функции сеансового, представительного и прикладного уровней. На основе SMB реализуется файловая служба, а также службы печати и передачи сообщений между приложениями.

Стеки SNA фирмы IBM, DECnet корпорации Digital Equipment и AppleTalk/AFP фирмы Apple применяются в основном в операционных системах и сетевом оборудовании этих фирм.

Модель OSI	IBM/Microsoft	TCP/IP	Novell	Стек OSI
Прикладной		Telnet, FTP, WWW, SNMP, SMTP		X.400, X.500, FTAM
Представительный	SMB		RPC, SAP	Представительный протокол OSI
Сеансовый		TCP		Сеансовый протокол OSI
Транспортный	NetBios		SPX	Транспортный протокол OSI
Сетевой		IP, RIP, OSPF	IPX, RIP, NLSP	EE-ES, IS-IS
Канальный	802.3 (Ethernet), 802.5 (Token Ring), FDDI, Fast Ethernet, SLIP, 100VG AnyLAN, VLS ATM, T-ABR, T-AD, D-VBR			
Физический	Консоль, экран, кабель и неэкранированная витая пара, оптоволокно, телефонный кабель			

Рис. 3.5. Соответствие популярных стеков протоколов модели OSI

На рис. 3.5 показано соответствие наиболее популярных протоколов уровням модели OSI. Стек OSI разбит на семь уровней. Обычно в нем выделяются три-четыре уровня: уровень сетевых адаптеров, в котором реализуются протоколы физического и канального уровней, сетевой уровень, транспортный уровень и уровень служб, вбирающий в себя функции сеансового, представительного и прикладного уровней. Поэтому модель взаимодействия открытых систем является эталонной.

## ГЛАВА 4 ЛОКАЛЬНЫЕ ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ

Локальные сети передачи данных (LAN) служат для объединения компьютеров, территориально расположенных либо в одном здании, либо в близко расположенных зданиях. В локальной сети из-за коротких расстояний, скорость передачи очень высокая. Вся процедура передачи концентрируется на первом и втором уровнях модели OSI/ISO, отвечающих за работу сети. Поэтому протоколы верхних уровней в большинстве случаев одни и те же как для локальных, так и для глобальных сетей. В локальных сетях топология проста и не зависит от интенсивности передаваемой нагрузки. Наиболее распространенными являются звезда, кольцо и шина.

Для передачи данных используется топология шина и построенные по шинной топологии, целый сети шин (рис. 4.1) и конструкция представляет собой Схематично шину можно кабель, проходящий через все компьютеры подключены к нему подключения к шине существует таким образом, представляет собой

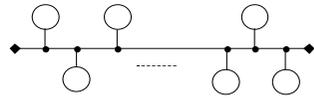


Рис. 4.1. Пример топологии «шина»

общую для всех компьютеров среду передачи, которую нужно уметь делить между всеми рабочими станциями. При кольцевой топологии (рис. 4.2) все рабочие станции оказываются соединенными последовательно. Для управления доступом к общей среде передачи нужны определенные механизмы.

Для работы в сети компьютеру необходима сетевая плата, реализующая конкретный протокол сети. Протоколы у каждой технологии разные, но общими являются адреса отправителя и получателя, находящиеся в заголовке. Этот адрес называется MAC-адресом (Medium Access Control), управляющий доступом к среде передачи.

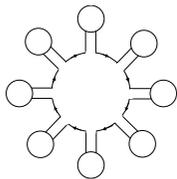


Рис. 4.2. Пример кольцевой топологии

MAC-адрес любой сетевой платы или любого порта локальной сети уникален. Его записывают на фирме и каждому предприятию выделяют свой диапазон MAC адресов, в рамках которого они и работают. Длина MAC-адреса представляется шестью байтами. Этот адрес нужен устройствам для нахождения требуемого терминала. Основными видами физической среды передачи для локальных сетей являются витая пара, коаксиальный кабель и оптоволокно, причем коаксиальный кабель в последнее время используется все реже. Главное преимущество витой пары и коаксиального кабеля перед оптическим кабелем является простота подключения к нему. По этой причине оптоволокно используют в основном для кольцевых схем.

Преимущества оптического кабеля для локальных сетей составляет защищенность от электромагнитных воздействий и от несанкционированного подключения, а также способность передавать данные с очень большой скоростью на большие расстояния. Наибольшая дальность у оптоволокна составляет несколько километров. Коаксиальный кабель имеет дальность порядка 300 метров, а витая пара — 180 метров. И тем не менее, коаксиальный кабель применяют реже, чем витую пару из-за неудобств, связанных с его прокладкой и подключением. Оптический кабель, помимо больших трудностей с организацией шинной топологии, еще и достаточно дорог. Поэтому для случаев, когда не требуется очень высокие скорости и не требуется охватить много помещений, наиболее выгодной оказывается витая пара.

Немного подробнее о типах кабелей с витой парой внутри. Различаются они по так называемым категориям. Наиболее распространены кабели третьей и пятой категории. Первый — это неэкранированный кабель с двумя витыми парами внутри. Второй — это экранированный кабель также с двумя парами. За счет экранирования удается обеспечить лучшую помехоустойчивость и уменьшить затухание. Поэтому для высокоскоростных сетей применяют именно его. Неэкранированная пара вполне подходит для низкоскоростных сетей, работающих на скоростях 10 или 16 мбит/сек.

### 4.1. Принципы функционирования и особенности сетей Ethernet

Технология Ethernet предназначена для работы только в шинных топологиях. Все рабочие станции подключены параллельно к общему кабелю. Обмены данными между любыми парами машин происходит по нему. Кабель является средой так называемого множественного доступа.

Все протоколы управления локальной сетью согласно модели открытых систем находятся на втором уровне и поэтому все то, что поступает на вход протокола, является пользовательскими данными. Эти данные на передающей станции запаковываются в кадры, в заголовке которого необходимо указать адрес получателя. После того как кадр сформирован (к поступившему блоку данных добавлен заголовок), он посылается в кабель (рис. 4.3). Система Ethernet использует способ множественного доступа с прослушиванием несущей и обнаружением коллизий (МДКН/ОК). Метод заключается в том, что все рабочие станции постоянно находятся в ре-

жиме прослушивания канала на предмет обнаружения передаваемого кадра данных. Соответственно, когда одна из станций обнаруживает, что передаваемый кадр содержит в заголовке ее адрес как адрес получателя, то она продолжит чтение кадра и по окончании приема проинформирует отправителя о его успешной доставке. Следовательно, в заголовке также должен содержаться и адрес отправителя. Остальные станции анализировать и принимать этот кадр не будут, поскольку в его заголовке указан не их адрес.

Может возникнуть ситуация, когда одновременно начать передачу. Смешиваются и разделить их будет чтобы одна станция начала передачу другой станции уже начал конечности времени распространения успел достичь ее. Если же станция обнаружила в нем передачу, то свой Это значит, что протокол предусматривает CS). Если же все же произошло, то станция должна передачу и дожидаться, пока канал не освободится. Во время передачи станция должна сравнивать то, что передала с тем, что слышит. Если переданное совпадает с принятым, то машина считает, что все в порядке, а когда выясняется, что в канале имеется другая передача, то очевидным образом на приеме будет услышана сумма двух сигналов. Станция посчитает, что обнаружена коллизия (collision detected). И в этот момент станции должны замолчать. Получается та же ситуация, что и при разговоре людей, которые вдруг начинают перебивать друг друга, затем вдруг опомнились и оба замолчали, давая слово другому. Если продолжить аналогию, то после того, как они замолчали, каждый из них может подумать, что собеседник молчит потому, что хочет дать ему слово. Так подумают оба и через некоторое время они опять заговорят одновременно и ситуация повторится. Для выхода из ситуации одновременного доступа устанавливается таймер на случайное время ожидания. Если две передачи столкнулись и станции обнаружили это, они запускают таймер, в течение действия которого они ожидают передачи от собеседника. Если же за это время собеседник не заговорил, что будет принято решение, что он молчит, потому что хочет дать слово ему и станция может начать передачу.

Если же коллизия все же произошла, то весь процесс повторится с тем лишь условием, что каждый новый запуск таймера будет проводиться со все возрастающим его значением. Конечно, этот процесс не может проходить бесконечно и поэтому каждая станция имеет у себя счетчик числа попыток. Если он досчитал до конца, станция будет считать канал вышедшим из строя и прекратит дальнейшие попытки. Шинная технология имеет ограничения параметров передаваемых кадров и протяженности шины. Минимально возможный интервал ожидания между обнаружением коллизии и возобновлением передачи должен быть не меньше, чем максимальное удвоенное время распространения сигнала. С другой стороны, это время влияет и на минимально допустимый размер кадра. Поэтому на шине Ethernet минимальная длина кадра составляет 64 байта, что вычисляется исходя из скорости работы сети (10мбит/с) и максимальной протяженности шины (2.5 км).

Технология Ethernet позволяет иметь максимальное расстояние между двумя компьютерами 2.5 км, однако, это не удастся сделать без дополнительных устройств. Во-первых, такая длина может быть только при использовании коаксиального кабеля. Те приемопередатчики (трансиверы — transceivers), которые установлены в платах с разъемом для коаксиала, вырабатывают мощность, которой хватает только на 500 метров. Поэтому, если необходима большая мощность, то придется ставить специальные повторители для усиления и исправления сигналов. Согласно требованиям технологии, таких репитеров не может быть более четырех. В противном случае нарушаются временные параметры, и могут появиться необнаруженные коллизии.

Если же сеть строится на витой паре, то эти расстояния значительно меньше. Так, максимальное расстояние, перекрываемое без исправления сигнала, — 180 метров, количество репитеров остается тем же — не более 4. Максимальная длина получается около 750 метров. Причем все эти параметры означают всего лишь, что все коллизии будут замечены и специальными протокольными средствами исправлены.

Другим способом управления доступом к среде передачи является управление с помощью маркера (token), который проходит от одной рабочей станции к другой в соответствии с заданным набором правил. Он воспринимается каждой станцией и задерживается в ней на некоторое время. Любая станция может начать передачу только тогда, когда она завладела маркером. После того, как кадр был передан, маркер должен быть отдан следующей станции. Последовательность действий получается следующей:

- формируется логическое кольцо, связывающее все станции и создается один маркер;
- маркер проходит от станции к станции по кольцу до тех пор, пока не достигнет станции, ожидающей разрешения на передачу;
- станция передает кадры данных, после чего передает маркер дальше по кольцу.

### 4.2. Принципы функционирования и особенности сетей Token Ring

Другим способом управления доступом к среде передачи является управление с помощью маркера (token), который проходит от одной рабочей станции к другой в соответствии с заданным набором правил. Он воспринимается каждой станцией и задерживается в ней на некоторое время. Любая станция может начать передачу только тогда, когда она завладела маркером. После того, как кадр был передан, маркер должен быть отдан следующей станции. Последовательность действий получается следующей:

- формируется логическое кольцо, связывающее все станции и создается один маркер;
- маркер проходит от станции к станции по кольцу до тех пор, пока не достигнет станции, ожидающей разрешения на передачу;
- станция передает кадры данных, после чего передает маркер дальше по кольцу.

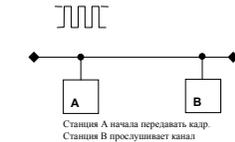


Рис. 4.3. Ввод данных в шину

две или более станций захотят. Следовательно, данные в канале невозможны. Поэтому нужно, в тот момент, когда кадр от передатчика, но из-за электромагнитного поля еще не при прослушивании канала кадр в канал она уже не выдст. сматривает контроль несущей — столкновение данных в канале немедленно остановить свою

сравнивать то, что передала с тем, что слышит. Если переданное совпадает с принятым, то машина считает, что все в порядке, а когда выясняется, что в канале имеется другая передача, то очевидным образом на приеме будет услышана сумма двух сигналов. Станция посчитает, что обнаружена коллизия (collision detected). И в этот момент станции должны замолчать. Получается та же ситуация, что и при разговоре людей, которые вдруг начинают перебивать друг друга, затем вдруг опомнились и оба замолчали, давая слово другому. Если продолжить аналогию, то после того, как они замолчали, каждый из них может подумать, что собеседник молчит потому, что хочет дать ему слово. Так подумают оба и через некоторое время они опять заговорят одновременно и ситуация повторится. Для выхода из ситуации одновременного доступа устанавливается таймер на случайное время ожидания. Если две передачи столкнулись и станции обнаружили это, они запускают таймер, в течение действия которого они ожидают передачи от собеседника. Если же за это время собеседник не заговорил, что будет принято решение, что он молчит, потому что хочет дать слово ему и станция может начать передачу.

Если же коллизия все же произошла, то весь процесс повторится с тем лишь условием, что каждый новый запуск таймера будет проводиться со все возрастающим его значением. Конечно, этот процесс не может проходить бесконечно и поэтому каждая станция имеет у себя счетчик числа попыток. Если он досчитал до конца, станция будет считать канал вышедшим из строя и прекратит дальнейшие попытки.

Шинная технология имеет ограничения параметров передаваемых кадров и протяженности шины. Минимально возможный интервал ожидания между обнаружением коллизии и возобновлением передачи должен быть не меньше, чем максимальное удвоенное время распространения сигнала. С другой стороны, это время влияет и на минимально допустимый размер кадра. Поэтому на шине Ethernet минимальная длина кадра составляет 64 байта, что вычисляется исходя из скорости работы сети (10мбит/с) и максимальной протяженности шины (2.5 км).

Технология Ethernet позволяет иметь максимальное расстояние между двумя компьютерами 2.5 км, однако, это не удастся сделать без дополнительных устройств. Во-первых, такая длина может быть только при использовании коаксиального кабеля. Те приемопередатчики (трансиверы — transceivers), которые установлены в платах с разъемом для коаксиала, вырабатывают мощность, которой хватает только на 500 метров. Поэтому, если необходима большая мощность, то придется ставить специальные повторители для усиления и исправления сигналов. Согласно требованиям технологии, таких репитеров не может быть более четырех. В противном случае нарушаются временные параметры, и могут появиться необнаруженные коллизии.

Если же сеть строится на витой паре, то эти расстояния значительно меньше. Так, максимальное расстояние, перекрываемое без исправления сигнала, — 180 метров, количество репитеров остается тем же — не более 4. Максимальная длина получается около 750 метров. Причем все эти параметры означают всего лишь, что все коллизии будут замечены и специальными протокольными средствами исправлены.

Все станции, подключенные к сети, имеют возможность реинициализации маркера в случае его потери, однако, в каждый момент времени только одна из них имеет на это право.

Физическое кольцо имеет тот же вид, что и логическое. В нем заложено направление, по которому маркер должен обходить все станции. На рис. 4.4 показан пример организации кольца, когда одна из машин выключена. Кольцо должно быть организовано так, чтобы при выключении питания одной из станций оно оставалось бы неразорванным.

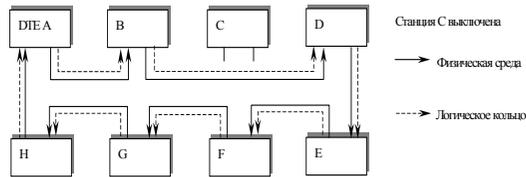


Рис. 4.4. Организация маркерного кольца

Особенностью системы Token Ring является то, что в ней не может быть коллизий, поскольку в каждый момент времени только одна станция может передавать данные, которая в данный момент имеет у себя маркер. Процесс передачи кадров в этой системе показан на рис. 4.5. Пусть станция A ожидает разрешения на передачу кадра (или кадров) и ждет прихода маркера. В момент, когда он у нее появился, начинается передача кадра, в заголовке которого указан адрес получателя и адрес отправителя. Для этого, помимо адресов, здесь так же требуются специальные поля. Кадр проходит по кольцу и каждая станция, принимая его, анализирует адрес получателя. Если кадр адресован не ей, то он передается дальше по кольцу до тех пор, пока не достигнет станции назначения. Станция назначения сохранит у себя копию этого кадра, а сам кадр отправит дальше по сети, указав в специальном поле метку, что кадр был станцией назначения прочитан. Далее, пройдя по всему кольцу, он вернется к отправителю, который, посмотрев, что он помечен как доставленный, уничтожит его. Кроме того, станция-отправитель, после того, как кадр был передан, уничтожает старый маркер и формирует новый, после чего выдает его в канал, не дожидаясь возвращения кадра данных. Это означает, что в кольце могут находиться одновременно много кадров, правда, все они будут находиться в разных звеньях кольца и поэтому не будут мешать друг другу. Станция, оставившая у себя копию кадра, после окончания его передачи дальше по кольцу отдает его для обработки в процедуры верхних уровней.

Сети строят на базе экранированной витой пары, причем длина кольца не имеет жесткого ограничения, так как нет необходимости иметь механизм обнаружения коллизий.

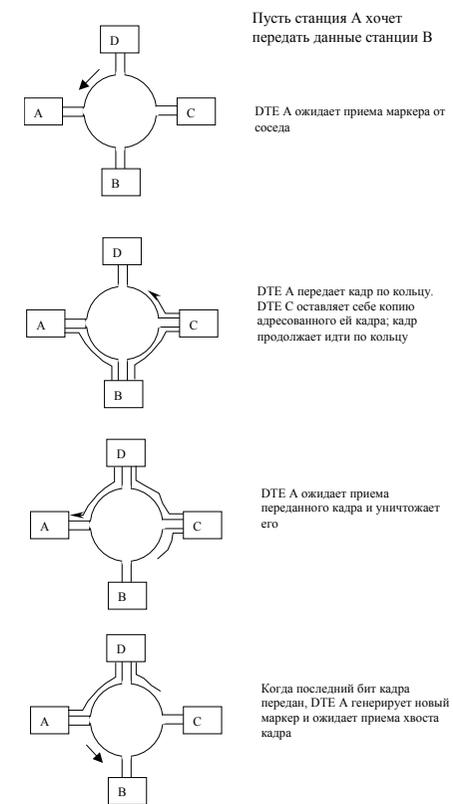


Рис. 4.5. Организация работы в Token Ring

### 4.3. Высокоскоростные локальные сети

При передаче больших объемов данных за ограниченное время в случае, если специфика его работы связана с обработкой графики, или технология требует большого обмена между технологическими машинами, необходимы сети, работающие на скорости 100 Мбит. Наиболее известные среди них системы FDDI (Fiber Distributed Data Interface), система Fast Ethernet и Gigabitethernet. Первая организована, как и следует из названия, на оптическом кабеле, другие на медных парах.

Система FDDI имеет очень много общего с Token Ring. Она так же работает по кольцевой схеме, правда в ней не одно кольцо, а два, передача по которым идет в разных направлениях. Большинство остальных отличий связаны с функционированием электроники в сетевых платах, а не с технологией. По сути, в основном они сводятся к принципу кодирования бит. Максимальная протяженность кольца FDDI составляет 200 км и может содержать более 1000 рабочих станций.

Другой высокоскоростной технологией является так называемый Fast Ethernet или 100BaseT. Как FDDI очень напоминает Token Ring, так Fast Ethernet очень напоминает простой Ethernet в том смысле, что изменился главным образом только способ кодирования бит и метод их ввода в кабель. Существенным пользовательским отличием является то, что этот стандарт не работает на коаксиальном кабеле, а только на витой паре или на оптическом кабеле. Что касается технологии передачи данных, т.е. работы второго уровня модели, то здесь используется протокол CSMA/CD.

Длина шины с ростом скорости уменьшается и составляет около 250 метров, что для большинства приложений бывает достаточно. Если же требуется шина более протяженная, то также, как и раньше, требуются репитеры и мосты для разделения сегментов.

#### **4.4. Подключение локальной сети к магистральной**

Все те устройства, о которых мы говорили в предыдущем разделе, имеют одну особенность — они работают только в локальных сетях. Однако сегодня уже никто не мыслит себе построение локальной сети без возможности выхода рабочих станций во внешний мир, т.е. без подключения ее к магистральной сети общего пользования. На границах между ними уже никак не обойдешься ни репитером, ни хабом, ни мостом, поскольку речь идет именно о стыковке разных адресных планов. Следовательно, здесь должен стоять маршрутизатор.

## ГЛАВА 5 ПОСТРОЕНИЕ БОЛЬШИХ СЕТЕЙ

Составная сеть (Internetwork) образуется при соединении двух или нескольких сетей, за организацию которых отвечает сетевой уровень (по стандарту OSI/ISO), в функции которого входит решение следующих задач:

- передача пакетов между конечными узлами в составных сетях;
- выбор маршрута передачи пакетов, наилучшего по некоторому критерию;
- согласование разных протоколов канального уровня, использующихся в отдельных подсетях одной составной сети.

Сети, входящие в составную сеть, называются подсетями, составляющими сетями или просто сетями (рис. 5.1).

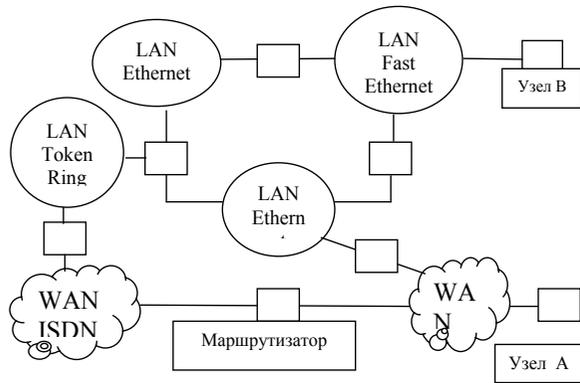


Рис. 5.1. Фрагмент составной сети

Компонентами составной сети могут являться как локальные, так и глобальные сети. В составную сеть могут входить сети различных технологий: как локальные сети (Ethernet, Fast Ethernet, Token Ring, FDDI), так и глобальные сети (frame relay, X.25, ЦСИО). Каждая из этих технологий может организовать взаимодействие всех узлов в своей подсети, но не способна построить информационную связь между произвольно выбранными узлами, принадлежащими разным подсетям. Поэтому для организации взаимодействия между любой произвольной парой узлов составной сети требуются средства, которые предоставляет сетевой уровень.

Сетевой уровень организует работу всех подсетей, лежащих на пути продвижения пакета по составной сети. Для перемещения данных в пределах подсетей сетевой уровень обращается к используемым в этих подсетях технологиям.

Сетевой уровень имеет собственную систему адресации (номер сети и номер узла), не зависящую от способов адресации узлов в отдельных подсетях и позволяющую идентифицировать любой узел составной сети. В качестве номера узла используется либо локальный адрес этого узла, либо некоторое число, не связанное с локальной технологией. Каждый узел составной сети имеет наряду со своим локальным адресом и универсальный сетевой адрес.

Данные, поступающие на сетевой уровень, снабжаются заголовком сетевого уровня и образуют пакет. Заголовок пакета имеет унифицированный формат, не зависящий от форматов кадров канального уровня тех сетей, которые могут входить в объединенную сеть, и несет наряду с другой служебной информацией данные о номере сети, которой предназначается пакет.

При передаче из одной подсети в другую пакет сетевого уровня, инкапсулированный в прибывший канальный кадр первой подсети, освобождается от заголовков этого кадра и окружается заголовками кадра канального уровня следующей подсети. Информацией, на основе которой делается эта замена, являются служебные поля пакета сетевого уровня. В поле адреса назначения нового кадра указывается локальный адрес следующего маршрутизатора.

Если в подсети доставка данных осуществляется средствами канального и физического уровней, то пакеты сетевого уровня упаковываются в кадры канального уровня.

Основным полем заголовка сетевого уровня является номер сети-адресата. Кроме номера сети заголовок сетевого уровня должен содержать следующую информацию, необходимую для успешного перехода пакета из сети одного типа в сеть другого типа:

- номер фрагмента пакета для проведения операций сборки-разборки фрагментов при соединении сетей с разными максимальными размерами пакетов;

- время жизни пакета;
- качество услуги – критерий выбора маршрута при межсетевых передачах.

Когда две и более сети организуют совместную транспортную службу, то такой режим взаимодействия называют межсетевым взаимодействием.

### 5.1. Устройства, позволяющие расширить сеть

К устройствам, которые позволяют расширить сеть, относятся:

- повторители;
- мосты;
- маршрутизаторы;
- мосты-маршрутизаторы;
- шлюзы.

Повторители. При распространении по кабелю сигнал искажается, поскольку уменьшается его амплитуда, и накладываются помехи. Причина этого явления — затухание. При достаточной длине кабеля, затухание и воздействие помех может исказить сигнал до неузнаваемости. Чтобы этого не произошло, восстанавливают повторители, благодаря которым сигналы способны распространяться на большие расстояния. Повторитель работает на физическом уровне модели ISO, восстанавливая сигнал и передавая его в другие сегменты.

Повторитель принимает затухающий сигнал из одного сегмента, восстанавливает его и передает в следующий сегмент. Повторители не имеют функций преобразования и фильтрации. Чтобы повторитель работал, оба соединяемые им сегмента должны иметь одинаковый метод доступа. Наиболее распространенные методы доступа – CSMA/CD и передача маркера. Повторители не могут транслировать пакеты Ethernet в пакеты Token Ring.

Однако повторители могут передавать пакеты из одного типа физического носителя в другой. Если повторитель имеет соответствующие разъемы, он примет пакет Ethernet, приходящий из сегмента на тонком коаксиальном кабеле, и передаст его в сегмент на оптоволокне.

Мосты. Мост, как и повторитель, может соединять сегменты или локальные сети рабочих групп. Однако, в отличие от повторителя, мост позволяет разбить сеть на несколько сегментов, изолировав за счет этого часть трафика. Мосты предназначены для:

- увеличения размеров сети;
- соединения разнородных физических сред (витая пара и коаксиальный кабель);
- устранения узких мест, появляющихся в результате подключения избыточного числа компьютеров, и, как следствие, возрастания трафика;
- соединения сегментов разнородных сети (например, Ethernet и Token Ring) и переноса между ними пакетов.

Мосты работают на канальном уровне модели OSI, поэтому им не доступна информация, содержащаяся на более высоких уровнях. Мосты допускают использование в сети всех протоколов (не отличая при этом один протокол от другого), поэтому каждый компьютер должен определять, с какими протоколами он работает.

Мосты функционируют на подуровне управления доступом к среде, и выполняют следующие действия:

- «слушают» весь трафик;
- проверяют адреса источника и получателя каждого пакета;
- строят таблицу маршрутизации;
- передают пакеты.

Передача пакетов осуществляется следующим образом. Если адресат не указан в таблице маршрутизации, мост передает пакет во все сегменты. Если адресат указан в таблице маршрутизации, мост передает пакет в этот сегмент (если сегмент получателя не совпадает с сегментом источника).

Мосты обладают некоторым «интеллектом», поскольку изучают, куда следует направить данные. Когда пакеты передаются через мост, данные об адресах компьютеров сохраняются в оперативной памяти моста и используются для построения таблицы маршрутизации.

Мосты строят таблицы маршрутизации на основе адресов компьютеров, которые передавали данные в сеть. Принимая пакет, мост ищет адрес источника в таблице маршрутизации. Если адрес источника не найден, он добавляет его в таблицу маршрутизации. Затем мост сравнивает адреса назначения с базой данных таблицы маршрутизации. При этом возможны следующие варианты:

- если адрес получателя есть в таблице маршрутизации и адрес находится в одном сегменте с источником, пакет отбрасывается. Эта фильтрация уменьшает сетевой трафик и изолирует сегменты сети;
- если адрес получателя есть в таблице маршрутизации, а адресат и источник находятся в разных сегментах, мост передает пакет адресату через соответствующий порт;
- если адреса получателя нет в таблице маршрутизации, мост передает пакет во все свои порты, исключая тот, через который пакет был принят.

Чтобы объединить несколько малых сетей в одну большую, используется несколько мостов.

Существует также мост-маршрутизатор, обладающий свойствами как моста, так и маршрутизатора (в зависимости от протоколов). С одними протоколами он работает как маршрутизатор, с другими как мост. Мосты-маршрутизаторы выполняют следующие функции:

- маршрутизируют маршрутизируемые протоколы;
- функционируют как мосты для немаршрутизируемых протоколов;
- обеспечивают более экономичное и более управляемое взаимодействие сетей по сравнению с раздельными мостами и маршрутизаторами.

Шлюзы также являются средствами расширения сетей. Они обеспечивают связь между различными архитектурами и сетевыми средами. Они распаковывают и преобразуют данные, передаваемые из одной среды в другую, чтобы каждая среда могла понимать сообщения извне.

Шлюз связывает две системы, которые применяют разные:

- коммуникационные протоколы;
- структуры и форматы данных;
- языки;
- архитектуры.

Шлюзы создаются для выполнения конкретного типа преобразования данных. Обработывая данные, шлюз выполняет следующие операции:

- извлекает данные из входящих пакетов, пропуская их снизу вверх через полный стек протоколов передающей сети;
- заново упаковывает полученные данные, пропуская их сверху вниз через стек протоколов сети назначения.

Маршрутизаторы. В среде, объединяющей несколько сетевых сегментов с различными протоколами и архитектурами, необходимо устройство, которое не только знает адрес каждого сегмента, но и определяет наилучший маршрут для передачи данных, а также фильтрует широковещательные сообщения.

Маршрутизаторы работают на сетевом уровне модели OSI, поэтому они могут переадресовывать и маршрутизировать пакеты через множество сетей, обмениваясь информацией между отдельными сетями. Они считывают в пакете адресную информацию сложной сети и поскольку они функционируют на более высоком по сравнению с мостами уровне модели OSI, имеют доступ к дополнительным данным. Маршрутизаторы могут выполнять следующие функции мостов:

- фильтровать и изолировать трафик;
- соединять сегменты сети.

Эти устройства оптимизируют доставку пакетов, обеспечивают управление трафиком, не пропускают широковещательные сообщения, также могут обмениваться данными о состоянии маршрутов и, основываясь на этой информации, обходить медленные и неисправные каналы связи.

Таблица маршрутизации, находящаяся в маршрутизаторах, содержит сетевые адреса для определения адреса назначения. Для каждого протокола, используемого в сети, строится своя таблица, которая содержит:

- все известные сетевые адреса;
- способы связи с другими сетями;
- возможные пути между маршрутизаторами;
- «стоимость» передачи данных по этим маршрутам.

Данное устройство выбирает наилучший путь для данных, сравнивая различные варианты.

Маршрутизаторы требуют специальной адресации: им понятны только номера сетей (что позволяет им обращаться друг к другу) и адреса локальных плат сетевого адаптера, однако они не могут обращаться к удаленным компьютерам. Принимая пакеты, предназначенные для удаленной сети, маршрутизатор пересылает их другому маршрутизатору, точнее тому, который обслуживает сеть назначения. Такой механизм передачи пакетов можно рассматривать как достоинство этих устройств, потому что они позволяют:

- сегментировать большие сети на меньшие;
- действовать как барьер безопасности между сегментами;
- предотвращать широковещательный шторм (широковещательные сообщения не передаются).

Так как маршрутизаторы выполняют сложную обработку каждого пакета, они медленнее большинства мостов. Когда пакеты передаются от одного маршрутизатора к другому, то адреса источника и получателя канального уровня отсекаются, а затем создаются заново. Это позволяет маршрутизатору направлять пакеты из сети TCP/IP Ethernet серверу сети TCP/IP Token Ring.

Пропуская только адресные сетевые пакеты, маршрутизаторы препятствуют проникновению в сеть некорректных пакетов.

Адрес узла назначения маршрутизаторы не проверяют – они смотрят только на адрес сети. Эта возможность контролировать данные, передаваемые через маршрутизатор, позволяет, во-первых, уменьшить трафик между сетями, и, во-вторых, использовать его гораздо эффективнее, чем это делают мосты.

## 5.2. Маршрутизация больших сетей

Важнейшей задачей сетевого уровня является маршрутизация — передача пакетов между двумя конечными узлами в составной сети. В сложных составных сетях существуют альтернативные маршруты для передачи пакетов между двумя конечными узлами. Маршрут — это последовательность маршрутизаторов, которые должен пройти пакет от отправителя до пункта назначения. Задачу выбора маршрута из нескольких возможных решают маршрутизаторы, а также конечные узлы. Маршрут выбирается на основании имеющейся у этих уст-

ройств информации о текущей конфигурации сети, а также на основании указанного критерия выбора маршрута. Обычно в качестве критерия выступает задержка прохождения маршрута отдельным пакетом или средняя пропускная способность маршрута для последовательности пакетов.

Для того чтобы по адресу сети назначения можно было бы выбрать рациональный маршрут дальнейшего следования пакета, каждый конечный узел и маршрутизатор анализируют специальную информационную структуру, называемую таблицей маршрутизации.

Таблица 5.1

Пример таблицы маршрутизации конечного узла

Номер сети назначения	Сетевой адрес следующего маршрутизатора	Сетевой адрес выходного порта	Расстояние до сети назначения
S12	-	MA	2
Default	M17(1)	MA	-

В первом столбце таблицы перечисляются номера сетей, входящих в интересующую сеть. В каждой строке таблицы следом за номером сети указывается сетевой адрес следующего маршрутизатора, на который надо направить пакет, чтобы тот передвигался по направлению к сети с данным номером по рациональному маршруту.

Когда на маршрутизатор поступает новый пакет, номер сети назначения, извлеченный из поступившего кадра, последовательно сравнивается с номерами сетей из каждой строки таблицы. Строка с совпавшим номером сети указывает, на какой ближайший маршрутизатор следует направить пакет. Поскольку пакет может быть адресован в любую сеть составной сети, то каждая таблица маршрутизации должна иметь записи обо всех сетях, входящих в составную сеть. При таком подходе объем таблиц маршрутизации может оказаться большим. Поэтому на практике число записей в таблице маршрутизации уменьшают за счет использования специальной записи — «маршрутизатор по умолчанию» (default).

Перед тем как передать пакет следующему маршрутизатору, текущий маршрутизатор должен определить, на какой из нескольких собственных портов он должен поместить пакет. Для этого служит третий столбец таблицы маршрутизации.

При выборе маршрута используется столбец «Расстояние до сети назначения». При этом под расстоянием понимается любая метрика, используемая в соответствии с заданным в сетевом пакете критерием. Расстояние может измеряться хабами, временем прохождения пакета по линиям связи или другой величиной, отражающей качество данного маршрута по отношению к заданному критерию.

Задачу маршрутизации решают не только промежуточные узлы- маршрутизаторы но и конечные узлы- компьютеры. Средства сетевого уровня, установленные на конечном узле, при обработке пакета должны, прежде всего, определить, направляется ли он в другую сеть или адресован какому-нибудь узлу данной сети.

Для конечных узлов таблицы маршрутизации создаются вручную администраторами и хранятся в виде постоянных файлов на диске.

## 5.3. Способы маршрутизации

Для автоматического построения таблиц маршрутизации маршрутизаторы обмениваются информацией о топологии составной сети в соответствии со специальным служебным протоколом. Протоколы этого типа называются протоколами маршрутизации.

С помощью протоколов маршрутизации маршрутизаторы составляют карту связей сети, на основании которой для каждого номера сети принимается решение о рациональном направлении передачи пакетов. Результаты этих решений заносятся в таблицу маршрутизации. При изменении конфигурации сети некоторые записи в таблице становятся недействительными. В таких случаях пакеты, отправленные по ложным маршрутам, могут заклиниваться и теряться. От того, насколько быстро протокол маршрутизации приводит в соответствие содержимое таблицы реальному состоянию сети, зависит качество работы всей сети.

Протоколы маршрутизации могут быть построены на основе разных алгоритмов, отличающихся способами построения таблиц маршрутизации, способами выбора наилучшего маршрута и другими особенностями своей работы.

Существуют следующие алгоритмы маршрутизации (рис. 5.2):

Одношаговые. При выборе рационального маршрута определяется только следующий (ближайший) маршрутизатор, а не вся последовательность маршрутизаторов от начального до конечного узла.



Рис. 5.2. Классификация алгоритмов маршрутизации

Эти алгоритмы в зависимости от способа формирования таблиц маршрутизации делятся на три класса.

**Алгоритмы статической маршрутизации.** В этих алгоритмах все записи в таблице маршрутизации являются статическими. Администратор сети сам решает, на какие маршрутизаторы надо передавать пакеты с теми или иными адресами, и вручную заносит соответствующие записи в таблицу маршрутизации. Таблица создается в процессе загрузки, в дальнейшем она используется без изменений до тех пор, пока ее содержимое не будет отредактировано вручную. Различают одномаршрутные таблицы, в которых для каждого адресата задан один путь, и многомаршрутные таблицы, определяющие несколько альтернативных путей для каждого адресата. В многомаршрутных таблицах должно быть задано правило выбора одного из маршрутов. Чаще всего один путь является основным, а остальные – резервными.

**Алгоритмы простой маршрутизации.** В этих алгоритмах таблица маршрутизации либо вовсе не используется, либо строится без участия протоколов маршрутизации. Выделяют три типа простой маршрутизации:

- 1) случайная маршрутизация, когда прибывший пакет посылается в первом попавшем случайном направлении, кроме исходного;
- 2) лавинная маршрутизация, когда пакет широковещательно посылается по всем возможным направлениям, кроме исходного;
- 3) маршрутизация по предыдущему опыту, когда выбор маршрута осуществляется по таблице, но таблица строится по принципу моста путем анализа адресных полей пакетов, появляющихся на входных портах.

**Алгоритмы адаптивной (динамической) маршрутизации.** Эти алгоритмы обеспечивают автоматическое обновление таблиц маршрутизации после изменения конфигурации сети. Протоколы, построенные на основе адаптивных алгоритмов, позволяют всем маршрутизаторам собирать информацию о топологии связей в сети, оперативно обрабатывая все изменения конфигурации связей. В таблицах маршрутизации при адаптивной маршрутизации обычно имеется информация об интервале времени, в течение которого данный маршрут будет оставаться действительным. Это время называют временем жизни маршрута. Эти алгоритмы обычно имеют распределенный характер, который выражается в том, что в сети отсутствуют какие-либо выделенные маршрутизаторы, которые собирали бы и обобщали топологическую информацию: эта работа распределена между всеми маршрутизаторами.

Адаптивные алгоритмы обмена маршрутной информацией, применяемые в настоящее время в вычислительных сетях, в свою очередь делятся на две группы, каждая из которых связана с одним из следующих типов алгоритмов.

**Дистанционно-векторные алгоритмы (DVA).** В таких алгоритмах каждый маршрутизатор периодически и широковещательно рассылает по сети вектор, компонентами которого являются расстояния от данного маршрутизатора до всех известных ему сетей. Под расстоянием обычно понимается число хабов. При получении вектора от соседа маршрутизатор наращивает расстояния до указанных в векторе сетей на расстояние до данного соседа. Получив вектор от соседнего маршрутизатора, каждый маршрутизатор добавляет к нему информацию об известных ему других сетях, о которых он узнал непосредственно или из аналогичных объявлений других маршрутизаторов, а затем снова рассылает новое значение вектора по сети. Эти алгоритмы хорошо работают в небольших сетях. В больших сетях они засоряют линии связи интенсивным широковещательным трафи-

ком. Наиболее распространенным протоколом, основанным на дистанционно-векторном алгоритме, является протокол RIP.

Алгоритмы состояния связей обеспечивают каждый маршрутизатор информацией для построения графа связей сети. Все маршрутизаторы работают на основании одинаковых графов, что делает процесс маршрутизации более устойчивым к изменениям конфигурации. Вершинами графа являются как маршрутизаторы, так и объединяемые ими сети.

Протоколами, основанными на алгоритме состояния связей, являются протоколы IS-IS стека OSI, OSPF стека TCP/IP и недавно реализованный протокол NLSР стека Novell.

Многошаговые алгоритмы или маршрутизация от источника. Этот метод является прямо противоположным вышеописанному алгоритму. Он состоит в том, что узел-источник задает в отправляемом в сеть пакете полный маршрут его следования через все промежуточные маршрутизаторы. При использовании этого метода нет необходимости строить и анализировать таблицы маршрутизации. Это ускоряет прохождение пакета по сети, разгружает маршрутизаторы, но при этом большая нагрузка ложится на конечные узлы.

Протоколы маршрутизации RIP, OSPF, NLSР следует отличать от собственно сетевых протоколов таких, как IP, IPX. И те и другие выполняют функции сетевого уровня модели OSI — участвуют в доставке пакетов адресату через разнородную составную сеть. Но в то время, как первые собирают и передают по сети чисто служебную информацию, вторые предназначены для передачи пользовательских данных, как это делают протоколы канального уровня. Протоколы маршрутизации используют сетевые протоколы как транспортное средство. При обмене маршрутной информацией пакеты протокола маршрутизации помещаются в поле данных пакетов сетевого уровня или даже транспортного уровня, поэтому с точки зрения вложенности пакетов протоколы маршрутизации формально следовало бы отнести к более высокому уровню, чем сетевой.

#### 5.4. Функции маршрутизатора

Основная функция маршрутизатора — чтение заголовков пакетов сетевых протоколов, принимаемых и буферизуемых по каждому порту, и принятие решения о дальнейшем маршруте следования пакета по его сетевому адресу, включающему, как правило, номер сети и номер узла.

Функции маршрутизатора могут быть разбиты на три группы в соответствии с уровнями модели OSI: нижний уровень, уровень интерфейсов и уровень протоколов.

На нижнем уровне маршрутизатор, как и любое другое устройство, подключенное к сети, обеспечивает физический интерфейс со средой передачи, включая согласование уровней электрических сигналов, линейное и логическое кодирование, оснащение определенным типом разъема. В разных моделях маршрутизаторов часто предусматриваются различные наборы физических интерфейсов, представляющих собой комбинацию портов для подсоединения локальных и глобальных сетей. С каждым интерфейсом для подключения локальной сети неразрывно связан определенный протокол канального уровня (например, Ethernet, Token Ring, FDDI).

Уровень интерфейсов маршрутизатора выполняет набор функций физического и канального уровней по передаче кадра, включая получение доступа к среде, формирование битовых сигналов, прием кадра, подсчет его контрольной суммы и передачу поля данных кадра верхнему уровню, в случае если контрольная сумма имеет корректное значение.

Кадры, которые поступают на порты маршрутизатора, после обработки соответствующими протоколами физического и канального уровней, освобождаются от заголовков канального уровня. Извлеченные из поля данных кадра пакеты передаются модулю сетевого протокола.

На уровне протоколов (сетевой и выше) из пакета извлекается заголовок сетевого уровня анализируется содержимое его полей и проверяется контрольная сумма. Если пакет пришел поврежденным, то он отбрасывается. Выполняется проверка на превышение времени, которое провел пакет в сети (время жизни пакета), допустимой величины.

Модуль сетевого протокола маршрутизатора способен производить разбор и анализ отдельных полей пакета. Он оснащен развитыми средствами пользовательского интерфейса, позволяющие администратору без особых усилий задавать сложные правила фильтрации.

Маршрутизаторы могут анализировать структуру сообщений транспортного уровня, поэтому фильтры могут не пропускать в сеть сообщения определенных прикладных служб (например, службы telnet).

В случае, если интенсивность поступления пакетов выше интенсивности, с которой они отбрасываются, пакеты могут образовать очередь. При этом программное обеспечение маршрутизатора может реализовать различные дисциплины обслуживания очередей пакетов: в порядке поступления по принципу «первый пришел — первым обслужен» (FIFO), случайное раннее обнаружение, когда обслуживание идет по правилу FIFO, но при достижении длины очереди некоторого порогового значения вновь поступающие пакеты отбрасываются (RED), а также различные варианты приоритетного обслуживания.



Рис. 5.3. Функциональная модель маршрутизатора

На сетевом уровне определяется маршрут пакета. По номеру сети, извлеченному из заголовка пакета, модуль сетевого протокола находит в таблице маршрутизации строку, содержащую сетевой адрес следующего маршрутизатора и номер порта, на который нужно передать данный пакет, чтобы он двинулся в правильном направлении.

Перед тем, как передать сетевой адрес следующего маршрутизатора на канальный уровень, необходимо преобразовать его в локальный адрес той технологии, которая используется в сети, содержащей следующий маршрутизатор. Для этого сетевой протокол обращается к протоколу разрешения адресов. Протоколы этого типа устанавливают соответствие между сетевыми и локальными адресами либо на основании заранее составленных таблиц, либо путем рассылки широковещательных запросов. Таблица соответствия локальных адресов сетевым адресам строится отдельно для каждого сетевого интерфейса. Протоколы разрешения адресов занимают промежуточное положение между сетевым и канальным уровнями.

С сетевого уровня пакет, локальный адрес следующего маршрутизатора и номер порта маршрутизатора передаются, канальному уровню. На основании указанного номера порта осуществляется коммутация с одним из интерфейсов маршрутизатора, средствами которого выполняется упаковка пакета в кадр соответствующего формата. В поле адреса назначения заголовка кадра помещается локальный адрес следующего маршрутизатора. Готовый кадр отправляется в сеть.

### 5.5. Протокол TCP/IP

Стек TCP/IP является самым популярным средством организации составных сетей. Стек состоит из 4 уровней (табл. 5.2), каждый из которых отвечает за организацию эффективной работы составной сети, построенной на основе разных сетевых технологий.

Таблица 5.2

Многоуровневая архитектура стека TCP/IP

Уровень 1	Прикладной уровень
Уровень 2	Основной (транспортный) уровень
Уровень 3	Уровень межсетевого взаимодействия
Уровень 4	Уровень сетевых интерфейсов

Стержнем всей архитектуры (рис. 5.4) является уровень межсетевого взаимодействия, который передает пакеты в режиме без установления соединений (дейтаграммным способом). Именно этот уровень обеспечивает возможность перемещения пакетов по сети, используя тот маршрут, который в данный момент является наиболее рациональным.

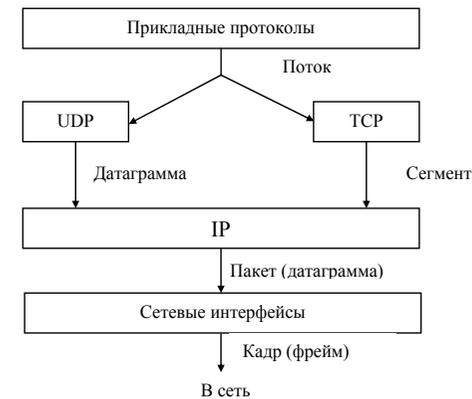


Рис. 5.4. Название единиц данных, используемые в TCP/IP

Потоком называют данные, поступающие от приложений на вход протоколов транспортного уровня TCP и UDP. Протокол TCP нарезает из потока сегменты. Единицу данных протокола UDP часто называют дейтаграммой. Дейтаграмма — это общее название для единиц данных, которым оперируют протоколы без установления соединений. К таким протоколам относится и протокол межсетевого взаимодействия IP. Дейтаграмму протокола IP называют также пакетом.

В стеке TCP/IP кадрами (фреймами) называют единицы данных протоколов, на основе которых IP-пакеты переносятся через подсети составной сети. При этом не имеет значения, какое название используется для этой единицы данных в локальной технологии.

Основным протоколом сетевого уровня в стеке TCP/IP является протокол IP, предназначенный для передачи пакетов в составных сетях, состоящих из большого количества сетей, объединенных как локальными, так и глобальными связями. Поэтому протокол IP хорошо работает в сетях со сложной топологией, рационально используя наличие в них подсистем и экономно расходуя пропускную способность низкоскоростных линий связи. Поскольку протокол IP является дейтаграммным протоколом, он не гарантирует доставку пакетов до узла назначения.

К уровню межсетевого взаимодействия относятся также все протоколы, связанные с составлением и модификацией таблиц маршрутизации. Это протоколы сбора маршрутной информации RIP и OSPF, а также протокол межсетевых управляющих сообщений ICMP. Последний протокол предназначен для обмена информацией об ошибках между маршрутизаторами сети и узлом-источником пакета. С помощью специальных пакетов ICMP сообщает о невозможности доставки пакета, о превышении времени жизни или продолжительности сборки пакета из фрагментов, об аномальных величинах параметров, об изменении маршрута пересылки и типа обслуживания, о состоянии системы и т.п.

Поскольку на сетевом уровне не устанавливаются соединения, то нет никаких гарантий, что все пакеты будут доставлены в место назначения или придут в том же порядке, в котором они были отправлены. Задачу обеспечения надежной информационной связи между двумя конечными узлами решает основной уровень стека TCP/IP, называемый также транспортным.

На этом уровне функционируют протокол управления передачей TCP и протокол дейтаграмм пользователя UDP. Протокол TCP обеспечивает надежную передачу сообщений между удаленными прикладными процессами за счет образования логических соединений. Этот протокол позволяет равноправным объектам на компьютере-отправителе и компьютере-получателе поддерживать обмен данными в дуплексном режиме. TCP позволя-

ет без ошибок доставить сформированный на одном из компьютеров поток байт в любой другой компьютер, входящий в составную сеть. TCP делит поток байт на части – сегменты и передает их нижнему уровню межсетевого взаимодействия. После того, как эти сегменты будут доставлены средствами уровня межсетевого взаимодействия в пункт назначения, протокол TCP снова соберет их в непрерывный поток байт.

Протокол UDP обеспечивает передачу прикладных пакетов дейтаграммным способом, как и главный протокол уровня межсетевого взаимодействия IP, и выполняет только функции связующего звена между сетевым протоколом и многочисленными службами прикладного уровня или пользовательскими процессами.

Прикладной уровень объединяет все службы, предоставляемые системой пользовательским приложениям. Он реализуется программными системами, построенными в архитектуре клиент-сервер, базирующимися на протоколах нижних уровней. Этот уровень постоянно расширяется за счет присоединения к старым, прошедшим многолетнюю эксплуатацию сетевым службам (Telnet, FTP, TFTP, DNS, SNMP) сравнительно новых служб (например, протокол передачи гипертекстовой информации HTTP).

Протоколы уровня сетевых интерфейсов TCP/IP обеспечивают интеграцию в составную сеть других сетей независимо от того, какую бы внутреннюю технологию передачи данных эта сеть не использовала. В то же время для каждой технологии, включаемой в составную сеть подсети, должны быть разработаны собственные интерфейсные средства. К таким интерфейсным средствам относятся протоколы инкапсуляции IP-пакетов уровня межсетевого взаимодействия в кадры локальных технологий.

Уровень сетевых интерфейсов в протоколах TCP/IP поддерживает стандарты физического и канального уровней: для локальных сетей это Ethernet, Token Ring, FDDI, Fast Ethernet, Gigabit Ethernet, 100VG-AnyLAN, для глобальных сетей это протоколы соединений «точка-точка»(SLIP и PPP), протоколы территориальных сетей с коммутацией пакетов X.25, frame relay. Разработана также спецификация, определяющая использование технологии ATM в качестве транспорта канального уровня.

Стек TCP/IP имеет многоуровневую структуру (рис. 5.5), функции которой зависят от конкретной технической реализации сети, функции уровней ориентированы на работу с приложениями (рис. 5.6).

7	WWW, Gopher, WAIS	SNMP	FTP	Telnet	SMTP	TFTP	I
6							II
5	TCP					UDP	
4							
3	IP	ICMP	RIP	OSPF	ARP		III
2	Не регламентируется Ethernet, Token Ring, FDDI, X.25, SLIP, PPP						IV
1							

Уровни модели  
OSI

Уровни стека  
TCP/IP

Рис 5.6 Рис. 5.5. Стек TCP/IP и семиуровневая модель OSI

Протоколы прикладного уровня стека TCP/IP работают на компьютерах, выполняющих приложения пользователей. При этом модернизация оборудования не влияет на работу приложений, если они получают доступ к сетевым возможностям через протоколы прикладного уровня.

Протоколы транспортного уровня зависят от сети, так как они реализуют интерфейс к уровням, непосредственно организующим передачу данных по сети. Протоколы прикладного уровня и программные модули, реализующие протоколы транспортного уровня, устанавливаются только на конечных узлах. Протоколы двух нижних уровней являются сетезависимыми, и, следовательно, программные модули протоколов межсетевого уровня и уровня интерфейсов устанавливаются как на конечных узлах составной сети, так и на маршрутизаторах.

Каждый коммуникационный протокол оперирует с некоторой единицей передаваемых данных. Названия этих единиц иногда закрепляются стандартом, а чаще просто определяются традицией. В стеке TCP/IP за многие годы его существования образовалась устоявшаяся терминология в этой области.

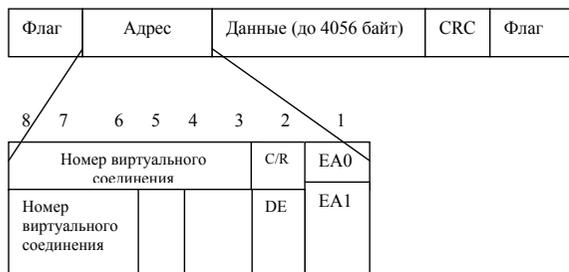


Рис. 6.5. Формат кадра LAP-F

#### **Поддержка качества обслуживания**

Благодаря особому подходу технология frame relay гарантированно обеспечивает основные параметры качества транспортного обслуживания, необходимые при объединении локальных сетей.

Используется процедура заказа качества обслуживания при установлении соединения. Для каждого виртуального соединения определяется несколько параметров, влияющих на качество обслуживания:

- CIR (Committed Information Rate) - согласованная информационная скорость, с которой сеть будет передавать данные пользователя;
- Bc (Committed Burst Size) - согласованный объем пульсации, то есть максимальное количество байтов, которое сеть будет передавать от этого пользователя за интервал времени T;
- Be (Excess Burst Size) - дополнительный объем пульсации, то есть максимальное количество байтов, которое сеть будет пытаться передать сверх установленного значения Bc за интервал времени T.

Основной параметр, по которому абонент и сеть заключают соглашение при установлении виртуального соединения, является CIR. Если пользователь на каком-то промежутке времени T передает в сеть данные со средней скоростью, превосходящей CIR, то кадр подлежит удалению, предварительно пометив кадр признаком DE (Discard Eligibility) равным 1.

Для контроля соглашения о параметрах качества обслуживания все коммутаторы сети frame relay выполняют алгоритм «дырявого ведра». Алгоритм использует счетчик С поступивших байт. Каждые T секунд этот счетчик уменьшается на величину Bc. Все кадры, данные которых не увеличили значение счетчика свыше порога Bc, пропускаются в сеть со значение признака DE=0, другие тоже передаются в сеть, но со значением признака DE=1. Если коммутаторы испытывают перегрузку, кадры помеченные признаком DE=1, удаляются.

Пользователь может договориться о включении не всех параметров качества обслуживания на данном виртуальном канале. Например, можно использовать только параметры CIR и Bc. Этот вариант дает более качественное обслуживание, так как кадры никогда не отбрасываются коммутатором сразу.

## ГЛАВА 6

### ГЛОБАЛЬНЫЕ СЕТИ

Глобальные сети объединяют источники информации, территориально расположенные на больших пространствах. Прокладка высококачественных линий связи на большие расстояния обходится очень дорого, из-за чего в глобальных сетях используются существующие линии связи. Поэтому к глобальным сетям также относятся телефонные, телеграфные и телексовые сети, получившие название интегрированных.

Основная функция, которую выполняют глобальные сети — предоставление транспортных и высокоуровневых услуг.

Глобальная вычислительная сеть (ГВС) должна передавать информацию любого типа: пакеты локальных сетей, мини-компьютеров и мэйнфреймов, факсы, трафики офисных АТС с выходом в городские, междугородные и международные телефонные сети, видеоизображения и высококачественный звук при организации видеоконференций, трафики кассовых аппаратов, банкоматов и т.д.

К высокоуровневым услугам относятся:

- поддержка служб прикладного уровня для абонентов глобальной сети;
- распространение публично-доступной аудио-, видео- и текстовой информации;
- организация интерактивного взаимодействия абонентов сети в реальном масштабе времени.

Структура глобальной сети приведена на рис. 6.1.

На рисунке: S – коммутаторы; К – компьютеры; R – маршрутизаторы; MUX – мультиплексоры; UNI – интерфейс пользователь-сеть; NNI – интерфейс сеть-сеть; PBX – офисная АТС.

Основные элементы сети — это коммутаторы, соединенные выделенными каналами связи. Коммутаторы обрабатывают пакеты, кадры, ячейки. Для подключения конечных пользователей используются коммутируемые каналы телефонных сетей.

Конечные узлы или терминалы (DTE — Data terminal equipment) — это отдельные компьютеры, локальные сети, маршрутизаторы и мультиплексоры, которые используются для одновременной передачи по компьютерной сети данных и голоса или изображения. К ним также относятся банкоматы и источники телеметрии.

Все эти устройства вырабатывают данные для передачи в глобальной сети, поэтому являются для нее устройствами типа DTE (Data Terminal Equipment). Локальная сеть отделяется от глобальной маршрутизатором или удаленным мостом, поэтому локальная сеть представляется единым устройством DTE — портом маршрутизатора или моста.

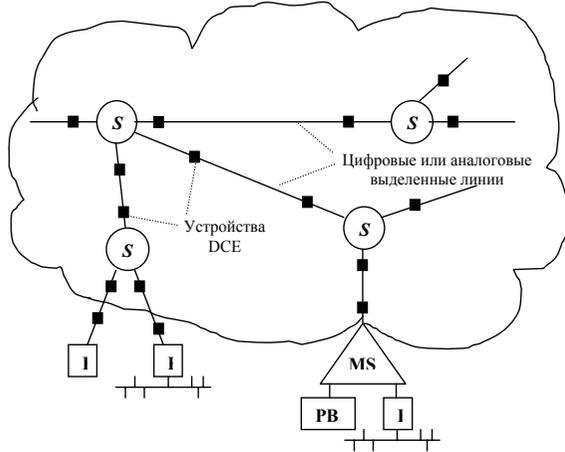


Рис. 6.1. Структура глобальной сети

При передаче данных через глобальную сеть мосты и маршрутизаторы работают так же, как и при соединении локальных сетей. Мосты, которые в этом случае называются удаленными мостами, строят таблицу MAC-адресов и на основании таблицы принимают решение о том, передавать кадры в удаленную сеть или нет. Маршрутизаторы принимают решение на основании номера сети пакета какого-либо протокола сетевого уровня (например, IP или IPX) и, если пакет нужно переправить следующему маршрутизатору по глобальной сети, например frame relay, упаковывают его в кадр этой сети, снабжают соответствующим аппаратным адресом следующего маршрутизатора и отправляют в глобальную сеть.

Так как конечные узлы глобальной сети должны передавать данные по каналу связи определенного стандарта, то каждое устройство типа DTE требуется оснастить устройством типа DCE (Data Circuit terminating Equipment), обеспечивающее необходимый протокол физического уровня данного канала. В зависимости от канала для связи используются DCE трех основных типов: модемы для работы по выделенным и коммутируемым аналоговым каналам, устройства DSU/CSU для работы по цифровым выделенным каналам сетей технологии TDM и терминальные адаптеры для работы по цифровым каналам сетей ISDN и ATM.

#### 6.1. Типы глобальных сетей

Принято различать следующие виды глобальных сетей (рис. 6.2)

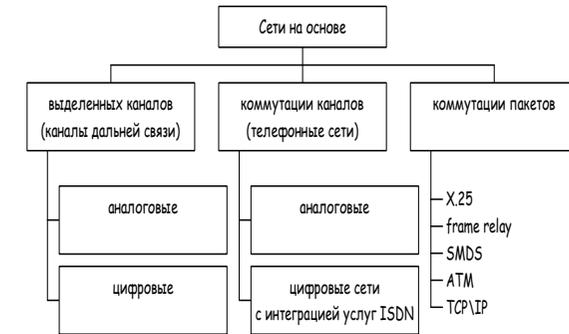


Рис. 6.2. Классификация глобальных сетей

Существует большой выбор выделенных каналов — от аналоговых каналов тональной частоты с полосой пропускания 3,1 кГц до цифровых каналов технологии с пропускной способностью 155 и 622 Мбит/с. Выделенные линии представляют собой надежное средство соединения локальных сетей через глобальные каналы связи, так как вся пропускная способность такой линии всегда находится в распоряжении взаимодействующих сетей. Однако это и наиболее дорогой вид глобальных связей - при наличии N удаленных локальных сетей, которые интенсивно обмениваются данными друг с другом, нужно иметь  $\frac{N \cdot (N-1)}{2}$  выделенных линий.

##### 6.1.1. Выделенные аналоговые линии

Обеспечивают готовый к немедленному использованию коммуникационный канал. Арендуемая телефонная линия быстрее и надежнее, чем коммутируемое соединение, хотя и дороже. Для аналоговых сетей с коммутацией каналов характерна неустойчивость соединения. Каждый сеанс связи полностью зависит от качества каналов, скоммутированных для этого конкретного сеанса. Достоинством сетей с коммутацией каналов является их распространенность.

Недостатком аналоговых телефонных сетей является низкое качество составного канала, которое объясняется использованием телефонных коммутаторов устаревших моделей. На такие коммутаторы сильно воздействуют внешние помехи. Телефонные сети, полностью построенные на цифровых коммутаторах, и сети ЦСИО свободны от многих недостатков традиционных аналоговых телефонных сетей. Они предоставляют пользователям высококачественные линии связи, а время установления соединения в сетях ЦСИО существенно сокращено.

##### 6.1.2. Цифровые выделенные линии

Цифровые выделенные линии образуются путем постоянной коммутации в первичных сетях, работающих на принципе разделения канала во времени — TDM. Существует два поколения технологий первичных цепей — технология псевдосинхронной (почти) цифровой иерархии (PDH) и более поздняя технология синхронная цифровая иерархия (SDH/SONET).

Технология псевдосинхронной цифровой иерархии (PDH). Для реализации цифровых методов передачи, а также для того, чтобы улучшить исчерпавшие себя каналы с частотным уплотнением, разработана аппаратура T1. Цифровой подход позволяет мультиплексировать, передавать и коммутировать данные 24-х абонентов. Преобразование в цифру и обратно осуществляется в мультиплексорах с частотой 8000 Гц и 256 уровнями дискретизации (8 бит). В результате каждый абонентский канал формирует цифровой поток 64 Кбит/с. Для по-

вышения скорости передачи была образована иерархия скоростей. Четыре канала T1 объединяются в канал следующего уровня иерархии T2, передающий со скоростью 6,312 Мбит/с, а семь каналов T2 дают при объединении канал T3, передающий со скоростью 44,746 Мбит/с. Аппаратура T1, T2, T3 может взаимодействовать между собой, образуя иерархическую сеть с магистральными и периферийными каналами трех уровней скоростей. Сети T1 и более скоростные T2 и T3 позволяют передавать не только голос, но и любые данные представленные в цифровой форме: компьютерные данные, видеозображение, факсимильные сообщения и т.п.

Высокоскоростные системы цифровой передачи. Системы SDH/SONET. Система SONET наряду с SDH использует наиболее современные и перспективные процедуры цифровой передачи информации, скорость работы которой практически ничем, кроме пропускной способности каналов связи, не ограничена. В системах типа E или T при повышении скорости сильно усложняются процедуры синхронизации, и поэтому их не используют на скоростях более 150 Мбит/сек. Основная цель — создание технологии, позволяющей передавать трафик всех существующих цифровых каналов по высокоскоростной магистрали на волоконно-оптических кабелях и поддерживающих общепринятую иерархию скоростей PDH.

SONET ориентирован на работу в частных сетях, а SDH — в сетях общего пользования. Это определяется тем, что процедура уплотнения низкоскоростных потоков в единую систему передачи организована в SDH лучше, чем в SONET. Базовой иерархической структурой в SONET является так называемый синхронный транспортный сигнал (STS — Synchronous Transport Signal). STS — это стандартная форма кадров данных систем передачи, причем для разных скоростей эта форма остается постоянной, меняется только ее содержание.

Таблица 6.1

Ступени уплотнения в системе SONET

Уровень уплотнения	Скорость передачи (Мбит/с)
OC-1	51.84
OC-3	155.52
OC-9	466.56
OC-12	622.08
OC-18	933.12
OC-24	1244.16
OC-36	1866.24
OC-48	2488.32
OC-192	9953.28

Базовой скоростью в иерархии SONET является 51.84 Мбит/сек. Кадры, передаваемые с такой скоростью, называются STS-1. Полная иерархия, принятая в SONET, представлена на рисунке 4.8. Технология ATM, опирается на кадры STS-3 или STM-1, т.е. на 155.52 Мбит/сек и на STS-12 или STM-4, т.е. на 622 мбит/сек. Можно заметить, что скорость работы системы STS-n определяется как  $51.84 \cdot n$ .

Таблица 6.2

Спектр скоростей в системе SDH

Уровень SDH	Скорость передачи (Мбит/с)
1	155.520
4	622.080
16	2488.320
64	9900

Кадры данных SDH по-другому также можно назвать STM (Synchronous Transfer Module). Все ступени иерархии SDH имеют точный аналог по скорости в структуре SONET.

## 6.2. Глобальные связи на основе сетей с коммутацией каналов

Сети с использованием коммутации каналов являются широко используемыми, т.к. на них построены телефонные сети. Этим обусловлена низкая стоимость услуг связи.

Телефонные сети делятся на аналоговые и цифровые в зависимости от способа мультиплексирования абонентских каналов. Аналоговыми называют сети, которые принимают данные от абонентов аналоговой формы, то есть от классических аналоговых телефонных аппаратов, а мультиплексирование и коммутацию осуществляют как аналоговыми методами, так и цифровыми. Цифровыми называются сети, в которых на абонентских окончаниях информация представлена в цифровом виде и используются цифровые методы мультиплексирования и коммутации. К телефонным сетям с цифровыми абонентскими окончаниями относятся так называемые службы Switched 56 (коммутируемые каналы 56 Кбит/с) и цифровые сети с интегральными услугами ISDN (Integrated Services Digital Network).

### 6.2.1. Аналоговые телефонные сети

Всемирная сеть, которую использует телефон и которая может быть доступна компьютерам, называется общедоступной коммутируемой телефонной сетью (PSTN). В вычислительной среде ее можно рассматривать как один большой канал связи для ГВС (для передачи речи PSTN предлагает коммутируемые телефонные линии). Изначально PSTN была создана для передачи речи, поэтому она обладает низкой скоростью, а модемы, которые необходимы для связи по коммутируемым аналоговым линиям, также не увеличивают скорость. Со средней пропускной способностью 9600 Кбит/с коммутируемые аналоговые линии, оснащенные модемами, подходят только для пользователя с минимальными требованиями к времени реакции системы. Максимальная на сегодня пропускная способность в 56 Кбит/с достигается только в том случае, если все коммутаторы в сети на пути следования данных являются цифровыми.

Основные характеристики аналоговых телефонных сетей:

- при вызове пользователи получают прямое соединение через коммутаторы в сети. Абонентское окончание 2-проводное;
- вызов абонента может осуществляться двумя способами: с помощью импульсного набора или тонового набора. При импульсном наборе длительность набора зависит от того, какие цифры образуют номер, при тоновом наборе любая цифра передается подачей в сеть двух синусоидальных сигналов разной частоты в течение 50мс. Поэтому набор номера тоновым способом в среднем в 5 раз быстрее, чем импульсный;
- коммутаторы сети не позволяют обеспечить промежуточное хранение данных. Поскольку запоминающие устройства в коммутаторах отсутствуют, возможен отказ в соединении при занятости абонента;
- для передачи дискретных данных по аналоговым коммутируемым сетям используются модемы, поддерживающие процедуру вызова абонента;
- пропускная способность коммутируемого канала заранее неизвестна, так как модемы устанавливают соединение на скорости, подходящей для реального качества канала.

В телефонных коммутаторах аналоговых телефонных сетей могут использоваться два принципа коммутации — аналоговый, основанный на частотном разделении канала (FDM), и цифровой, основанный на разделении канала во времени (TDM).

Для передачи данных по аналоговым коммутируемым телефонным каналам используют модемы, которые поддерживают процедуру автовызова абонента и работают по 2-проводному окончанию. Для передачи данных по коммутируемому каналу разработан ряд основных стандартов, определяющих скорость и метод кодирования сигналов: V.21, V.22, V.22 bis, V.26 ter, V.32, V.32 bis, V.34, V.34+. На практике сегодня в основном применяют модемы, поддерживающие стандарт V.34+, которые могут адаптироваться к качеству линии.

### 6.2.2. Цифровые сети с коммутацией каналов

Цифровые сети с коммутацией каналов представлены двумя технологиями: Switched 56 и ISDN. Switched 56 — это переходная технология, которая основана на предоставлении пользователю 4-проводного цифрового абонентского окончания, но со скоростью 56 Кбит/с. Коммутаторы такой сети работают с использованием цифровой коммутации. Технология Switched 56 обеспечивает соединение компьютеров и локальных сетей со скоростью 56 Кбит/с.

ISDN разработаны для объединения в одной сети различных транспортных и прикладных служб. ISDN предоставляет своим абонентам услуги выделенных каналов, коммутируемых каналов, а также коммутацию пакетов.

### 6.3. Компьютерные глобальные сети с коммутацией пакетов

Сети на основе коммутируемых каналов используют сетевые протоколы IP или IPX поверх физического и канального уровней, которые применялись и для объединения локальных сетей. Однако для глобальных сетей с коммутацией пакетов, таких как X.25, frame relay или ATM, характерна оригинальная техника маршрутизации пакетов, основанная на понятии «виртуальный канал» и обеспечивающая эффективную передачу долговременных устойчивых потоков данных.

Техника виртуальных каналов, используемая во всех территориальных сетях с коммутацией пакетов, кроме TCP/IP, состоит в следующем. Сначала устанавливается виртуальное соединение между абонентами сети — терминалами, маршрутизаторами или компьютерами. Существуют два типа виртуальных соединений — коммутируемый виртуальный канал SVC (Switched Virtual Circuit) и постоянный виртуальный канал PVC (Permanent Virtual Circuit). При создании коммутируемого виртуального канала коммутаторы сети настраиваются на передачу пакетов динамически (по запросу абонента), а создание постоянного виртуального канала происходит заранее путем послышки соответствующих пакетов. При этом маршрутизация пакетов между коммутаторами сети на основании таблиц маршрутизации происходит только один раз — при создании виртуального канала. После создания виртуального канала передача пакетов коммутаторами происходит на основании так называемых номеров или идентификаторов виртуальных каналов (Virtual Channel Identifier, VCI). Каждому виртуальному каналу присваивается значение VCI на этапе создания виртуального канала. Это значение имеет

не глобальный характер, как адрес абонента, а локальный — каждый коммутатор самостоятельно нумерует новый виртуальный канал. Кроме нумерации виртуального канала, каждый коммутатор при создании этого канала автоматически настраивает так называемые таблицы коммутации портов. Эти таблицы описывают, на какой порт нужно передать пришедший пакет, если он имеет определенный номер VCI. После прокладки виртуального канала через сеть коммутаторы больше не используют для пакетов этого соединения таблицу маршрутизации, а продвигают пакеты на основании номеров VCI небольшой разрядности. Сами таблицы коммутации портов также включают обычно меньше записей, чем таблицы маршрутизации, так как хранят данные только о действующих на данный момент соединениях, проходящих через данный порт.

Режим продвижения пакетов на основе готовой таблицы коммутации портов обычно называют не маршрутизацией, а коммутацией и относят не к третьему, а ко второму (канальному) уровню стека протоколов.

### 6.3.1. Сети X.25

#### Назначение и структура сетей X.25

Сети X.25 являются на сегодняшний день самыми распространенными сетями с коммутацией пакетов, используемые для построения корпоративных сетей. Сети X.25 хорошо работают на ненадежных линиях благодаря протоколам с установлением соединения и коррекцией ошибок на двух уровнях — канальном и сетевом.

Сеть X.25 состоит из коммутаторов S (Switches), называемых также центрами коммутации пакетов ЦКП, расположенных в различных географических точках и соединенных высокоскоростными выделенными каналами. Выделенные каналы могут быть как цифровыми, так и аналоговыми.

Поясним структуру сети X.25 по рис. 6.3.

Терминалы (Т) подключаются к сети через устройства PAD. Они могут быть встроенными (PAD2, PAD3) или удаленными (PAD1). Терминалы получают доступ к встроенному устройству PAD по телефонной сети с помощью модемов. Удаленный PAD представляет собой небольшое автономное устройство, подключенное к коммутатору через выделенный канал связи X.25.

К основным функциям PAD относятся:

- сборка символов, полученных от асинхронных терминалов, в пакеты;
- разборка полей данных в пакетах и вывод данных на терминалы;
- управление процедурами установления соединения и разъединения по сети X.25;
- передача символов, включающих старт-стопные сигналы и биты проверки на четность, по требованию асинхронного терминала;
- продвижение пакетов при наличии соответствующих условий, таких, как заполнение пакета, истечение времени ожидания и др.

Стандарт X.28 определяет параметры терминала, а также протокол взаимодействия терминала с устройством PAD. При работе на терминале пользователь проводит некоторый текстовый диалог с устройством PAD, используя стандартный набор символьных команд. PAD может работать с терминалом в управляющем режиме и режиме передачи данных. В управляющем режиме пользователь может указать адрес компьютера, с которым нужно установить соединение по сети X.25. Компьютеры и локальные сети обычно подключаются к сети X.25 непосредственно через адаптер или маршрутизатор, поддерживающий на своих интерфейсах протоколы X.25. Для управления устройствами PAD в сети существует протокол X.29, с помощью которого узел сети может управлять и конфигурировать PAD удаленно по сети. При необходимости передачи данных компьютеры, подключенные к сети X.25, непосредственно услугами PAD не пользуются, а самостоятельно устанавливают виртуальные каналы в сети и передают по ним данные в пакетах X.25.

#### Адресация в сетях X.25

Если сеть не связана с внешним миром, то она может использовать адрес любой длины (в пределах формата поля адреса) и давать адресам произвольные значения. Максимальная длина поля адреса в пакете X.25 составляет 16 байт.

Код идентификации сети		Номер национального терминала (National Terminal Number, NTN)
Страна (3 цифры)	Номер сети X.25 в стране	

Рис. 6.4. Формат адреса X.121

Если сеть X.25 хочет обмениваться данными с другими сетями X.25, то в ней нужно придерживаться адресации стандарта X.121. Адреса X.121 (International Data Numbers, IDN) имеют различную длину, которая может доходить до 14 десятичных знаков. Формат адреса представлен на рисунке 6.4.

#### Стек протоколов сети X.25

Стандарты сетей X.25 описывают три уровня протоколов:

- 1) на физическом уровне определены синхронные интерфейсы X.21 и X.21 bis к оборудованию передачи данных;
- 2) на канальном уровне используется подмножество протоколов HDLC, обеспечивающее возможность автоматической передачи в случае возникновения ошибок в линии;
- 3) на сетевом уровне определен протокол X.25/3 обмена пакетами между оконечным оборудованием и сетью передачи данных.

Протокол физического уровня канала связи не оговорен. Это дает возможность использовать каналы разных стандартов.

На канальном уровне используется протокол LAP-B. По протоколу LAP-B устанавливается соединение между пользовательским оборудованием DTE и коммутатором сети.

Сетевой уровень X.25/3 реализуется с использованием 14 различных типов пакетов, по назначению аналогичных типам кадров протокола LAP-B. Так как LAP-B обеспечивает надежную передачу данных, протокол X.25/3 выполняет функции маршрутизации пакетов, установления и разрыва виртуального канала между конечными абонентами сети и управления потоком пакетов.

После установления соединения на канальном уровне конечный узел должен установить виртуальное соединение с другим конечным узлом сети. Для этого посылается пакет Call Request протокола X.25. Этот пакет принимается коммутатором сети и маршрутизируется на основании таблицы маршрутизации, прокладывая при этом виртуальный канал. Протокол маршрутизации для сетей X.25 не определен. После установления виртуального канала конечные узлы обмениваются пакетами другого формата - формата пакетов данных. Таким образом, коммутатор X.25 принимает кадр LAP-B и отвечает на него другим кадром LAP-B, подтверждающим получение кадра с конкретным номером. При утере или искажении кадра коммутатор организывает повторную передачу кадра. Если же с кадром LAP-B все в порядке, то коммутатор извлекает пакет X.25, на основании номера виртуального канала определяет выходной порт, а затем сформировывает новый кадр LAP-B для дальнейшего продвижения пакета.

Протоколы сетей X.25 были специально разработаны для низкоскоростных линий с высоким уровнем помех. Именно такие линии составляют большую часть телекоммуникационной структуры нашей страны, поэтому сети X.25 будут по-прежнему еще долго являться наиболее рациональным выбором для многих пользователей.

### 6.3.2. Сети frame relay

#### Назначение и общая характеристика

Сети frame relay — сравнительно новые сети, которые гораздо лучше подходят для передачи пульсирующего трафика локальных сетей по сравнению с сетями X.25. Преимущество сетей frame relay заключается в их низкой протокольной избыточности и дейтаграммном режиме работы, что обеспечивает высокую пропускную способность и небольшие задержки кадров. Сети frame relay обеспечивают скорость передачи данных до 2 Мбит/с.

#### Стек протоколов frame relay

Технология frame relay использует для передачи данных технику виртуальных соединений, аналогичную той, которая применялась в сетях X.25, однако стек протоколов frame relay передает кадры по протоколам только физического и канального уровней, в то время как в сетях X.25 и после установления соединения пользовательские данные передаются протоколом 3-го уровня.

Основу технологии составляет протокол LAR-F core, который является весьма упрощенной версией протокола LAR-D. Терминальное оборудование посылает в сеть кадры LAR-F в любой момент времени, считая что виртуальный канал в сети коммутаторов уже проложен. Протокол LAR-F комммутирует кадры с помощью таблиц коммутации портов, в которых используются локальные значения номера виртуального соединения.

В сети frame relay обнаруженные в кадрах искажения не исправляются. Протокол frame relay подразумевает, что конечные узлы будут обнаруживать и корректировать ошибки за счет работы протоколов транспортного или более высоких уровней. В этом отношении технология frame relay близка к технологиям локальных сетей.

Структура кадра протокола LAR-F представлена на рис. 6.5.

Как видно, поле управления отсутствует в структуре кадра LAR-F. Поле номера виртуального соединения состоит из 10 битов. Это позволяет использовать до 1024 виртуальных каналов. Поля EA0 и EA1 предназначены для расширения поля номера виртуального соединения.

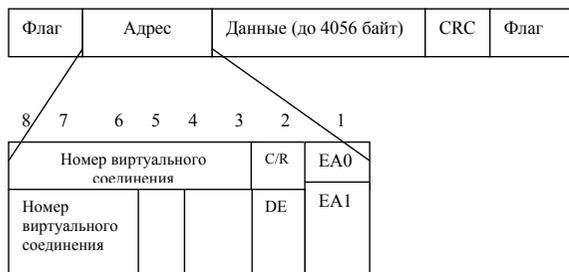


Рис. 6.5. Формат кадра LAR-F

#### **Поддержка качества обслуживания**

Благодаря особому подходу технология frame relay гарантированно обеспечивает основные параметры качества транспортного обслуживания, необходимые при объединении локальных сетей.

Используется процедура заказа качества обслуживания при установлении соединения. Для каждого виртуального соединения определяется несколько параметров, влияющих на качество обслуживания:

- CIR (Committed Information Rate) - согласованная информационная скорость, с которой сеть будет передавать данные пользователя;
- Bc (Committed Burst Size) - согласованный объем пульсации, то есть максимальное количество байтов, которое сеть будет передавать от этого пользователя за интервал времени T;
- Be (Excess Burst Size) - дополнительный объем пульсации, то есть максимальное количество байтов, которое сеть будет пытаться передать сверх установленного значения Bc за интервал времени T.

Основной параметр, по которому абонент и сеть заключают соглашение при установлении виртуального соединения, является CIR. Если пользователь на каком-то промежутке времени T передает в сеть данные со средней скоростью, превосходящей CIR, то кадр подлежит удалению, предварительно пометив кадр признаком DE (Discard Eligibility) равным 1.

Для контроля соглашения о параметрах качества обслуживания все коммутаторы сети frame relay выполняют алгоритм «дырявого ведра». Алгоритм использует счетчик С поступивших байт. Каждые T секунд этот счетчик уменьшается на величину Bc. Все кадры, данные которых не увеличили значение счетчика свыше порога Bc, пропускаются в сеть со значение признака DE=0, другие тоже передаются в сеть, но со значением признака DE=1. Если коммутаторы испытывают перегрузку, кадры помеченные признаком DE=1, удаляются.

Пользователь может договориться о включении не всех параметров качества обслуживания на данном виртуальном канале. Например, можно использовать только параметры CIR и Bc. Этот вариант дает более качественное обслуживание, так как кадры никогда не отбрасываются коммутатором сразу.

## ГЛАВА 7 СЕТЕВЫЕ ОПЕРАЦИОННЫЕ СИСТЕМЫ

Операционная система (ОС) в наибольшей степени определяет облик всей вычислительной системы в целом, выполняя две основные функции:

- 1) обеспечение пользователю-программисту удобств посредством предоставления для него расширенной машины;
- 2) повышение эффективности использования компьютера путем рационального управления его ресурсами.

Операционная система управляет обработкой прерываний, управлением таймерами и оперативной памятью, решает другие низкоуровневые проблемы. Функцией ОС является предоставление пользователю виртуальной машины, работать и программировать с которой удобней, чем непосредственно с аппаратурой, составляющей реальную машину.

ОС — это система, обеспечивающая удобный интерфейс. Современные вычислительные системы состоят из процессоров, памяти, таймеров, дисков, накопителей на магнитных лентах, сетевой коммуникационной аппаратуры. При этом основной функцией ОС является распределение процессоров, памяти, устройств и данных между процессами, конкурирующими за эти ресурсы, и обеспечение максимальной эффективности их функционирования. Управление ресурсами включает решение двух общих, не зависящих от типа ресурса задач:

- планирование ресурса — определение кому, когда и в каком количестве необходимо выделить данный ресурс;

- отслеживание состояния ресурса — то есть поддержание оперативной информации о том, занят или не занят ресурс, а для делимых ресурсов — какое количество ресурса уже распределено, а какое свободно.

Для решения этих общих задач ОС используют различные алгоритмы, определяющие производительность, области применения и даже пользовательский интерфейс. ОС могут различаться особенностями реализации внутренних алгоритмов управления основными ресурсами компьютеров (процессорами, памятью, коммуникационными устройствами), особенностями использованных методов проектирования, типами аппаратных платформ, областями использования и т.д.

### 7.1. Классификация ОС

От эффективности алгоритмов управления локальными ресурсами компьютера во многом зависит эффективность всей сетевой ОС в целом. В зависимости от особенностей использованного алгоритма управления процессором, операционные системы делят на:

- многозадачные и однозадачные,
- многопользовательские и однопользовательские,
- на системы, поддерживающие многопользовательскую обработку и не поддерживающие ее,
- на многопроцессорные и однопроцессорные системы.

Поддержка многозадачности. По числу одновременно выполняемых задач операционные системы могут быть разделены на два класса: однозадачные (например, MS-DOS, MSX) и многозадачные (ОС ЕС, OS/2, UNIX, Windows 9x, 200x).

Однозадачные ОС выполняют функцию предоставления пользователю виртуальной машины, делая более простым и удобным процесс взаимодействия пользователя с компьютером. Однозадачные ОС включают средства управления периферийными устройствами, средства управления файлами, средства общения с пользователем.

Многозадачные ОС, кроме вышеперечисленных функций, управляют разделением совместно используемых ресурсов, таких, как процессор, оперативная память, файлы и внешние устройства.

Поддержка многопользовательского режима. По числу одновременно работающих пользователей ОС делятся на однопользовательские (MS-DOS, Windows 3.x, ранние версии OS/2) и многопользовательские (UNIX, Windows NT).

Главным отличием многопользовательских систем от однопользовательских является наличие средств защиты информации каждого пользователя от несанкционированного доступа других пользователей. Следует заметить, что не всякая многозадачная система является многопользовательской, и не всякая однопользовательская ОС является однозадачной.

Вытесняющая и невытесняющая многозадачность. Важнейшим разделяемым ресурсом является процессорное время. Способ распределения процессорного времени между несколькими одновременно существующими в системе процессами (или нитями) во многом определяет специфику ОС. Среди множества существующих вариантов реализации многозадачности можно выделить две группы алгоритмов: невытесняющей многозадачности (NetWare, Windows 3.x) и вытесняющей многозадачности (Windows NT, OS/2, UNIX).

Основным различием между вытесняющим и невытесняющим вариантами многозадачности является степень централизации механизма планирования процессов. В первом случае механизм планирования процессов целиком сосредоточен в операционной системе, а во втором - распределен между системой и прикладными программами. При невытесняющей многозадачности активный процесс выполняется до тех пор, пока он сам не отдаст управление операционной системе для того, чтобы та выбрала из очереди другой готовый к выполнению

процесс. При вытесняющей многозадачности решение о переключении процессора с одного процесса на другой принимается операционной системой, а не самим активным процессом.

Поддержка многопользовательского режима. Важным свойством операционных систем является возможность распараллеливания вычислений в рамках одной задачи. Многопользовательская ОС разделяет процессорное время не между задачами, а между их отдельными ветвями (нитями).

Многопроцессорная обработка. Другим важным свойством ОС является отсутствие или наличие в ней средств поддержки многопроцессорной обработки - мультипроцессорирование. Такие функции имеются в операционных системах Solaris 2.x фирмы Sun, Open Server 3.x компании Santa Cruz Operations, OS/2 фирмы IBM, Windows NT фирмы Microsoft и NetWare 4.1 фирмы Novell.

Многопроцессорные ОС могут классифицироваться по способу организации вычислительного процесса в системе с многопроцессорной архитектурой: асимметричные ОС и симметричные ОС. Асимметричная ОС целиком выполняется только на одном из процессоров системы, распределяя прикладные задачи по остальным процессорам. Симметричная ОС полностью децентрализована и использует весь пул процессоров, разделяя их между системными и прикладными задачами.

Облик операционной системы в целом и возможности ее использования в той или иной области зависят и от других подсистем управления локальными ресурсами — подсистем управления памятью, файлами, устройствами ввода-вывода.

Специфика сетевых ОС проявляется в реализации сетевых функций: распознавание и перенаправление в сеть запросов к удаленным ресурсам, передача сообщений по сети, выполнение удаленных запросов. При реализации сетевых функций возникают задачи, связанные с распределенным характером хранения и обработки данных в сети: ведение справочной информации о всех доступных в сети ресурсах и серверах, адресация взаимодействующих процессов, обеспечение прозрачности доступа, тиражирование данных, согласование копий, поддержка безопасности данных.

На свойства операционной системы непосредственное влияние оказывают аппаратные средства, на которые она ориентирована. По типу аппаратуры различают операционные системы персональных компьютеров, мини-компьютеров, мейнфреймов, кластеров и сетей ЭВМ. Среди перечисленных типов компьютеров могут встречаться как однопроцессорные варианты, так и многопроцессорные.

Сетевая ОС имеет в своем составе средства передачи сообщений между компьютерами по линиям связи. На основе этих средств сетевая ОС поддерживает разделение ресурсов компьютера между удаленными пользователями, подключенными к сети. Для поддержания функций передачи сообщений сетевые ОС содержат специальные программные компоненты, реализующие популярные коммуникационные протоколы (IP, IPX, Ethernet и другие).

Многопроцессорные системы требуют от операционной системы особой организации, с помощью которой сама операционная система, а также поддерживаемые ею приложения могли бы выполняться параллельно отдельными процессорами системы. Параллельная работа отдельных частей ОС создает дополнительные проблемы, так как в этом случае гораздо сложнее обеспечить согласованный доступ отдельных процессов к общим системным таблицам, исключить эффект гонок и прочие нежелательные последствия асинхронного выполнения работ.

Другие требования предъявляются к операционным системам кластеров. Кластер — слабо связанная совокупность нескольких вычислительных систем, работающих совместно для выполнения общих приложений и представляющихся пользователю единой системой. Наряду со специальной аппаратурой для функционирования кластерных систем необходима и программная поддержка со стороны операционной системы, которая сводится в основном к синхронизации доступа к разделяемым ресурсам, обнаружению отказов и динамической реконфигурации системы.

Наряду с ОС, ориентированными на совершенно определенный тип аппаратной платформы, существуют операционные системы, специально разработанные таким образом, чтобы они могли быть легко перенесены с компьютера одного типа на компьютер другого типа, так называемые *мобильные* ОС. Наиболее ярким примером такой ОС является популярная система UNIX. В этих системах аппаратно-зависимые места тщательно локализованы, так что при переносе системы на новую платформу переписывают только их. Средством, облегчающим перенос остальной части ОС, является написание ее на машинно-независимом языке, например, на «С», который и был разработан для программирования операционных систем.

Многозадачные ОС подразделяются на три типа в соответствии с использованными при их разработке критериями эффективности:

- 1) системы пакетной обработки (например, ОС ЕС),
- 2) системы разделения времени (UNIX, VMS),
- 3) системы реального времени (QNX, RT/11).

Системы пакетной обработки предназначались для решения задач в основном вычислительного характера, не требующих быстрого получения результатов. Главной целью и критерием эффективности систем пакетной обработки является максимальная пропускная способность, то есть решение максимального числа задач в единицу времени. Для достижения этой цели используется следующая схема функционирования. В начале работы формируется пакет заданий, каждое задание содержит требование к системным ресурсам. Из этого пакета заданий формируется мультипрограммная смесь, то есть множество одновременно выполняемых задач. Для одновременного выполнения выбираются задачи, предъявляющие отличающиеся требования к ресурсам, так, чтобы обеспечивалась сбалансированная загрузка всех устройств вычислительной машины. Так, например, в мульти-

программной смеси желательное одновременное присутствие вычислительных задач и задач с интенсивным вводом-выводом. В системах пакетной обработки переключение процессора с выполнения одной задачи на выполнение другой происходит только в случае, если активная задача сама отказывается от процессора (например, из-за необходимости выполнить операцию ввода-вывода). Поэтому одна задача может надолго занять процессор, что делает невозможным выполнение интерактивных задач. Таким образом, взаимодействие пользователя с вычислительной машиной, на которой установлена система пакетной обработки, сводится к тому, что пользователь приносит задание, отдает его диспетчеру-оператору, а в конце дня (после выполнения всего пакета заданий) получает результат.

В системы с разделением времени каждому пользователю предоставляется терминал, с которого он может вести диалог со своей программой. Каждой задаче выделяется только квант процессорного времени, ни одна задача не занимает процессор надолго, и время ответа оказывается приемлемым. Если квант выбран достаточно небольшим, то у всех пользователей, одновременно работающих на одной и той же машине, складывается впечатление, что каждый из них единолично использует машину. Системы разделения времени обладают меньшей пропускной способностью, чем системы пакетной обработки, так как на выполнение принимается каждая запущенная пользователем задача, а не та, которая «выгодна» системе. Кроме того, имеются накладные расходы вычислительной мощности на более частое переключение процессора с задачи на задачу. Критерием эффективности систем разделения времени является не максимальная пропускная способность, а удобство и эффективность работы пользователя.

Системы реального времени применяются для управления различными техническими объектами (например, станком, спутником, научной экспериментальной установкой или технологическими процессами — гальванической линией, доменным процессом и т.п. Во всех этих случаях существует предельно допустимое время, в течение которого должна быть выполнена та или иная программа, управляющая объектом. В противном случае может произойти авария: спутник выйдет из зоны видимости, экспериментальные данные, поступающие с датчиков, будут потеряны, толщина гальванического покрытия не будет соответствовать норме. Таким образом, критерием эффективности для систем реального времени является их способность выдерживать заранее заданные интервалы времени между запуском программы и получением результата (управляющего воздействия). Для этих систем мультипрограммная смесь представляет собой фиксированный набор заранее разработанных программ, а выбор программы на выполнение осуществляется, исходя из текущего состояния объекта или в соответствии с расписанием плановых работ.

Некоторые операционные системы могут совмещать в себе свойства систем разных типов, например, одна часть задач может выполняться в режиме пакетной обработки, другая — в режиме реального времени или в режиме разделения времени. В таких случаях режим пакетной обработки часто называют фоновым режимом.

## 7.2. Особенности методов построения

При описании операционной системы часто указываются особенности ее структурной организации и основные концепции, положенные в ее основу.

К таким базовым концепциям относятся:

- способ построения ядра системы — монолитное ядро или микроядерный подход. Большинство ОС использует монолитное ядро, которое компонуется как одна программа, работающая в привилегированном режиме и использующая быстрые переходы с одной процедуры на другую, не требующие переключения из привилегированного режима в пользовательский и наоборот;

- альтернативой является построение ОС на базе микроядра, работающего также в привилегированном режиме и выполняющего только минимум функций по управлению аппаратурой, в то время как функции ОС более высокого уровня выполняют специализированные компоненты ОС — серверы, работающие в пользовательском режиме. При таком построении ОС работает более медленно, так как часто выполняются переходы между привилегированным режимом и пользовательским, но система получается более гибкой — ее функции можно наращивать, модифицировать или сужать, добавляя, изменяя или исключая серверы пользовательского режима. Кроме того, серверы хорошо защищены друг от друга, как и любые пользовательские процессы;

- построение ОС на базе объектно-ориентированного подхода дает возможность использовать все его достоинства, хорошо зарекомендовавшие себя на уровне приложений, внутри операционной системы. А именно:

- аккумуляцию удачных решений в форме стандартных объектов;
- возможность создания новых объектов на базе имеющихся с помощью механизма наследования;
- хорошую защиту данных за счет их инкапсуляции во внутренние структуры объекта, что делает данные недоступными для несанкционированного использования извне;
- структурированность системы, состоящей из набора хорошо определенных объектов.

- наличие нескольких прикладных сред дает возможность в рамках одной ОС одновременно выполнять приложения, разработанные для нескольких ОС. Многие современные операционные системы поддерживают одновременно прикладные среды MS-DOS, Windows, UNIX (POSIX), OS/2. Концепция множественных прикладных сред наиболее просто реализуется в ОС на базе микроядра, над которым работают различные серверы, реализующие прикладную среду той или иной операционной системы;

- распределенная организация операционной системы позволяет упростить работу пользователей и программистов в сетевых средах. В распределенной ОС реализованы механизмы, которые дают возможность пользователю представлять и воспринимать сеть в виде традиционного однопроцессорного компьютера. Характерными признаками распределенной организации ОС являются: наличие единой справочной службы разделяемых ресурсов, единой службы времени, использование механизма вызова удаленных процедур (RPC) для прозрачного распределения программных процедур по машинам, многократной обработки, позволяющей распараллеливать вычисления в рамках одной задачи и выполнять эту задачу сразу на нескольких компьютерах сети и т.д.

## 7.3. Организация структур операционных систем

Для удовлетворения требований, предъявляемых к современной ОС, большое значение имеет ее структурное построение. Операционные системы прошли длительный путь развития от монолитных систем к хорошо структурированным модульным системам, способным к системному развитию, расширению и легкому переносу на новые платформы.

### 7.3.1 Монолитные структуры

В общем случае структура монолитной системы представляет собой отсутствие структуры (рис. 7.1). ОС написана как набор процедур, каждая из которых может вызывать другие, когда ей это нужно. При использовании этой техники каждая процедура системы имеет хорошо определенный интерфейс в терминах параметров и результатов и может вызвать любую другую для выполнения нужной для нее работы.

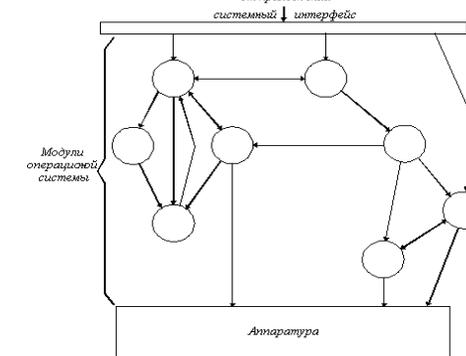


Рис. 7.1. Монолитная структура ОС

Для построения монолитной системы необходимо скомпилировать все отдельные процедуры, а затем связать их вместе в единый объектный файл с помощью компоновщика (примерами могут служить ранние версии ядра UNIX или Novell NetWare). Каждая процедура видит любую другую процедуру (в отличие от структуры, содержащей модули, в которой большая часть информации является локальной для модуля, и процедуры модуля можно вызвать только через специально определенные точки входа).

Однако, даже такие монолитные системы могут быть немного структурированными. При обращении к системным вызовам, поддерживаемым ОС, параметры помещаются в строго определенные места, такие, как регистры или стек, а затем выполняется специальная команда прерывания, известная как вызов ядра или вызов супервизора. Эта команда переключает машину из режима пользователя в режим ядра, называемый также режимом супервизора, и передает управление ОС. ОС проверяет параметры вызова для того, чтобы определить, какой системный вызов должен быть выполнен. После этого ОС индексирует таблицу, содержащую ссылки на процедуры, и вызывает соответствующую процедуру. Такая организация ОС предполагает следующую структуру:

- главная программа, которая вызывает требуемые сервисные процедуры;
- набор сервисных процедур, реализующих системные вызовы;
- набор утилит, обслуживающих сервисные процедуры.

В этой модели для каждого системного вызова имеется одна сервисная процедура. Утилиты выполняют функции, которые нужны нескольким сервисным процедурам. Это деление процедур на три слоя показано на рисунке 7.2.

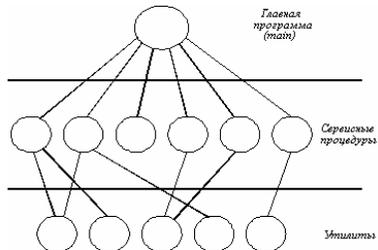


Рис. 7.2. Простая структуризация монолитной ОС

Обобщением предыдущего подхода является организация ОС как иерархии уровней (многоуровневые системы). Уровни образуются группами функций операционной системы — файловая система, управление процессами и устройствами и т.п. Каждый уровень может взаимодействовать только со своим непосредственным соседом - выше- или нижележащим уровнем. Прикладные программы или модули самой операционной системы передают запросы вверх и вниз по этим уровням. Многоуровневый подход был использован при реализации различных вариантов ОС UNIX.

У монолитного варианта построения имеются недостатки. В системах, имеющих многоуровневую структуру, было нелегко удалить один слой и заменить его другим в силу множественности и размытости интерфейсов между слоями. Добавление новых функций и изменение существующих требовало хорошего знания операционной системы и массы времени.

### 7.3.2. Модель клиент-сервер

Операционные системы должны иметь возможности развития и расширения, поэтому более предпочтительной оказалась модель клиент-сервер и концепция микроядра.

Модель клиент-сервер и микроядра — это современный подход к структурированию ОС. Модель клиент-сервер предполагает наличие потребителя какого-либо сервиса — клиента и поставщика этого сервиса — сервера. Эта модель успешно применяется при построении сетевых операционных систем.

Суть построения структуры ОС в разбиении ее на несколько процессов - серверов, каждый из которых выполняет отдельный набор сервисных функций (например, управление памятью, создание или планирование процессов). Каждый сервер выполняется в пользовательском режиме. Клиентом может быть либо другой компонент ОС, либо прикладная программа. Клиент запрашивает сервис, посылая сообщение на сервер. Ядро ОС (называемое здесь микроядром), работая в привилегированном режиме, доставляет сообщение нужному серверу. Сервер выполняет операцию, после чего ядро возвращает результаты клиенту с помощью другого сообщения (рис. 7.3).

Различные варианты реализации модели клиент-сервер в структуре ОС могут существенно различаться по объему работ, выполняемых в режиме ядра.

Микроядро реализует жизненно важные функции, лежащие в основе операционной системы. Это основа для менее существенных системных служб и приложений. Главный принцип разделения работы между микроядром и окружающими его модулями — включать в микроядро только те функции, которым абсолютно должны исполняться в режиме супервизора и в привилегированном пространстве. Под этим обычно подразумеваются машинно-зависимые программы (включая поддержку нескольких процессоров), некоторые функции управления процессами, обработка прерываний, поддержка пересылки сообщений, некоторые функции управления устройствами ввода-вывода, связанные с загрузкой команд в регистры устройств. Эти функции операционной системы трудно, если не невозможно, выполнить программам, работающим в пространстве пользователя.

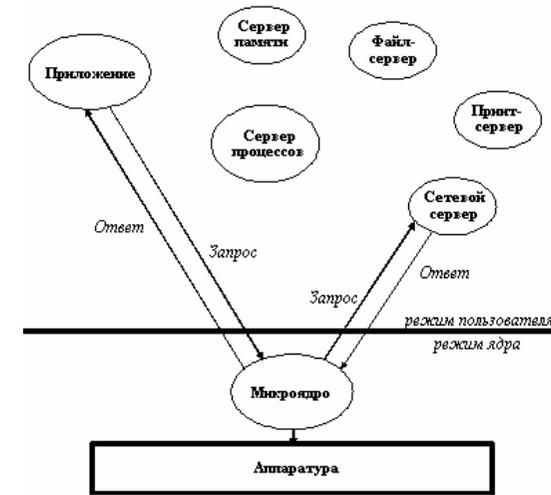


Рис. 7.3. Структура ОС клиент-сервер

Управление памятью может распределяться между микроядром и сервером, работающим в пользовательском режиме. Драйверы устройств также могут располагаться как внутри ядра, так и вне его. При размещении драйверов устройств вне микроядра для обеспечения возможности разрешения и запрещения прерываний, часть программы драйвера должна исполняться в пространстве ядра. Отделение драйверов устройств от ядра делает возможной динамическую конфигурацию ОС, оптимизацию доступа СУБД к диску, обеспечение переносимости системы. В настоящее время именно операционные системы, построенные с использованием модели клиент-сервер и концепции микроядра, в наибольшей степени удовлетворяют требованиям, предъявляемым к современным ОС.

Высокая степень переносимости обусловлена тем, что весь машинно-зависимый код изолирован в микроядре, поэтому для переноса системы на новый процессор требуется меньше изменений. К тому же все они логически сгруппированы вместе.

Использование модели клиент-сервер повышает надежность. Каждый сервер выполняется в виде отдельного процесса в своей собственной области памяти, и, таким образом, защищен от других процессов. Более того, поскольку серверы выполняются в пространстве пользователя, они не имеют непосредственного доступа к аппаратуре и не могут модифицировать память, в которой хранится управляющая программа.

Эта модель хорошо подходит для распределенных вычислений, так как отдельные серверы могут работать на разных процессорах мультипроцессорного компьютера или даже на разных компьютерах. При получении от процесса сообщения микроядро может обработать его самостоятельно или переслать другому процессу. Пересылка сообщений осуществляется быстро благодаря операционной системе на основе микроядра.

### 7.4. Обзор сетевых операционных систем

Большое разнообразие типов компьютеров, используемых в вычислительных сетях, влечет за собой разнообразие операционных систем: для рабочих станций, для серверов сетей уровня отдела и серверов уровня предприятия в целом. К ним могут предъявляться различные требования по производительности и функциональным возможностям. Желательно, чтобы они обладали свойством совместимости, которое позволило бы обеспечить совместную работу различных ОС.

Сетевые ОС делятся на две группы: масштаба отдела и масштаба предприятия. ОС для отделов или рабочих групп обеспечивают набор сетевых сервисов, включая разделение файлов, приложений и принтеров. Они должны обеспечивать свойства отказоустойчивости, например, работать с RAID-массивами, поддерживать кластерные архитектуры. Сетевые ОС отделов обычно более просты в установке и управлении по сравнению с сетевыми ОС предприятия. У них меньше функциональных свойств, они меньше защищают данные и имеют более слабые возможности по взаимодействию с другими типами сетей, а также худшую производительность.

Сетевая операционная система масштаба предприятия прежде всего должна обладать основными свойствами любых корпоративных продуктов, в том числе:

- масштабируемостью, то есть способностью одинаково хорошо работать в широком диапазоне различных количественных характеристик сети;

- совместимостью с другими продуктами, то есть способностью работать в сложной гетерогенной среде интернета в режиме plug-and-play.

Корпоративная сетевая ОС должна поддерживать более сложные сервисы. Подобно сетевой ОС рабочих групп, сетевая ОС масштаба предприятия должна позволять пользователям разделять файлы, приложения и принтеры, причем делать это для большего количества пользователей и объема данных и с более высокой производительностью. Кроме того, сетевая ОС масштаба предприятия обеспечивает возможность соединения разнородных систем — как рабочих станций, так и серверов. Например, даже если ОС работает на платформе Intel, она должна поддерживать рабочие станции UNIX, работающие на RISC-платформах. Аналогично, серверная ОС, работающая на RISC-компьютере, должна поддерживать DOS, Windows и OS/2. Сетевая ОС масштаба предприятия должна поддерживать несколько стеков протоколов (TCP/IP, IPX/SPX, NetBIOS, DECnet и OSI), обеспечивая простой доступ к удаленным ресурсам, удобные процедуры управления сервисами, включая агентов для систем управления сетью.

Важным элементом сетевой ОС масштаба предприятия является централизованная справочная служба, в которой хранятся данные о пользователях и разделяемых ресурсах сети. Такая служба, называемая также службой каталогов, обеспечивает единый логический вход пользователя в сеть и предоставляет ему удобные средства просмотра всех доступных ему ресурсов. При наличии в сети централизованной справочной службы, администратор избавлен от необходимости заводить на каждом сервере повторяющийся список пользователей, а значит избавлен от большого количества рутинной работы и от потенциальных ошибок при определении состава пользователей и их прав на каждом сервере.

Важным свойством справочной службы является ее масштабируемость, обеспечиваемая распределенностью базы данных о пользователях и ресурсах.

Такие сетевые ОС, как Banyan Vines, Novell NetWare 4.x, IBM LAN Server, Sun NFS, Microsoft LAN Manager и Windows NT Server, могут служить в качестве операционной системы предприятия, в то время как ОС NetWare 3.x, Personal Ware, Artisoft LANtastic больше подходят для небольших рабочих групп.

Критериями для выбора ОС масштаба предприятия являются следующие характеристики:

- органичная поддержка многосерверной сети;
- высокая эффективность файловых операций;
- возможность эффективной интеграции с другими ОС;
- наличие централизованной масштабируемой справочной службы;
- хорошие перспективы развития;
- эффективная работа удаленных пользователей;
- разнообразные сервисы: файл-сервис, принт-сервис, безопасность данных и отказоустойчивость, архивирование данных, служба обмена сообщениями, разнообразные базы данных и другие;
- разнообразные программно-аппаратные хост-платформы: IBM SNA, DEC NSA, UNIX;
- разнообразные транспортные протоколы: TCP/IP, IPX/SPX, NetBIOS, AppleTalk;
- поддержка многообразных операционных систем конечных пользователей: DOS, UNIX, OS/2, Mac;
- поддержка сетевого оборудования стандартов Ethernet, Token Ring, FDDI, ARCnet;
- наличие популярных прикладных интерфейсов и механизмов вызова удаленных процедур RPC;
- возможность взаимодействия с системой контроля и управления сетью, поддержка стандартов управления сетью SNMP.

Конечно, ни одна из существующих сетевых ОС не отвечает в полном объеме перечисленным требованиям, поэтому выбор сетевой ОС, как правило, осуществляется с учетом производственной ситуации и опыта.

## ГЛАВА 8 СЕТИ ИНТЕГРАЛЬНОГО ОБСЛУЖИВАНИЯ ЦСИО (ISDN)

По мере развития систем связи постоянно растет число служб, предоставляющих своим абонентам широкий набор услуг, начиная от простой телефонной связи и заканчивая сложными системами передачи данных. При этом все службы работают в отрыве друг от друга, что предполагает наличие у пользователя для каждой абонируемой им службы собственного терминального оборудования. Если на одном компьютере установлено несколько абонентских мест различных служб (например, факс-плата, терминал передачи данных, терминал видеотекста и т. д.), тем не менее работа с ними идет строго по очереди. Совместная работа систем для речи, данных и изображений возможна лишь в исключительных случаях, поскольку оконечные установки, процессы доступа и управления связью различны и специфически приспособлены для решения конкретной задачи. Наилучшими вариантами для передачи всех видов информации являются цифровые системы.

С помощью такой единой сети достигаются две цели: интеграции аппаратуры ДТЕ и ДСЕ в цифровом варианте и интеграции служб обеспечения передачи разнородной информации. Последовательное достижение этих двух целей становится возможным в концепции цифровой сети интегрального обслуживания ЦСИО (ISDN).

Цифровой сетью называют сеть электросвязи, в которой информация передается (по абонентским и соединительным линиям) и коммутируется (на станциях и узлах) в цифровой форме.

Цифровой сетью интегрального обслуживания называют такую цифровую сеть, которая поддерживает множество служб электросвязи.

Под интеграцией обслуживания понимают объединение нескольких служб (речи, данных, изображений и др.), поддерживаемых одной сетью.

### 8.1. Особенности ЦСИО

Основными свойствами ЦСИО являются:

- возможность передачи информации в цифровой форме от одного терминала до другого;
- предоставление широкого спектра услуг, включающего передачу речевой и неречевой информации;
- возможность подключения разнообразных терминалов к сети с помощью многоцелевых стандартных согласующих устройств пользователь – сеть;
- обеспечение централизованной сигнализации с высокой скоростью и верностью;
- обеспечение любого из требуемых способов коммутации: каналов или пакетов;
- обеспечение цифрового транспортного соединения между терминалами оконечных абонентских пунктов;
- предоставление пользователям доступа к большому числу речевых и неречевых служб через общую абонентскую линию;
- предоставление пользователям доступа к сети через небольшое число стандартных многоцелевых интерфейсов.

Различают три условия интеграции цифровых сетей:

- элементной базы (использование однотипных компонентов в аппаратных средствах управления, коммутации и каналообразования);
- способов разделения каналов (временное разделение) в коммутационном и каналообразующем оборудовании;
- служб электросвязи.

### 8.2. Требования, предъявляемые к ЦСИО

Цифровая сеть интегрального обслуживания должна обеспечивать следующие требования:

- установление связи различных служб к одному абоненту по одной абонентской линии, имеющей один номер;
- передачу любого вида информации (представленной изначально в аналоговой или дискретной форме) с помощью одного многофункционального терминала;
- возможность одновременно передавать информацию различных видов;
- снижение тарифов за услуги электросвязи;
- улучшение качества передачи информации (по сравнению с качеством передачи на существующих сетях);
- более эффективное использование каналов и линий сети;
- возможность передачи информации с помощью старт-стопных, синхронных и пакетных установок;
- установление соединения для передачи данных (в режиме коммутации каналов) не более чем за 1 с;
- доставку сообщения не более чем за 10 мс;
- разъединение соединения не более чем за 10 мс;
- возможность расширения обслуживания на подвижные объекты;
- возможность расширения служб и ввода новых видов информации;

- коэффициент ошибок не должен превышать  $10^{-6}$ ;
  - предоставление по требованию пользователя широкого круга дополнительных видов обслуживания (например, прямой вызов, многоадресный вызов и др.);
  - передача абоненту любых необходимых сигналов, оповещающих его о фазе соединения или об отклонении от нормы процессов установления соединения.
- Узкополосные ЦСИО, обладающие перечисленными свойствами, имеют следующие достоинства:
- высокая скорость передачи информации (до 64 Кбит/с);
  - предоставление абонентам возможности пользоваться многофункциональным терминалом, подключенным к одной линии и имеющим один номер для входящего вызова;
  - возможность передачи информации в цифровой форме между двумя абонентскими пунктами (терминалами);
  - наличие системы сигнализации №7 с коммутацией пакетов, обеспечивающей эффективное использование средств связи;
  - возможность выбора одного из способов коммутации на станциях ЦСИО;
  - совместимость с существующими сетями;
  - адаптируемость терминалов для передачи информации различными способами.

### 8.3. Структура и функции ЦСИО

На рис. 8.1 приведена схема первой ISDN в виде телефонной сети, при этом цифровой поток не доводится до абонентского пункта. Сеть поддерживает два вида служб: телефонную и ПД. Для каждого вида служб необходим свой интерфейс с сетью.

Основу ЦСИО образуют компоненты телефонной сети. Особенностью ЦСИО, отличающей ее от цифровых телефонных сетей, является то, что все сообщения передаются в цифровом виде, в том числе и по абонентским линиям. В обычной цифровой сети сообщения на вход станции коммутации подаются в аналоговом виде, где и происходит преобразование в цифровой сигнал. С использованием соответствующих методов передачи по двухпроводной медной абонентской линии (АЛ) можно передать требуемый для основного абонентского окончания сигнал со скоростью 144 Кбит/с. При этом, как правило, не требуется никаких дополнительных расходов.

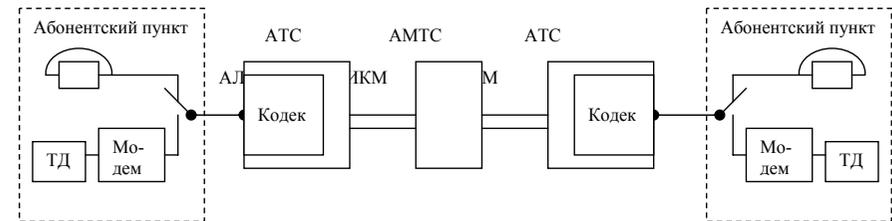


Рис. 8.1. Структурная схема телефонной сети

Служба телефонной связи обслуживает речевой трафик. Особенность его состоит в том, что информация передается по каналу в одном направлении в любой момент времени. При передаче речевой информации недопустимы задержки, превышающие 25 мс. Положительная черта речевого графика — его относительная устойчивость к потере части сообщения при передаче по сети.

Особенность трафика данных состоит в малой чувствительности к абсолютной величине задержки и в большой чувствительности к потере части сообщения из-за блокировок сети.

### 8.4. Службы ЦСИО

Архитектура сети ЦСИО предусматривает несколько видов служб (рис. 8.2):

- некоммутируемые средства (выделенные цифровые каналы);
- коммутируемая телефонная сеть общего пользования;
- сеть передачи данных с коммутацией каналов;
- сеть передачи данных с коммутацией пакетов;
- сеть передачи данных с трансляцией кадров (frame relay);
- средства контроля и управления работой сети.

Транспортные службы сетей ISDN покрывают очень широкий спектр услуг. Большое внимание уделено средствам контроля сети, позволяющим маршрутизировать вызовы для установления соединения с абонентом сети, а также осуществлять мониторинг и управление сетью.

К службам, предоставляющим услуги, относятся: диалоговые службы, службы с накоплением и службы по запросу.

Диалоговые службы обеспечивают прямую передачу информации в реальном масштабе времени между пользователями или между пользователем и ЭВМ. Этот поток может направляться в обе стороны, быть симметричным или несимметричным. Примером диалоговой службы является телефонная, служба речевой конференц-связи, телетекста, телекса, передачи данных, служба передачи изображений, служба безопасности. Служба передачи подвижных изображений на скорости 64-х Кбит/с представляет услугу видеотелефона или видеоконференции. К службам безопасности причисляются службы тревоги и экстренного вызова при пожаре, несчастном случае и т.д. Службы с накоплением предназначаются для не прямой связи между пользователями с помощью промежуточного хранения сообщений (электронная почта).

Службы по запросу дают возможность пользователю извлекать информацию из банков данных и функционируют по его требованию и в заданный момент времени (видеотекст).

### 8.5. Пользовательские интерфейсы ЦСИО

Базовый принцип ЦСИО — это предоставление пользователю стандартного интерфейса для запроса у сети разнообразных услуг, который образуется между двумя типами оборудования, устанавливаемого в помещении пользователя, терминальным оборудованием пользователя ТЕ (компьютер с соответствующим адаптером, маршрутизатор, телефонный аппарат) и сетевым окончателем NT, которое представляет собой устройство, завершающее канал связи с ближайшим коммутатором ЦСИО.

Пользовательский интерфейс основан на каналах трех типов:

В – со скоростью передачи данных 64 Кбит/с;

D – со скоростью передачи данных 16 или 64 Кбит/с;

H – со скоростью передачи данных 384 Кбит/с (H0), 1536 Кбит/с (H1) или 1920 Кбит/с (H2).

При передаче каждому каналу отводится свой квант времени (TDM). Различные типы каналов ЦСИО перечислены в табл. 8.1.

#### D-канал

D-каналы используются в основном для передачи сигналов между пользователем ЦСИО и самой сетью ЦСИО. В различных пользовательских устройствах ЦСИО (телефонах, факсимильных аппаратах и компьютерах) применяются разные способы соединения с ЦСИО, но все они работают с помощью общего протокола передачи и приема сигналов из сети, используя для коммуникаций D-канал.

Таблица 8.1

Типы каналов ЦСИО

Абонентское окончание	Основное	С первичной скоростью	
		1984 Кбит/с	1536 Кбит/с
Реальная скорость цифрового потока	144 Кбит/с	1984 Кбит/с	1536 Кбит/с
В-канальная структура	$V + V + D_{16}$	$30V + D_{64}$ 30B	$23V + D_{64}$ 24B <sup>1</sup>
H0-канальная структура	–	$5H0 + D_{64}$ 5H0	$3H0 + D_{64}$ 4H0 <sup>1</sup>
H1-канальная структура	–	$H12 + D_{64}$ H12 <sup>1</sup>	– H11 <sup>1</sup>
Комбинированная структура	–	$nB + mH0 + D_{64}$ $nB + mH0$	$nB + mH0 + D_{64}$ $nB + mH0$

В каждый момент времени передача сигналов данных не занимает всей полосы частот, предусмотренной для D-канала, поэтому возможно вторичное использование этого канала для передачи в сетях с коммутацией пакетов (сети IP, X.25).

В зависимости от типа предоставляемого пользователю интерфейса D-канал может иметь скорость передачи данных 16 или 64 Кбит/с.

#### V-канал

V-канал ЦСИО применяется для передачи пользовательской информации: оцифрованная речь, звук, видео, двоичные данные. Это основной пользовательский канал передачи, описываемый в стандартах ЦСИО. Для него определена скорость передачи данных 64 Кбит/с, соответствующая полосе частот, которая необходима для эффективного обмена оцифрованной речью за установленное этими стандартами время. V-каналы обслуживают соединения с коммутацией каналов, коммутацией пакетов или полупостоянные соединения (эквивалент выделенной линии в ЦСИО).

#### H-канал

Применяется для обеспечения пользовательских приложений, требующих большой пропускной способности. Для видеоконференций необходима высокоскоростная передача данных и мультиплексирование большого числа каналов с низкой скоростью передачи (в сумме требуется более 64 Кбит/с).

Канал H0 является логической группой из шести V-каналов с общей скоростью передачи данных 384 Кбит/с. Канал H1 состоит из всех доступных каналов H0 в одном пользовательском интерфейсе, в котором задействована линия T1 (23 V-канала с общей скоростью 1472 Кбит/с плюс D-канал 64 Кбит/с). Канал H1 эквивалентен четырем каналам H0 и имеет совокупную пропускную способность 1536 Мбит/с.

Стандарты широкополосной ISDN (B-ISDN) допускают скорость передачи данных порядка 600 Мбит/с. B-ISDN представляет сеть, ориентированную на службы для передачи мультимедийной информации, интегрируя данные разных типов. Службы B-ISDN сгруппированы в слабо связанные коммуникационные службы (communications services), аналогичные традиционным телефонным службам, и в службы обобщения (conversational services), обеспечивающие пользователям ISDN двухстороннюю сквозную пересылку информации для приложений, подобных видеоконференциям, или для высокоскоростной пересылки данных. ISDN поддерживается двумя типами пользовательских интерфейсов: начальный (Basic Rate Interface, BRI) и основной (Primary Rate Interface, PRI).

#### Начальный интерфейс BRI

Начальный интерфейс BRI предоставляет пользователю два канала по 64 Кбит/с для передачи данных (каналы типа V) и один канал с пропускной способностью 16 Кбит/с для передачи управляющей информации (канал типа D). Все каналы работают в полнодуплексном режиме. Суммарная скорость интерфейса BRI для пользовательских данных составляет 144 Кбит/с по каждому направлению, а с учетом служебной информации — 192 Кбит/с. Различные каналы пользовательского интерфейса разделяют один и тот же физический двухпроводный кабель по технологии TDM, то есть являются логическими каналами, а не физическими. Данные по интерфейсу BRI передаются кадрами, состоящими из 48 бит. Каждый кадр содержит по 2 байта каждого из V-каналов, а также 4 бита канала D. Передача кадра длится 250 мс, что обеспечивает скорость данных 64 Кбит/с для каналов V и 16 Кбит/с для канала D. Кроме битов данных кадр содержит служебные биты для обеспечения синхронизации кадров, а также обеспечения нулевой постоянной составляющей электрического сигнала. Интерфейс BRI может поддерживать не только схему 2B+D, но и V+D и просто D (когда пользователь направляет в сеть только пакетизированные данные). Начальный интерфейс стандартизован в рекомендации I.430.

#### Основной интерфейс PRI

Основной интерфейс PRI предназначен для пользователей с повышенными требованиями к пропускной способности сети. Интерфейс PRI поддерживает либо схему 30B+D, либо схему 23B+D. В обеих схемах канал D обеспечивает скорость 64 Кбит/с.

Возможны варианты интерфейса PRI с меньшим количеством каналов типа V, например 20B+D. Каналы типа V могут объединяться в один логический высокоскоростной канал с общей скоростью до 1920 Кбит/с. Основной интерфейс может быть основан на каналах типа H. При этом общая пропускная способность интерфейса все равно не должна превышать 2,048 или 1,544 Мбит/с.

Абоненты сервиса BRI могут пользоваться интерфейсами типа U, S или T. U-интерфейс – одна витая пара, проложенная от абонента к коммутатору, обеспечивающая полный дуплекс. К U-интерфейсу может подключаться только одно устройство, называемое NT-1. Устройство NT-1 может быть и довольно простым преобразователем двухпроводного U-интерфейса в четырехпроводной S/T-интерфейс с раздельными парами для приема и передачи. Интерфейс S/T является шиной, допускающей подключение до семи устройств. U-интерфейс предоставляется конечным пользователям только в США. Конечное устройство со встроенным U-интерфейсом дешевле, чем комплект преобразователя U-S/T и устройства S/T, однако, эти устройства полностью занимают линию ISDN. В других странах конечному пользователю предоставляется S/T-интерфейс, а устройство NT-1, устанавливаемое на территории пользователя, принадлежит провайдеру и часто соединяется с базовой сетью оптоволоконной линией связи.

Устройства ISDN подключаются через NT-2, преобразующее интерфейс S в T. NT-2, поддерживающее второй и третий уровни протокола ISDN, входит в состав всех устройств. К шине S/T или S могут подключаться ISDN-устройства разных типов: телефоны, факсы, оборудование видеоконференцсвязи, мосты/маршрутизаторы, терминальные адаптеры. Эти устройства обозначаются как TE1. Другие коммуникационные устройства с традиционным аналоговым телефонным интерфейсом (POTS, PTSN, R-интерфейс), не поддерживающие ISDN, - аналоговые телефоны, факсы и модемы – обозначаются как TE2. Они могут подключаться к шине S/T через терминальный адаптер TA — отдельное устройство.

Коммутатор ISDN имеет два типа интерфейсов:

- U-интерфейсы линейных окончаний (Line Termination, LT function), обращенные к пользователям;
- V-интерфейс для соединения с другими коммутаторами (Exchange Termination, ET function). Этот интерфейс интересен только владельцу сети (провайдера услуг) ISDN и далее не рассматривается.

Пользователь от провайдера (телефонной компании) получает один из интерфейсов, приведенных в таблице 8.2.

Таблица 8.2

## Информационные характеристики интерфейсов ISDN

Интерфейс	BRI U-интерфейс	BRI S-интерфейс	T1 PRI (США, Япония)	E1 PRI (Европа и др.)
В-каналы	2x64Кбит/с	2x64Кбит/с	23x64Кбит/с	30x64Кбит/с
Д-каналы	1x16Кбит/с	1x16Кбит/с	1x64Кбит/с	1x64Кбит/с
Синхронизация	16Кбит/с	48Кбит/с	8Кбит/с	64Кбит/с
Суммарный поток	160Кбит/с	192Кбит/с	1544Кбит/с	2048Кбит/с
Кодирование	2B1Q/4B3T	ASI (MAMI)	AMI/B8ZS	HDB3

U- и S-интерфейсы рассмотрим подробнее.

### U-интерфейсы BRI

На физическом уровне U-интерфейс, обеспечивающий сервис BRI, представляет собой одну пару проводов со скоростью передачи 160кбит/с. Для уменьшения шумов используется подавление эхоотражений. В разных странах применяются разные схемы кодирования: 2B1Q – в США, 4B3T – в Европе.

При кодировании 2B1Q каждая пара бит кодируется одним из символов: -3, -1, +1, +3. При битовой скорости в 160 кбит/с скорость изменения сигнала в линии составляет 80кбод, требуемая полоса частот – около 40кГц. Длина линии связи может достигать 5,5 км, допустимое затухание – 42дБ, а конечные устройства имеют импеданс 135 Ом.

Кадр U-интерфейса имеет длину 240 бит, длительность кадра – 1,5 мс. Каждый кадр имеет структуру, приведенную на рис. 8.3. В нем два В-канала по 64 кбит/с имеют полосу 128 кбит/с, D-канал – 16 кбит/с и накладные расходы на оформление кадра 16 кбит/с.

Sync	12(B1+B2+D)	Maintenance
18 бит	216 бит	6 бит

Рис.8.3. Структура U-кадра при кодировании 2B1Q

Поле Sync представляет собой последовательность: +3 +3 -3 -3 +3 -3 +3 -3.

Каждое из полей (B1+B2+D) содержит 8 бит канала B1, 8 бит канала B2 и 2 бита канала D. Разбиение каналов на 12 порций позволяет обеспечить более равномерную передачу потока, что удобно для передачи голоса и видеoinформации. 216-битный блок данных перед кодированием трюичными символами проходит через стадию скремблирования.

Поле Maintenance содержит CRC-код, флаг контроля ошибок блока и встроенные команды.

Данные передаются суперкадрами, состоящими из восьми 240-битных кадров с общей длиной 1920бит (240 октетов). Поле синхронизации первого кадра в суперкадре инвертировано (последовательность -3 -3 +3 +3 +3 -3 +3 -3 +3).

При кодировании 3B3T каждые четыре бита представляются последовательностью из трех состояний: -v, 0, +v – с возвратом к нулю. При битовой скорости 160кбит/с скорость изменения сигнала в линии составляет 120кбод. Длина линии связи может достигать 4,2км для кабеля с диаметром жилы 0,4мм и 8,2 км – для кабеля 0,6мм. Оконечное устройство имеет импеданс 150Ом.

Порции данных длиной 36 бит собираются из 16 бит канала B1, 16 бит канала B2 и 4 бит канала D. Эти порции проходят через 23-битный самосинхронизирующий скремблер (ITU V.29), после чего кодируются по схеме 4B3T в 27 символов. Четыре блока трюичных символов d1...d4 комбинируются с 11-символьной синхропоследовательностью и служебным символом M в 120-символьный кадр. Форматы кадров встречных направлений различны.

### U-интерфейсы PRI

U-интерфейс для сервиса PRI также различен для США и Европы. В США скорость передачи составляет 1,544Мбит/с: 23 В-канала (1472кбит/с) + 1D (64кбит/с) + 8 кбит/с для синхронизации и служебных целей. Здесь используются сигналы линий T1 с кодированием AMI или B8ZS. Амплитуда импульсов ±3Вт, импеданс 100Ом. Каждый кадр содержит 193 бита: по байту от каждого В-канала и D-канала 8x(23+1) = 192 бит и бит синхронизации. Системы D4 объединяют по двенадцать 193-битных кадры в суперкадры (Superframe), системы ESF объединяют по двадцать четыре 193-битных кадры в расширенные суперкадры (Extended Superframe).

Международный стандарт – 2,048 Мбит/с (полный дуплекс): тридцать В-каналов (1920 кбит/с) +1D (64 кбит/с) +64 кбит/с для синхронизации и служебных целей, линии E1, кодирование HDB3. Среда передачи – коаксиал 75 Ом, амплитуда 2,37В; витая пара 120 Ом, амплитуда 3В. Допустимое затухание – 6 дБ. Кадр содержит 256 бит: по байту от каждого В-канала и D-канала 8x(30+1)=192 бит и байт для синхронизации и служебных целей. 16 кадров комбинируются в мультикадр (Multiframe).

### S/T-интерфейсы BRI

S-интерфейс позволяет подключать несколько (до 8) устройств, T – только двухточечный.

S – интерфейс использует две пары проводов, скорость 192 кбит/с (полный дуплекс), кодирование ASI, максимальная частота в линии 96 кГц. Кадры имеют длину 48 бит, конструкция кадров зависит от направления (рис. 8.4)

Кадр от терминала к NT-1											
	1				a		2			1	2
Кадр от NT-1 к терминалу											
	1				a		2			1	2

Рис. 8.4. Форматы кадров S/T интерфейса

Терминальное оборудование подстраивает синхронизацию под кадры, исходящие от NT-1. В каждом кадре имеется два нарушения чередования полярности: последний импульс каждого кадра всегда положительный и первый бит кадра «F» тоже положительный, за которым следует отрицательный импульс «L». Если далее нет импульсов (в первом байте B1 – все «1»), бит Fa генерирует отрицательный импульс для формирования второго нарушения чередования в кадре. Байты В-каналов кодируются по схеме ASI, первый формируемый импульс всегда отрицательный. В канале D все нулевые биты кодируются отрицательными импульсами. NT-1 возвращает эхом (E) все принятые биты D-канала. Биты «L» вводятся с таким расчетом, чтобы с момента последнего L-бита число импульсов было четным.

Терминал, у которого нет данных для передачи, входит в состояние «Marking» — отсутствие импульсов. Использование В-каналов назначается коммутатором – при обслуживании вызова В- канал логически подключается к одному из устройств. Терминалы на шине могут соперничать только по каналу D. В этом канале организуется приоритетный метод доступа CSMA/CR.

## 8.6. Подключение пользовательского оборудования к сети ISDN

Вариант подключения пользовательского оборудования к сети ISDN приведен на рис. 8.5. Оборудование делится на функциональные группы.

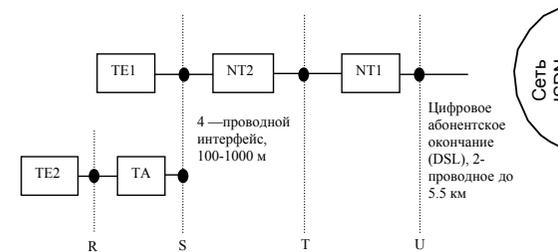


Рис. 8.5. Подключение пользовательского оборудования ЦСИО

Устройства функциональной группы NT1 (Network Termination 1) образуют цифровое абонентское окончание (Digital Subscriber Line, DSL) на кабеле, соединяющем пользовательское оборудование с сетью ISDN. Справочная точка U соответствует точке подключения устройства NT1 к сети. Устройство NT1 всегда устанавливается в помещении пользователя.

Устройства функциональной группы NT2 (Network Termination 2) представляют собой устройства канального или сетевого уровня, которые выполняют функции концентрации пользовательских интерфейсов и их мультиплексирование (офисная АТС, маршрутизатор, простой мультиплексор TDM).

Устройства функциональной группы TE1 (Terminal Equipment 1) относятся к устройствам, поддерживающих интерфейс пользователя BRI или PRI. Точка S соответствует точке подключения отдельного терминального оборудования, поддерживающего один из интерфейсов пользователя ISDN (цифровой телефон или факс-аппарат).

Устройства функциональной группы TE2 (Terminal Equipment 2) – это устройства, не поддерживающие интерфейс BRI или PRI (компьютер, маршрутизатор, не относящиеся к ЦСИО). Для подключения такого уст-

ройства к сети ISDN используется терминальный адаптер (Terminal Adaptor, TA). Для компьютеров терминальные адаптеры выпускаются в формате сетевых адаптеров (как встраиваемая карта).

### 8.7. Адресация в сетях ЦСИО

Технология ЦСИО предназначена для всемирной телекоммуникационной сети, связывающей телефонных абонентов и абонентов других глобальных сетей. Поэтому адресация узлов ЦСИО должна быть достаточно емкой для всемирной адресации и совместимой со схемами адресации других сетей, чтобы абоненты этих сетей, могли бы пользоваться привычными форматами адресов (используются в адресе ЦСИО адреса объединяемых сетей).

Формат адреса ЦСИО в стандарте E.164 расширен до 55 десятичных цифр. В сетях ЦСИО различают номер абонента и адрес абонента. Номер абонента соответствует точке Т подключения всего пользовательского оборудования к сети. Номер ЦСИО состоит из 15 десятичных цифр и делится на поле «Код страны» (от 1 до 3 цифр), поле «Код города» и поле «Номер абонента». Адрес ЦСИО включает номер плюс до 40 цифр подадреса. Подадрес используется для нумерации терминальных устройств за пользовательским интерфейсом, то есть подключаемых к точке S.

При вызове абонентов из сети, не относящейся к ЦСИО, их адрес может непосредственно заменять ЦСИО. Например, адрес абонента сети X.25, в которой используется система адресации по стандарту X.121, может быть помещен целиком в поле адреса ЦСИО, но для указания, что это адрес стандарта X.121, ему должно предшествовать поле префикса, в которое помещается код стандарта адресации, в данном случае стандарта X.121.

Стандарт ISO 7498 определяет формат адреса, причем основной схемы адресации являются первые два поля. Поле AFI (Authority and Form Identifier) задает значения всех остальных полей адреса и формат этих полей. Значением поля AFI является один из 6 типов поддоменов глобального домена адресации:

- четыре типа доменов соответствуют четырем типам публичных телекоммуникационных сетей — сетей с коммутацией пакетов, телексных сетей, публичных телефонных сетей и сетей ISDN;
- пятый тип домена — это географический домен, который назначается каждой стране (в одной стране может быть несколько географических доменов);
- шестой тип домена — это домен организационного типа, в который входят международные организации, например ООН или ATM Forum.

За полем AFI идет поле IDI (Initial Domain Identifier) — поле начального идентификатора домена, а за ним располагается дополнительное поле DSP (Domain Specific Part), которое может нести дополнительные цифры номера абонента, если разрядности поля INI не хватает.

Определены следующие значения AFI:

- международные сети с коммутацией пакетов со структурой адресов в стандарте X.121-36, если адрес задается только десятичными цифрами, и X.121-37, если адрес состоит из произвольных двоичных значений. При этом поле INI имеет формат в 14 десятичных цифр, а поле DSP может содержать еще 24 цифры;
- международные сети ISDN со структурой адресов в стандарте E.164-44, если адрес задается только десятичными цифрами, и E.164-45, если адрес состоит из произвольных двоичных значений. При этом поле IDI имеет формат в 15 десятичных цифр, а поле DSP может содержать еще 40 цифр;
- международные телефонные сети PSTN со структурой адресов в стандарте E.163-42, если адрес задается только десятичными цифрами, и E.163-43, если адрес состоит из произвольных двоичных значений. При этом поле IDI имеет формат в 12 десятичных цифр, а поле DSP может содержать еще 26 цифр;
- международные географические домены со структурой адресов в стандарте ISO DCC (Digital Country Codes) — 38, если адрес задается только десятичными цифрами, и 39, если адрес состоит из произвольных двоичных значений. При этом поле INI имеет формат в 3 десятичных цифры (код страны), а поле DSP может содержать еще 35 цифр;
- домен международных организаций. Для него однобайтовое поле IDI содержит код международной организации, от которой зависит формат поля DSP.

Для первых четырех доменов адрес абонента помещается непосредственно в поле IDI. Для пятого и шестого типов доменов IDI содержит только код страны или код организации, которая контролирует структуру и нумерацию части DSP.

Еще одним способом вызова абонентов из других сетей является указание в адресе ЦСИО двух адресов: адреса ЦСИО пограничного устройства, например, соединяющего сеть ЦСИО с сетью X.25, и адреса узла в сети X.25. Адреса должны разделяться специальным разделителем. Два адреса используются за два этапа — сначала сеть ЦСИО устанавливает соединение типа коммутируемого канала с пограничным устройством, присоединенным к сети ЦСИО, а затем передает ему вторую часть адреса, чтобы это устройство осуществило соединение с требуемым абонентом.

### 8.8. Стек протоколов и структура сети ЦСИО

В сети ЦСИО (рис. 8.6) существуют два стека протоколов: стек каналов типа D и стек каналов типа B.

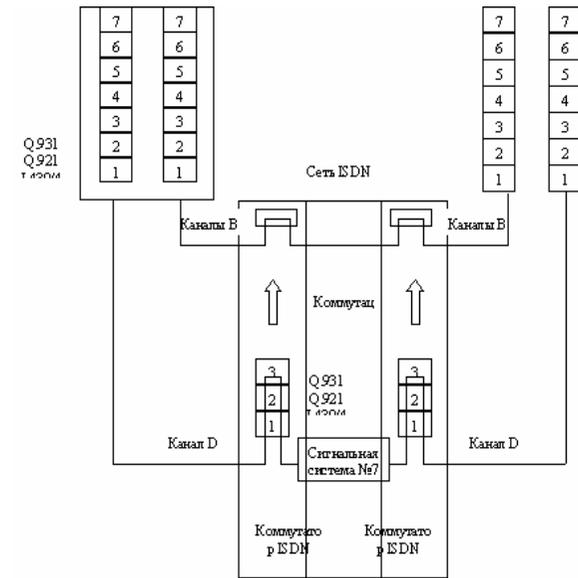


Рис. 8.6. Структура сети ЦСИО

Каналы типа D образуют сеть с коммутацией пакетов. Прообразом этой сети послужила технология сетей X.25. Для сети каналов D определены три уровня протоколов: физический протокол определяется стандартом I.430/431, канальный протокол LAP-D определяется стандартом Q.921, а на сетевом уровне может использоваться протокол Q.931, с помощью которого выполняется маршрутизация вызова абонента службы с коммутацией каналов, или же протокол X.25 — в этом случае в кадры протокола LAP-D вкладываются пакеты X.25, и коммутаторы ЦСИО выполняют роль коммутаторов X.25.

Сеть каналов типа D внутри сети ЦСИО служит транспортным уровнем для так называемой системы сигнализации номер 7 (Signal System Number 7, SS7). Система SS7 была разработана для целей внутреннего мониторинга и управления коммутаторами телефонной сети общего назначения. Эта система применяется и в сети ЦСИО. Служба SS7 относится к прикладному уровню модели OSI. Конечному пользователю ее услуги недоступны, так как сообщениями SS7 коммутаторы сети обмениваются только между собой.

Каналы типа B образуют сеть с коммутацией цифровых каналов. В терминах модели OSI на каналах типа B в коммутаторах сети ЦСИО определен только протокол физического уровня — протокол I.430/431. Коммутация каналов типа B происходит по указаниям, полученным по каналу D. Когда пакеты протокола Q.931 маршрутизируются коммутатором, одновременно происходит коммутация очередной части составного канала от исходного абонента к конечному.

В протоколе LAP-D адрес кадра LAP-D состоит из двух байт — один байт определяет код службы, который пересылаются вложенные в кадр пакеты, а второй используется для адресации одного из терминалов, если у пользователя к сетевому окончанию NT1 подключено несколько терминалов. Терминальное устройство может поддерживать разные службы — службу установления соединения по протоколу Q.931, службу коммутации пакетов X.25, службу мониторинга сети и т.п. Протокол LAP-D обеспечивает два режима работы: с установлением соединения (единственный режим работы протокола LLC2) и без установления соединения (например, для управления и мониторинга сети).

Протокол Q.931 переносит в своих пакетах адрес ЦСИО вызываемого абонента, на основании которого и происходит настройка коммутаторов на поддержку составного канала типа B.

## 8.9. Уровни ЦСИО

Подход ЦСИО предназначен для обеспечения конечного пользователя полной поддержкой на всех семи уровнях модели взаимодействия открытых систем (OSI).

Таким образом, ЦСИО подразделяется на два вида услуг: базовые услуги, ответственные за поддержку трех нижних уровней из семиуровневого стандарта, и телесервис (например, телефоны, телетекст, видеотекст, обработка сообщений), который отвечает за поддержку всех семи уровней модели и использует возможности услуг базовых уровней. Эти функции ЦСИО приведены в табл. 8.3.

## 8.10. Служебные коммуникации ЦСИО

Основным принципом ЦСИО является сквозное цифровое соединение, т.е. передача цифрового сигнала на всем пути от отправителя к получателю и обратно. Стандарты ЦСИО базируются в основном на существующих технологиях передачи данных.

К настоящему времени проведена значительная работа по проектированию и развертыванию устройств, обеспечивающих взаимодействие между локальными сетями и ЦСИО. По своей сути ЦСИО является глобальной сетевой службой. Разработанные стандарты облегчают соединение локальных сетей с ЦСИО для реализации сервиса глобальной сети. Если требуется, ЦСИО предоставляет сервис локальной сети в пользовательской среде (если это допускают параметры производительности ЛС).

Имеющиеся в организациях компьютеры соединяются в локальные сети. Телефоны подключаются к офисным АТС. Эти две сети, используемые для передачи речи и данных, как правило, не соединены друг с другом. Офисная АТС подключается к пользовательским устройствам (телефонам), а сеть пользователя связывается с местной телефонной компанией (LE — local exchange) с помощью абонентской линии. Компьютеры соединяются в локальную сеть посредством кабеля (физических линий). Локальные сети связываются друг с другом с помощью мостов и маршрутизаторов — устройств, направляющих трафик из одной сети в другую.

При такой конфигурации локальные сети и офисные АТС обычно никак не взаимодействуют. Между тем, можно, например, конфигурировать компьютер-шлюз, который будет через офисную АТС поддерживать удаленные глобальные линии. Учитывая последние разработки в компьютерной телефонии, а также созданный компанией Novell интерфейс программирования сервисных приложений телефонной связи TSAPI (Telephony Services Application Programming Interface) и программный интерфейс компьютерной телефонии TAPI (Telephony API) от Microsoft, можно предположить, что разрыв между локальными сетями и офисными АТС будет быстро исчезать.

Рано или поздно различие между сетевым сервером и PBX станет гораздо менее заметным, чем сегодня.

Локальные сети ЦСИО функционируют аналогично. Фактически сервис передачи данных предлагается большинством поставщиков услуг ЦСИО. Службы ЦСИО можно подключить к ПК, соединенным с сетью ЦСИО, с помощью интерфейсов BRI или PRI. В такой конфигурации отдельные ПК подключаются к поставщику услуг ЦСИО. Основной проблемой в конфигурациях подобного типа является производительность. Локальные сети Ethernet обеспечивают передачу 10 Мбит/с. Нередко встречаются и локальные сети, поддерживающие 100 Мбит/с. В то же время локальная сеть ISDN, работающая по В- или D- каналам, не способна превысить «ограничение скорости» В-канала в 64 Кбит/с.

ЦСИО представляет собой глобальную сеть. Ее применение в области локальных сетей связано в основном с тем, что ЦСИО обеспечивает связь между удаленными пользователями и локальной сетью или между удаленными локальными сетями.

Комитет IEEE 802.9 представил стандарты для интеграции трафика речи и данных в локальных сетях, предусматривающие активное использование ЦСИО. Стандарты 802.9 предназначены для соединения IVDTE с устройством доступа (AU — access unit), связанного с ЦСИО. Реализуемый AU сервис использует каналы ЦСИО:

- В-канал — канал 64 Кбит/с, идентичный В-каналу ЦСИО;
- С-канал — линия с коммутацией каналов, поддерживающая несколько каналов 64 Кбит/с, аналогично Н-каналам ЦСИО;
- D-канал — канал передачи сигналов в сети пользователя, полностью аналогичный D-каналу ЦСИО;
- Р-канал — канал передачи пакетов, реализующий функции локальной сети 802.

TCP/IP может функционировать поверх любых протоколов связи данных и физического уровня. Способы, применяемые в протоколе TCP/IP для передачи информации в сетях ЦСИО, описаны в серии документов — так называемых запросах на комментарии RFC (requests for comment). Эти документы выпускаются Рабочей группой инженеров Интернета (IETF — Internet Engineering Task Force), "руководящей" общемировой сетью под названием Интернет.

Интернет представляет собой совокупность локальных сетей и хост- компьютеров, связанных линиями T1 и T3, спутниковыми и радиоканалами, обычными телефонными сетями и ЦСИО. Их объединяет лишь то, что все они используют комплект протоколов TCP/IP — стандартный набор протоколов Интернета.

Протоколы TCP/IP специфицируются в документах RFC 1356 и описывают передачу пакетов IP в ЦСИО. Стандарты протоколов для взаимодействия между сетями ЦСИО и IP утверждены Консультативным

комитетом по международной телефонной и телеграфной связи (ССТТ) и Международной организацией стандартизации (ISO).

8-байтовый идентификатор протокола сетевого уровня NLPID (network layer protocol identifier) применяется в ЦСИО для идентификации типа используемых протоколов более высокого уровня. IP имеет идентификатор 11001100 (0хСС). В пакете данных ЦСИО идентификатор NLPID содержится в первом октете поля вызова пользователя

ISDN позволяет предоставлять два вида неречевого сервиса, получивших широкое распространение. Это службы пакетного режима X.25 и Frame Relay. В исходных стандартах ЦСИО для коммутации пакетов и неречевого трафика были использованы стандарты X.25. Стандарты ЦСИО, выпущенные в 1988 г., рекомендуют заменить коммутацию пакетов X.25 на Frame Relay, где предусматривается лишь минимальный контроль ошибок при передаче. Снижение непроизводительных потерь на контроль ошибок позволяет соответствующим образом увеличить скорость обмена данными.

Сети X.25 широко используются уже почти 20 лет. Стандарты ЦСИО разрабатывались так, чтобы сети X.25 можно было встроить в ЦСИО. Взаимодействие X.25 и ЦСИО описывается в рекомендациях ССТТ X.31.

По существу стандарты допускают два типа взаимодействия между ЦСИО и X.25. В одном стандарте, X.31 Case A, ЦСИО может обращаться к службам сети X.25. В другом, X.31 Case B, возможности коммутации каналов, предлагаемые X.25, становятся составной частью ЦСИО.

В стандарте Case A устройство DTE X.25 запрашивает через ТА соединение ЦСИО с другим устройством DCE X.25 и режиме виртуальной цепи. Путь от DCE к выбранному DTE устанавливается через третий уровень протокола X.25. В случае Case A D-канал ЦСИО не используется, поскольку его сигналы заканчиваются в LE. Именно поэтому для Case A трафик пакетов X.25 передается только по В-каналу ЦСИО.

В стандарте Case B возможности коммутации пакетов X.25 становятся частью ЦСИО. Устройство DTE X.25 создает виртуальную цепь средствами ЦСИО. LE ЦСИО может обеспечить коммутацию пакетов или получить доступ к DCE X.25. Настройка вызова и управление реализуются средствами ЦСИО. Case B является стандартом ЦСИО в Северной Америке и служит общепринятым способом запроса пересылки кадров LAPB по В-каналу, а также методом инкапсуляции кадров LAPB в кадрах LAPD для пересылки по D-каналу.

Высокая степень контроля ошибок и связанные с этим непроизводительные потери, характерные для X.25, уже не нужны в той мере, как это требовалось 20 лет назад.

Сегодня получили распространение средства доставки под названием «кадровый режим» или режим передачи кадров (frame mode). Возможности этого режима очень напоминают X.25, но в них отсутствует третий уровень модели OSI. Адреса и информация соединения обрабатываются протоколами второго уровня. Название «кадровый режим» объясняется тем, что информация уровня 2 передается по сети в кадрах, а не с помощью пакетов.

В результате протоколы уровня 2, кроме выполнения своих обычных функций второго уровня (контроль ошибок и мультиплексирование), отвечают за адресацию и последовательность кадров.

## ГЛАВА 9 ШИРОКОПОЛОСНЫЕ СЕТИ ИНТЕГРАЛЬНОГО ОБСЛУЖИВАНИЯ

Технология асинхронного режима передачи ATM (Asynchronous Transfer Mode) — это единый универсальный транспорт для широкополосных ISDN. Транспортная технология ATM обеспечивает следующие возможности:

- передачу в рамках одной транспортной системы компьютерного и мультимедийного (голос, видео) трафика, чувствительного к задержкам, причем для каждого вида трафика качество обслуживания будет соответствовать его потребностям;
- иерархию скоростей передачи данных от десятков мегабит до нескольких гигабит в секунду с гарантированной пропускной способностью для ответственных приложений;
- общие транспортные протоколы для локальных и глобальных сетей, сохранение имеющейся инфраструктуры физических каналов или физических протоколов (T1/E1, T3/E3, SDH STM-n, FDDI);
- взаимодействие с унаследованными протоколами локальных и глобальных сетей IP, SNA, Ethernet, ISDN.

Технология ATM представляет собой типичную технологию глобальных сетей, основанную на технике виртуальных каналов: конечные станции соединяются индивидуальными каналами с коммутаторами нижнего уровня, которые в свою очередь соединяются с коммутаторами более высоких уровней. Коммутаторы ATM пользуются 20-байтными адресами конечных узлов для маршрутизации трафика на основе техники виртуальных каналов.

Коммутация пакетов происходит на основе идентификатора виртуального канала (Virtual Channel Identifier, VCI), который назначается соединению при его установлении и уничтожается при разрыве соединения. Адрес конечного узла ATM, на основе которого прокладывается виртуальный канал, имеет иерархическую структуру, подобную номеру в телефонной сети, и использует префиксы, соответствующие кодам стран, городов, сетям поставщиков услуг и т.п., что упрощает маршрутизацию запросов установления соединения, как и при использовании агрегированных IP-адресов в соответствии с техникой CIDR.

Виртуальные соединения могут быть постоянными — PVC (Permanent Virtual Circuit) и коммутируемыми — SVC (Switched Virtual Circuit). Для ускорения коммутации в больших сетях используется понятие виртуального пути (Virtual Path), который объединяет виртуальные каналы, имеющие в сети ATM общий маршрут между исходным и конечным узлами или общую часть маршрута между некоторыми двумя коммутаторами сети. Идентификатор виртуального пути VPI (Virtual Path Identifier) является старшей частью локального адреса и представляет собой общий префикс для некоторого количества различных виртуальных каналов. Соединения конечной станции ATM с коммутатором нижнего уровня определяются стандартом UNI (User Network Interface). Спецификация UNI определяет структуру пакета, адресацию станций, обмен управляющей информацией, уровни протокола ATM, способы установления виртуального канала и способы управления трафиком.

Особенности технологии ATM заключаются в качественном обслуживании разнородного трафика и совмещении в одних и тех же каналах связи и в одном и том же коммуникационном оборудовании компьютерного и мультимедийного трафика таким образом, чтобы каждый тип трафика получил требуемый уровень обслуживания. Подход, реализованный в технологии ATM, состоит в передаче любого вида трафика — компьютерного, телефонного или видео — пакетами фиксированной и очень маленькой длины в 53 байта. Пакеты ATM называют ячейками (cell). Поле данных ячейки занимает 48 байт, а заголовок — 5 байт. Длина номера виртуального канала составляет 24 бит. Этого вполне достаточно для обслуживания большого количества виртуальных соединений каждым портом коммутатора глобальной сети ATM. Для пакета, состоящего из 53 байт, при скорости в 155 Мбит/с время передачи кадра на выходной порт составляет менее 3 мкс. Эта задержка не очень существенна для трафика, пакеты которого должны передаваться каждые 125 мкс.

Для передачи интегральной информации технология ATM использует идеи заказа пропускной способности и качества обслуживания, реализованные в технологии frame relay. Но если сеть frame relay изначально была предназначена для передачи только пульсирующего компьютерного трафика, то в технологии ATM выделено 4 основных класса трафика, для которых разработаны различные механизмы резервирования и поддержания требуемого качества обслуживания.

### 9.1. Классы (категории) гарантированного сервиса протокола ATM

Класс трафика качественно характеризует требуемые услуги по передаче данных через сеть ATM. Если приложение передает голосовой трафик, то для пользователя важны такие показатели качества обслуживания, как задержки и вариации задержек ячеек, существенно влияющие на качество переданной информации (голоса или изображения), а потеря отдельной ячейки с несколькими замерами не так уж важна. Требования к синхронности передаваемых данных важны для многих приложений — не только голоса, но и видеозаписи, и наличие этих требований стало первым критерием для деления трафика на классы.

Для поддержания требуемого качества обслуживания различных виртуальных соединений и рационального использования ресурсов в сети на уровне протокола ATM реализовано несколько служб, предоставляющих

услуги различных категорий по обслуживанию пользовательского трафика. Эти службы являются внутренними службами сети ATM. Они предназначены для поддержания пользовательского трафика различных классов совместно с протоколами AAL. Но в отличие от протоколов AAL, которые работают в конечных узлах сети, данные службы распределены по всем коммутаторам сети. Услуги этих служб развиты на категории, которые в общем соответствуют классам трафика, поступающим на вход уровня AAL конечного узла. Услуги уровня ATM заказываются конечным узлом через интерфейс UNI с помощью протокола Q.2931 при установлении виртуального соединения. Как и при обращении к уровню AAL, при заказе услуги необходимо указать категорию услуги, а также параметры трафика и параметры QoS. Эти параметры берутся из аналогичных параметров уровня AAL или же определяются по умолчанию в зависимости от категории услуги.

Всего на уровне протокола ATM определено пять категорий услуг, которые поддерживаются одноименными службами:

- 1) CBR — услуги для трафика с постоянной битовой скоростью;
- 2) rtVBR — услуги для трафика с переменной битовой скоростью, требующего соблюдения средней скорости передачи данных и синхронизации источника и приемника;
- 3) nrtVBR — услуги для трафика с переменной битовой скоростью, требующего соблюдения средней скорости передачи данных, но не требующего синхронизации источника и приемника;
- 4) ABR — услуги для трафика с переменной битовой скоростью, требующего соблюдения некоторой минимальной скорости передачи данных и не требующего синхронизации источника и приемника;
- 5) UBR — услуги для трафика, не предъявляющего требований к скорости передачи данных и синхронизации источника и приемника.

Названия большинства категорий услуг совпадают с названием типов пользовательского трафика, для обслуживания которого они разработаны, но необходимо понимать, что сами службы уровня ATM и их услуги — это внутренние механизмы сети ATM, которые экранруются от приложения уровнем AAL.

Услуги категории CBR предназначены для поддержания трафика синхронных приложений — голосового, эмуляции цифровых выделенных каналов и т.п. Когда приложение устанавливает соединение категории CBR, оно заказывает пиковую скорость трафика ячеек PCR, являющуюся максимальной скоростью, которую может поддерживать соединение без риска потерять ячейку, а также параметры QoS: величины максимальной задержки ячеек CTD, вариации задержки ячеек CDV и максимальной доли потерянных ячеек CLR.

Затем данные передаются по этому соединению с запрошенной скоростью (уменьшение скорости приложением возможно, например, при передаче компрессированного голоса с помощью услуги категории CBR). Любые ячейки, передаваемые станцией с большей скоростью, контролируются первым коммутатором сети и помечаются признаком низкого приоритета CLP=1. При перегрузках сети они могут просто отбрасываться сетью. Ячейки, которые запаздывают и не укладываются в интервал, оговоренный параметром вариации задержки CDV, также считаются мало значимыми для приложения и отмечаются признаком низкого приоритета CLP=1.

Для соединений CBR нет ограничений на некоторую дискретность заказа скорости PCR, как, например, в каналах T1/E1, где скорость должна быть кратна 64 Кбит/с.

По сравнению со службой CBR, службы VBR требуют более сложной процедуры заказа соединения между сетью и приложением. В дополнение к пиковой скорости PCR приложение VBR заказывает еще и два других параметра: длительно поддерживаемую скорость — SCR, которая представляет собой среднюю скорость передачи данных, разрешенную приложению, а также максимальный размер пульсации — MBS. Максимальный размер пульсации измеряется в количестве ячеек ATM. Пользователь может превышать скорость вплоть до величины PCR, но только на короткие периоды времени, в течение которых передается объем данных, не превышающий MBS. Этот период времени называется терпимостью к пульсации — BT (Burst Tolerance). Сеть вычисляет этот период как производный от трех заданных значений PCR, SCR и MBS. Если скорость PCR наблюдается в течение периода времени, большего чем BT, то ячейки помечаются как нарушители. Устанавливается признак CLP=1.

Для услуг категории rtVBR задаются и контролируются те же параметры QoS, что и для услуг категории CBR, а услуги категории nrtVBR ограничиваются поддержанием параметров трафика. Сеть также поддерживает для обеих категорий услуг VBR определенный максимальный уровень доли потерянных ячеек CLR, который либо задается явно при установлении соединения, либо назначается по умолчанию в зависимости от класса трафика.

Для контроля параметров трафика и QoS в технологии ATM применяется так называемый обобщенный алгоритм контроля скорости ячеек — Generic Cell Rate Algorithm, который может проверять соблюдение пользователем и сетью таких параметров, как PCR, CDV, SCR, BT, CTD и CDV. Он работает по модифицированному алгоритму «дырявого ведра», применяемому в технологии frame relay.

Для многих приложений, которые могут быть чрезвычайно «взрывными» в отношении интенсивности трафика, невозможно точно предсказать параметры трафика, оговариваемые при установлении соединения. Например, обработка транзакций или трафик двух взаимодействующих локальных сетей непредсказуемы по своей природе — изменения интенсивности трафика слишком велики, чтобы заключить с сетью какое-либо разумное соглашение.

В отличие от CBR и обеих служб VBR, служба UBR не поддерживает ни параметры трафика, ни параметры качества обслуживания. Служба UBR предлагает только доставку «по возможности» без каких-либо гаран-

тий. Разработанная специально для обеспечения возможности превышения полосы пропускания, служба UBR представляет собой частичное решение для тех непредсказуемых «взрывных» приложений, которые не готовы согласиться с фиксацией параметров трафика.

Главными недостатками услуг UBR являются отсутствие управления потоком данных и неспособность принимать во внимание другие типы трафика. Несмотря на перегрузку сети, соединения UBR будут продолжать передачу данных. Коммутаторы сети могут буферизовать некоторые ячейки поступающего трафика. В некоторый момент буферы переполняются, и ячейки теряются. А так как для соединений UBR не оговариваются никаких параметров трафика и QoS, то их ячейки отбрасываются в первую очередь.

Служба ABR подобно службе UBR предоставляет возможность превышения полосы пропускания, но благодаря технике управления трафиком при перегрузке сети она дает некоторые гарантии сохранности ячеек. ABR — это первый тип служб уровня ATM, который действительно обеспечивает надежный транспорт для пульсирующего трафика за счет того, что может находить неиспользуемые интервалы в общем трафике сети и заполнять их своими ячейками, если другим категориям служб эти интервалы не нужны.

Сеть и конечный узел заключают соглашение о требуемой минимальной скорости передачи MCR. Это гарантирует приложению, работающему в конечном узле, небольшую пропускную способность, обычно минимально необходимую для того, чтобы приложение работало. Конечный узел соглашается не передавать данные со скоростью, выше пиковой, то есть PCR, а сеть соглашается всегда обеспечивать минимальную скорость передачи ячеек MCR. Если при установлении соединения ABR не задаются значения максимальной и минимальной скорости, то по умолчанию считается, что PCR совпадает со скоростью линии доступа станции к сети, а MCR считается равной нулю.

Трафик соединения категории ABR получает гарантированное качество услуг в отношении доли потерянных ячеек и пропускной способности. Что касается задержек передачи ячеек, то хотя сеть и старается свести их к минимуму, но гарантий по этому параметру не дает. Следовательно, служба ABR не предназначена для приложений реального времени, а предназначена для приложений, в которых поток данных не очень чувствителен к задержкам в передаче.

При передаче трафика CBR, VBR и UBR явное управление перегрузками в сети отсутствует. Вместо этого используется механизм отбрасывания ячеек-нарушителей, а узлы, пользующиеся услугами CBR и VBR, стараются не нарушать условия контракта под угрозой потери ячеек, поэтому они обычно не пользуются дополнительной пропускной способностью, даже если она в данный момент доступна в сети.

Служба ABR позволяет воспользоваться резервами пропускной способности сети, так как сообщает конечному узлу о наличии в данный момент избыточной пропускной способности с помощью механизма обратной связи. Этот же механизм может помочь службе ABR снизить скорость передачи данных конечным узлом в сеть (вплоть до минимального значения MCR), если сеть испытывает перегрузку.

Стратегия приоритетного обслуживания трафика основана на категориях услуг каждого виртуального соединения. До принятия спецификации ABR в большинстве коммутаторов ATM была реализована простая одноуровневая схема обслуживания, которая давала графику CBR первый приоритет, трафику VBR второй, а трафику UBR — третий. При такой схеме комбинация CBR и VBR может потенциально заморозить трафик, обслуживаемый другим классом служб. Такая схема не будет правильно работать с графиком ABR, так как не обеспечит его требования к минимальной скорости передачи ячеек. Для обеспечения этого требования должна быть выделена некоторая гарантированная полоса пропускания.

Чтобы поддерживать службу ABR, коммутаторы ATM должны реализовать двухуровневую схему обслуживания, которая бы удовлетворяла требованиям CBR, VBR и ABR. По этой схеме коммутатор предоставляет некоторую часть своей пропускной способности каждому классу служб. Трафик CBR получает часть пропускной способности, необходимую для поддержания пиковой скорости PCR, трафик VBR получает часть пропускной способности, необходимую для поддержания средней скорости SCR, а трафик ABR получает часть пропускной способности, достаточную для обеспечения требования минимальной скорости ячеек MCR. Это гарантирует, что каждое соединение может работать без потерь ячеек и не будет доставлять ячейки ABR за счет трафика CBR или VBR. На втором уровне этого алгоритма график CBR и VBR может забрать всю оставшуюся пропускную способность сети, если это необходимо, так как соединения ABR уже получили свою минимальную пропускную способность, которая им гарантировалась.

## 9.2. Технология ATM как универсальный транспорт ЛВС и ГВС

Главная идея технологии асинхронного режима передачи была высказана давно — этот термин ввела лаборатория Bell Labs еще в 1968 году. Основной разрабатываемой технологией тогда была технология TDM с синхронными методами коммутации, основанными на порядковом номере байта в объединенном кадре. Главный недостаток технологии TDM, которую также называют технологией синхронной передачи STM (Synchronous Transfer Mode), заключается в невозможности перераспределять пропускную способность объединенного канала между подканалами. В те периоды времени, когда по подканалу не передаются пользовательские данные, объединенный канал все равно передает байты этого подканала.

Попытки загрузить периоды простоя подканалов приводят к необходимости введения заголовка для данных каждого подканала. В промежуточной технологии STDM (Statistical TDM), которая позволяет заполнять

периоды простоя передач пульсаций трафика других подканалов, действительно вводятся заголовки, содержащие номер подканала. Данные при этом оформляются в пакеты, похожие по структуре на пакеты компьютерных сетей. Наличие адреса у каждого пакета позволяет передавать его асинхронно, так как местоположение его относительно данных других подканалов уже не является его адресом. Асинхронные пакеты одного подканала вставляются в свободные тайм-слоты другого подканала, но не смешиваются с данными этого подканала, так как имеют собственный адрес.

Технология ATM совмещает в себе подходы двух технологий — коммутации пакетов и коммутации каналов. От первой она взяла на вооружение передачу данных в виде адресуемых пакетов, а от второй — использование пакетов небольшого фиксированного размера, в результате чего задержки в сети становятся более предсказуемыми. С помощью техники виртуальных каналов, предварительного заказа параметров качества обслуживания канала и приоритетного обслуживания виртуальных каналов с разным качеством обслуживания удается добиться передачи в одной сети разных типов трафика без дискриминации. Хотя сети ISDN также разрабатывались для передачи различных видов трафика в рамках одной сети, голосовой трафик явно был для разработчиков более приоритетным. Технология ATM с самого начала разрабатывалась как технология, способная обслуживать все виды трафиков.

## 9.3. Структура стека протоколов ATM

На рис. 9.1 представлена структура плоскостной модели стека протоколов в сети ATM (предполагает использование концепции нескольких плоскостей для разделения пользовательских функций, функций управления и контроля), которая содержит эти три плоскости: пользовательскую — для передачи абонентской информации, плоскость контроля — для передачи информации сигнализации и плоскость управления — для системы эксплуатации сети и реализации операторских функций. Кроме того, добавлено третье измерение в структуре, называемое управлением плоскостями, которое отвечает за управление системой в целом. Впрочем, поскольку технология ATM находится еще в стадии становления, очень много функций управления до сих пор не стандартизированы.

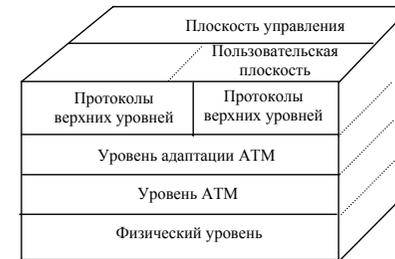


Рис. 9.1. Модель стека протоколов в сети ATM  
Каждая плоскость охватывает несколько уровней модели, причем уровни функционируют независимо друг от друга и общаются между собой стандартными протокольными блоками. Взаимосвязь уровней ATM и уровней модели OSI можно представить так: физический уровень приблизительно совпадает по функциям с первым уровнем модели OSI и занимается обработкой потока бит. Уровень ATM располагается в нижней части второго уровня стандартной модели. Уровень адаптации ATM — AAL (ATM adaptation layer) — выполняет задачи приспособления протоколов верхних уровней, пользовательской или сигнальной информации к ячейкам ATM фиксированной длины. Для плоскости контроля информация сигнализации эквивалентна нижней части второго уровня OSI, а пользовательская плоскость больше приложима к нижней части транспортного уровня, поскольку адаптация пользовательских данных выполняется из конца в конец между абонентскими установками. Функции системы можно разделить между уровнями ATM так, как представлено на рис. 9.2. Физический уровень отвечает за передачу бит/ячеек, уровень ATM занимается коммутацией и маршрутизацией, а также мультиплексированием информации уровня AAL, который отвечает за привязку пользовательских данных к потоку ячеек, причем эта привязка для различных типов служб может делаться по-разному.

Эти три уровня в свою очередь делятся на подуровни, каждый из которых также реализует свои функции.

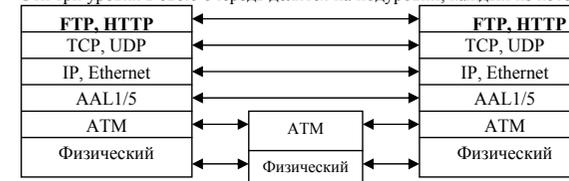


Рис. 9.2. Распределение протоколов по узлам и клавиатурам сети ATM

Стек протоколов ATM соответствует нижним уровням семиуровневой модели OSI/ISO и включает уровень адаптации ATM, уровень ATM и физический уровень.

На рис. 9.3. приведена схема функций различных подуровней модели стека протоколов в сети ATM.

конвергенция	CS	
сборка / разборка	SAR	AAL
общее управление потоком		
преобразование номеров VCI/VPI		ATM
мультиплексирование/ демупльтиплексирование		
выделение потока информационных селлов		
контроль правильности заголовка		
оформление селлов	TC	
подготовка кадров к передаче		PHY
оформление / расшифровка кадров		
битовая синхронизация		
физическая среда	PM	

CS	: подуровень конвергенции
SAR	: сборка / разборка
TC	: конвергенция передачи
PM	: физическая среда

Рис. 9.3. Схема функций различных подуровней модели

### 9.3.1. Физический уровень

Физический уровень состоит из подуровня физической среды и подуровня конвергенции, т.е. «подтягивания» вида передаваемых данных к виду, удобному для передачи по каналам. Подуровень физической среды отвечает за корректную передачу и прием битов по каналу. Иначе говоря, с его помощью осуществляется ввод потока данных в канал связи. Кроме того, этот уровень выполняет битовую синхронизацию на канале (отметим, что битовая синхронизация на канале никак не связана с синхронизацией ячеек, о которой говорилось выше — ячейка может быть выдана в канал в произвольный момент времени, т.е. битовая синхронизация присутствует в любой системе, а кадровая синхронизация может отсутствовать).

Подуровень конвергенции в первую очередь выполняет адаптацию к системе передачи (например, это может быть система 8B/10B или SONET). Это значит, что подуровень выполняет функции формирования той информационной структуры, которая соответствует системе передачи (например, здесь осуществляется вкладывание потока ячеек в кадры SONET или 8B/10 и формирование самих этих кадров). На приеме производится изъятие ячеек из кадров и кроме того, на этом подуровне осуществляется помехозащита заголовка ячеек, соответственно, на нем лежит и функция синхронизации ячеек, поскольку, как уже говорилось, она неотделима от системы кодирования заголовка. Помимо синхронизации, также выполняются все функции, связанные с обработкой ошибок в заголовке. Все вышесказанное означает, что выполняются некоторые функции по формированию ячеек — добавление в заголовок проверочного байта. Здесь же выполняется механизм вставки и изъятия «пустых» ячеек, которые нужны для того, чтобы не образовывалось пауз в потоке.

### 9.3.2. Протокол ATM

Протокол ATM занимает в стеке протоколов ATM примерно то же место, что протокол IP в стеке TCP/IP. Работа уровня ATM полностью независима от работы физического уровня, который выдает ячейки, проверенные по заголовкам и готовые к маршрутизации. Протокол ATM занимается передачей ячеек через коммутаторы при установленном и настроенном виртуальном соединении, то есть на основании готовых таблиц коммутации портов. Протокол ATM выполняет коммутацию по номеру виртуального соединения, который в технологии ATM разбит на две части — идентификатор виртуального пути VPI и идентификатор виртуального канала VCI. Кроме этой основной задачи протокол ATM выполняет ряд функций по контролю за соблюдением трафика-контракта со стороны пользователя сети, маркировке ячеек-нарушителей, отбрасыванию ячеек-нарушителей при перегрузке сети, а также управлению потоком ячеек для повышения производительности сети (естественно, при соблюдении условий трафика контракта для всех виртуальных соединений).

Протокол ATM работает с ячейками следующего формата, представленного на рис. 9.4. Поле «Управление потоком» (Generic Flow Control) используется только при взаимодействии конечного узла и первого коммутатора сети. В настоящее время его точные функции не определены. Поля «Идентификатор виртуального пути (VPI)» и «Идентификатор виртуального канала (VCI)» занимают соответственно 1 и 2 байта. Эти поля задают номер вир-

туального соединения, разделенный части: старшую (VPI) и младшую (VCI). Поле «Идентификатор типа данных (PTI)» (Payload Type Identifier) состоит из трех бит и задает тип данных, переносимых ячейкой, — пользовательские или управляющие (например, управляющие установлением виртуального соединения). Кроме того, один бит этого поля используется для указания перегрузки в сети — EFCI (Explicit Congestion Forward Identifier). Он передает информацию о перегрузке по направлению потока данных.

Управление потоком (GFC)		Идентификатор виртуального пути (VPI)	
Идентификатор виртуального пути (продолжение)		Идентификатор виртуального канала	
Идентификатор Виртуального канала (продолжение)			
Идентификатор виртуального канала (продолжение)	Тип данных (PTI)	Приоритет потери пакета	
Управление ошибками в заголовке (HEC)			
Данные пакета			

Рис. 9.4. Формат ячейки ATM

Поле «Приоритет потери кадра (CLP)» (Cell Loss Priority) играет в данной технологии следующую роль: в нем коммутаторы ATM отмечают ячейки, которые нарушают соглашения о параметрах качества обслуживания, чтобы удалить их при перегрузках сети. Таким образом, ячейки с CLP=0 являются для сети высокоприоритетными, а ячейки с CLP=1 — низкоприоритетными.

Поле «Управление ошибками в заголовке (HEC)» (Header Error Control) содержит контрольную сумму, вычисленную для заголовка ячейки. Контрольная сумма вычисляется с помощью техники корректирующих кодов Хэмминга, поэтому она позволяет не только обнаруживать ошибки, но и исправлять все одиночные ошибки, а также некоторые двойные. Поле HEC обеспечивает не только обнаружение и исправление ошибок в заголовке, но и нахождение границы начала кадра в потоке байтов кадров SDH, которые являются предпочтительным физическим уровнем технологии ATM, или же в потоке бит физического уровня, основанного на ячейках. Указателей, позволяющих в поле данных кадра STS-n (STM-n) технологии SONET/SDH обнаруживать границы ячеек ATM (подобных тем указателям, которые используются для определения, например, границ виртуальных контейнеров подканалов T1/E1), не существует. Поэтому коммутатор ATM вычисляет контрольную сумму для последовательности из 5 байт, находящихся в поле данных кадра STM-n, и, если вычисленная контрольная сумма говорит о корректности заголовка ячейки ATM, первый байт становится границей ячейки. Если же это не так, то происходит сдвиг на один байт и операция продолжается. Таким образом, технология ATM выделяет асинхронный поток ячеек ATM в синхронных кадрах SDH или потоке бит физического уровня, основанного на ячейках.

### 9.3.3. Уровень адаптации ATM

Уровень адаптации AAL представляет собой набор протоколов AAL1-AAL5, которые преобразуют сообщения протоколов верхних уровней сети ATM в ячейки ATM нужного формата. AAL обеспечивает связку сервиса, поставляемого уровнем ATM с пользовательскими уровнями. На нем лежит реализация функций пользовательской плоскости, плоскости контроля и управления. Поскольку системой могут пользоваться различные службы, то и вариантов реализации уровня AAL также несколько, и они зависят от потребностей служб. Функции этих уровней достаточно условно соответствуют функциям транспортного уровня модели OSI, например функциям протоколов TCP или UDP. Протоколы AAL при передаче пользовательского трафика работают только в конечных узлах сети, как и транспортные протоколы большинства технологий.

Каждый протокол уровня AAL обрабатывает пользовательский трафик определенного класса. На начальных этапах стандартизации каждому классу трафика соответствовал свой протокол AAL, который принимал в конечном узле пакеты от протокола верхнего уровня и заказывал с помощью соответствующего протокола нужные параметры трафика и качества обслуживания для данного виртуального канала. При развитии стандартов ATM такое однозначное соответствие между классами трафика и протоколами уровня AAL исчезло. Сегодня разрешается использовать для одного и того же класса трафика различные протоколы уровня AAL.

Уровень адаптации состоит из нескольких подуровней. Нижний подуровень AAL называется подуровнем сегментации и реассемблирования (Segmentation And Reassemble, SAR). Эта часть не зависит от типа протокола AAL (и, соответственно, от класса передаваемого трафика) и занимается разбиением (сегментацией) сооб-

щения, принимаемого AAL от протокола верхнего уровня, на ячейки ATM, снабжением их соответствующим заголовком и передачей уровню ATM для отправки в сеть.

Верхний подуровень AAL называется подуровнем конвергенции — CS (Convergence Sublayer). Этот подуровень зависит от класса передаваемого трафика. Протокол подуровня конвергенции решает такие задачи, как обеспечение временной синхронизации между передающим и принимающим узлами (для трафика, требующего такой синхронизации), контролем и возможным восстановлением битовых ошибок в пользовательской информации, контролем целостности передаваемого пакета компьютерного протокола (X.25, frame relay).

Протоколы AAL для выполнения своей работы используют служебную информацию, размещаемую в заголовках уровня AAL. После приема ячеек, пришедших по виртуальному каналу, подуровень SAR протокола AAL собирает посланное по сети исходное сообщение (разбитое в общем случае на несколько ячеек ATM) с помощью заголовков AAL, которые для коммутаторов ATM являются прозрачными, так как помещаются в 48-битном поле данных ячейки, как и полагается протоколу более высокого уровня. После сборки исходного сообщения протокол AAL проверяет служебные поля заголовка и концевого кадра AAL и на их основании принимает решение о корректности полученной информации.

Ни один из протоколов AAL при передаче пользовательских данных конечных узлов не занимается восстановлением потерянных или искаженных данных. AAL только уведомляет конечный узел о таком событии. Так сделано для ускорения работы коммутаторов сети ATM в расчете на то, что случаи потерь или искажения данных будут редкими. Восстановление потерянных данных (или игнорирование этого события) отводится протоколам верхних уровней, не входящим в стек протоколов технологии ATM.

Протокол AAL1 обычно обслуживает трафик с постоянной битовой скоростью (Constant Bit Rate, CBR), который характерен для цифрового видео и цифровой речи и чувствителен к временным задержкам. В задачи протокола AAL1 входит сглаживание неравномерности поступления ячеек данных в узел назначения.

Протокол AAL2 был разработан для передачи трафика с минимальной битовой скоростью передачи данных, но при развитии стандартов он был исключен из стека протоколов ATM, и сегодня трафик класса В передается с помощью протокола AAL, AAL3/4 или AAL5.

Протокол AAL3/4 обрабатывает пульсирующий трафик — обычно характерный для трафика локальных сетей — с переменной битовой скоростью (Variable Bit Rate, VBR). Этот трафик обрабатывается так, чтобы не допустить потерь ячеек, но ячейки могут задерживаться коммутатором. Протокол AAL3/4 выполняет сложную процедуру контроля ошибок при передаче ячеек, нумеруя каждую составляющую часть исходного сообщения и снабжая каждую ячейку контрольной суммой. Правда, при искажениях или потерях ячеек уровень не занимается их восстановлением, а просто отбрасывает все сообщение (то есть все оставшиеся ячейки), так как для компьютерного трафика или компрессированного голоса потеря части данных является фатальной ошибкой. Протокол AAL3/4 образовался в результате слияния протоколов AAL3 и AAL4, которые обеспечивали поддержку трафика компьютерных сетей соответственно с установлением соединения и без установления соединения. Однако ввиду большой близости используемых форматов служебных заголовков и логики работы протоколы AAL3 и AAL4 были впоследствии объединены.

Протокол AAL5 является упрощенным вариантом протокола AAL4 и работает быстрее, так как вычисляет контрольную сумму не для каждой ячейки сообщения, а для всего исходного сообщения в целом, и помещает ее в последнюю ячейку сообщения. Первоначально протокол AAL5 разрабатывался для передачи кадров сетей frame relay, но теперь он чаще всего используется для передачи любого компьютерного трафика. Протокол AAL3 может поддерживать различные параметры качества обслуживания, кроме тех, которые связаны с синхронизацией передающей и принимающей сторон. Поэтому он обычно используется для поддержки всех классов трафика, относящегося к передаче компьютерных данных. Некоторые производители оборудования с помощью протокола AAL5 обслуживают трафик CBR, оставляя задачу синхронизации трафика протоколам верхнего уровня.

Протокол AAL5 работает не только в конечных узлах, но и в коммутаторах сети ATM. Однако там он выполняет служебные функции, не связанные с передачей пользовательских данных. В коммутаторах ATM протокол AAL5 поддерживает служебные протоколы более высоких уровней, занимающиеся установлением коммутируемых виртуальных соединений.

Существует определенный интерфейс между приложением, которому требуется передать трафик через сеть ATM, и уровнем адаптации AAL. С помощью этого интерфейса приложение (протокол компьютерной сети, модуль оцифровывания голоса) заказывает требуемую услугу, определяя тип трафика, его параметры, а также параметры QoS. Технология ATM допускает два варианта определения параметров QoS: первый — непосредственное задание их каждым приложением, второй — назначение их по умолчанию в зависимости от типа трафика. Последний способ упрощает задачу разработчика приложения, так как в этом случае выбор максимальных значений задержки доставки ячеек и вариации задержек перекладывается на плечи администратора сети.

Самостоятельно обеспечить требуемые параметры трафика и QoS протоколы AAL не могут. Для выполнения согласованной трафик-конт-ракта требуется согласованная работа коммутаторов сети вдоль всего виртуального соединения. Эта работа выполняется протоколом ATM, обеспечивающим передачу ячеек различных виртуальных соединений с заданным уровнем качества обслуживания.

#### 9.4. ATM как современная инфраструктура

Если виртуальные устройства напоминают реальные, ATM можно легко приспособить для текущих приложений, просто заменив выделенные или коммутируемые линии виртуальными устройствами ATM.

Типичный пользовательский сайт с устройствами порождает разнотипный трафик (голос, видео, данные). Все типы трафика могут передаваться с использованием сервиса ATM.

1. Голос, данные и видео преобразуются в ячейки ATM в сети оператора с использованием функций адаптации ATM. Оператор будет реализовывать все функции доступа и передачи, а для каждого устройства потребуются отдельная линия доступа в сеть ATM.

2. ЛВС, голосовые и видеоустройства подключаются к локальному коммутатору ATM для преобразования трафика в ячейки. Для доступа в сеть оператора используется одна линия, передающая все потоки трафика одновременно (как виртуальные устройства). Сеть оператора обеспечивает маршрутизацию трафика. Такое решение более экономично и может использоваться для организации «частных сетей ATM» для пользователей, которые имеют доступ к ATM-сервису или хотят создать свою распределенную сеть на базе ATM. Отметим, что находящийся в сети пользователя коммутатор ATM может принадлежать оператору и находиться у него на обслуживании.

3. Устройства оборудуются собственными интерфейсами ATM. Одно устройство доступа позволяет объединить весь пользовательский трафик в одном транке, связанном с сетью оператора. В этом случае на стороне пользователя устанавливается принадлежащее ему оборудование ATM, которое можно использовать для организации магистралей ЛВС или подключения настольных станций.

Скорое появление интерфейсов ATM в телефонном и видео-оборудовании не представляется вероятным, поэтому реализация третьего варианта соединения с сетью не сможет в ближайшие годы стать доминирующей. Скорость распространения каждого из приведенных вариантов будет определяться темпами снижения цен на оборудование и услуги операторов сетей ATM. Отсутствие эффективного управления этими процессами порождает определенный хаос и не позволяет надежно предсказать перспективы того или иного сервиса ATM.

Стандарт, определяющий интерфейс между операторами и пользователями ATM, называется Public User Network Interface или Public UNI. Этот интерфейс определяется для различных значений скорости. Первые услуги ATM предлагались в основном со скоростью T3 (45 Мбит/с). Сейчас многие операторы предлагают скорость 155 Мбит/с и выше, но такая полоса обычно не требуется пользователями, да и стоимость подобных услуг весьма высока. Для большинства пользователей, планирующих организовать доступ к ATM или создать частную сеть ATM, основной проблемой является стоимость оборудования.

## ГЛАВА 10 АДМИНИСТРИРОВАНИЕ СЕТЕЙ

Для обеспечения эффективной работы любой сети необходимо выполнять некоторые административные задачи: резервное копирование данных, управление заданием печати, наблюдение за правами доступа пользователей и мерами безопасности, добавление нового оборудования и программного обеспечения по мере роста сети, подключение новых пользователей и удаление некоторых из уже существующих и т.д.

Сетевое администрирование распространяется на пять основных областей, с которыми должен быть хорошо знаком администратор сети:

- управление пользователями — создание и поддержка учетных записей пользователей, управление доступом пользователей к ресурсам;
- управление ресурсами — установка и поддержка сетевых ресурсов;
- управление конфигурацией – планирование конфигурации сети, ее расширение, а также ведение необходимой документации;
- управление производительностью – мониторинг и контроль за сетевыми операциями для поддержания и улучшения производительности системы;
- поддержка — предупреждение, выявление и решение проблем сети.

Учитывая область сетевого управления, можно составить список задач, за выполнение которых отвечает администратор сети:

- создание учетных записей пользователей и управление ими;
- защита данных;
- обучение и поддержка пользователей (при необходимости);
- модернизация существующего программного обеспечения и установление нового;
- архивирование;
- предупреждение потерь данных;
- мониторинг и управление пространством для хранения данных на сервере;
- настройка сети для достижения максимальной производительности;
- резервное копирование данных;
- защита сети от вирусов;
- решение сетевых проблем;
- модернизация и замена компонентов сети (при необходимости);
- добавление в сеть новых компьютеров.

Помимо этого администратор может заниматься администрированием электронной почты, тогда в его функции дополнительно будет входить:

- установка приложений e-mail и организация центрального почтового сервера;
- управление доступом к системе электронной почты и назначение паролей;
- обучение пользователей процедурам, возможностям, этикету e-mail;
- выделение достаточного дискового пространства на почтовом сервере.

Каждому, кто работает в сети, необходимо выделить учетную запись пользователя. Учетная запись состоит из имени пользователя и назначенных ему параметров входа в систему. Эта информация вводится администратором и сохраняется сетевой операционной системой. При попытке пользователя войти в сеть его имя служит для проверки учетной записи.

Все сети имеют утилиты, которые помогают администраторам добавить в базу данных безопасности сети новые учетные записи. Этот процесс иногда называют «созданием пользователя».

Учетная запись содержит информацию, которая помогает идентифицировать пользователя в системе безопасности сети. Она включает:

- имя и пароль пользователя;
- права пользователя на доступ к ресурсам системы;
- группы, к которым относится учетная запись.

Эти данные необходимы администратору для создания новой учетной записи. При этом необходимо заполнить ряд полей, назначение которых поясним ниже.

Большинство сетей позволяет администраторам присваивать пользователям некоторые дополнительные параметры, в том числе:

- время регистрации — ограничение времени, в течение которого пользователь может войти в сеть;
- домашний каталог — предоставление пользователю места для хранения его личных файлов;
- продолжительность действия учетной записи — ограничение времени «пробытия» некоторых пользователей в сети.

Администратор в своей работе реализует и другую возможность – создание для некоторых пользователей сетевого окружения. Это необходимо для поддержки определенного уровня безопасности или для поддержки пользователей, не овладевших компьютерами и сетями в такой степени, чтобы самостоятельно работать с этой технологией. Администратор может создавать профили (profiles) для управления средой пользователей, в которой они оказываются после входа в систему. К среде относятся сетевые подключения и доступные программы,

а также подключения к принтерам, настройки языков и стандартов, настройки звуков, настройки мыши, настройки экрана.

К параметрам профилей, кроме того, иногда относятся специальные условия входа в систему и информация о том, где пользователь может хранить свои файлы.

Сетевые операционные системы поставляются с заранее созданными пользовательскими учетными записями, которые автоматически активизируются при установке системы. Известно несколько типов таких учетных записей.

При установке сетевой операционной системы автоматически создается учетная запись пользователя, обладающая полной «властью» в сети. Именно на него возлагаются следующие функции: формирование сети, установка начальных параметров защиты, создание учетных записей других пользователей.

В сетевой среде Microsoft этот пользователь носит имя Administrator (администратор). В среде Novell он известен как Supervisor (супервизор).

Обычно тот, кто установил операционную систему, первым входит в сеть. Войдя в сеть с учетной записью администратора, он имеет полный контроль над всеми сетевыми функциями.

Другой стандартный пользователь, создаваемый программой установки, называется Guest (гость). Эта учетная запись предназначена для людей, которые не являются полноправными пользователями сети, однако нуждаются во временном доступе к ней. Некоторые сетевые операционные системы, например, Microsoft Windows NT Server, после установки оставляют учетную запись гостя отключенной. Администратор сети может ее активизировать.

Пароли (passwords) обеспечивают защиту сетевой среды. Поэтому первая задача администратора при установке параметров своей учетной записи – изменить пароль. Тем самым он предотвратит и несанкционированный вход в сеть пользователей с правами администратора, и создание ими учетных записей.

Каждый пользователь должен придумать себе уникальный пароль и хранить его в тайне. В особо важных случаях надо обязать пользователей периодически менять свои пароли. Многие сетевые операционные системы предлагают средства, которые автоматически вынуждают пользователей делать это через заданный администратором промежуток времени.

В ситуациях, когда безопасность не столь существенна или права доступа ограничены (как в учетной записи гостя), можно модифицировать учетную запись так, чтобы для входа в сеть какого-то конкретного пользователя пароль не требовался.

Как только пользователи, которым при операциях с паролями помогал администратор, приобретут некоторый опыт, администратор в праве определить приемлемую для них политику защиты паролями.

Сети могут поддерживать тысячи учетных записей. Возникаю ситуации, когда администратор должен производить одни и те же действия над каждой из этих записей или, по крайней мере, над значительной их частью.

Иногда администратор вынужден посылать одно и то же сообщение большому количеству пользователей (извещая их о каком-либо событии), или разрешать доступ к определенным ресурсам только известной группе пользователей. Для этого администратору необходимо модифицировать каждую учетную запись конкретного пользователя, изменяя в ней его права доступа. Если 100 человек нуждаются в разрешении на использование какого-нибудь ресурса, администратор должен по очереди предоставлять это право каждому из ста.

Большинство сетей решает эту проблему автоматически, предлагая объединить отдельные пользовательские учетные записи в одну учетную запись специального типа, называемую группой. Группа (group) – это учетная запись, включающая в себя другие учетные записи. Основная цель создания групп — упростить администрирование. Благодаря группам администраторы могут оперировать большим числом пользователей так, как будто они работают с одним сетевым пользователем.

Если 100 учетных записей объединены в группу, администратор может послать группе одно сообщение, и оно дойдет до каждого члена этой группы. Аналогично право на доступ к ресурсу можно присвоить группе, и все ее члены получат его.

Поскольку группы — очень мощный инструмент администрирования, при планировании сети им необходимо уделять особое внимание. Опытные администраторы знают, что практически не должно быть индивидуальных пользователей сети. Каждый пользователь будет разделять с другими определенные привилегии и обязанности. Привилегии (rights) разрешают пользователю выполнять в системе некоторые действия, например, проводить ее резервное копирование. Привилегии относятся системе в целом и этим отличаются от прав. Права (permissions) и привилегии должны быть присвоены группам так, чтобы администратор мог обращаться с ними, как с одиночными пользователями.

Группы помогают осуществлять следующие действия:

- 1) предоставить доступ к ресурсам, таким, как файлы, каталоги и принтеры. Права, предоставленные группе, автоматически предоставляются ее членам;
- 2) предоставить привилегии для выполнения системных задач, таких, как резервное копирование, восстановление файлов с резервных копий или изменение системного времени. По умолчанию ни одному из пользователей ни одна из привилегий не присваивается. Пользователи, как правило, получают привилегии через членство в группах;
- 3) упростить связь за счет уменьшения количества подготавливаемых и передаваемых сообщений.

Создание групп подобно созданию учетной записи индивидуального пользователя. Большинство сетей имеют утилиты, с помощью которых администратор может формировать новые группы. В Microsoft Windows NT Server эта программа называется User Manager for Domains и находится в группе программ Administrative Tools.

Основное различие между созданием группы и созданием индивидуального пользователя состоит в том, что группа должна «знать», какие пользователи являются ее членами. Поэтому задача администратора — выбрать соответствующих пользователей и присвоить их группе.

Microsoft Windows NT Server использует группы четырех типов:

- локальные (local) группы реализуются в базе данных учетных записей отдельного компьютера. Локальные группы состоят из учетных записей пользователей, которые имеют права и привилегии на локальном компьютере, и учетных записей глобальных групп.
- глобальные (global) группы используются в границах всего домена. Глобальные группы регистрируются на главном контроллере домена (PDC) и могут содержать только тех пользователей, чьи учетные записи находятся в базе данных этого домена.
- специальные (special) группы обычно используются Windows NT Server для внутренних нужд.
- встроенные (built-in) группы. Некоторые функции групп этого типа общие для всех сетей. К ним относятся большинство задач администрирования и обслуживания. Чтобы выполнять некоторые стандартные операции, администраторы должны создавать учетные записи пользователей и группы с соответствующими привилегиями, однако многие поставщики сетей избавляют администраторов от этих хлопот, предлагая им встроенные локальные или глобальные группы. Встроенные группы делятся на три категории:
  - администраторы — пользователи этих групп имеют максимально возможные привилегии;
  - операторы — пользователи этих групп имеют ограниченные административные возможности для выполнения специфических задач;
  - другие — пользователи этих групп выполняют ограниченные задачи.

Простейший способ предоставить одинаковые права большому количеству пользователей — присвоить эти права группе, а затем добавить в группу выбранных пользователей. Аналогично добавляются пользователи во встроенную группу. Например, если администратор хочет, чтобы какой-то пользователь выполнял в сети административные задачи, он сделает этого пользователя членом группы Administrators.

Иногда администратору приходится исключать из сетевого обращения какую-нибудь учетную запись. Для этого используется блокирование или удаление этой учетной записи.

Если учетную запись заблокировать, она по-прежнему будет находиться в базе данных учетных записей сети, однако никто не сможет с ее помощью войти в сеть. Блокированная учетная запись как бы не существует.

Администратору следует отключить учетную запись сразу после того, как пользователь закончил работать с ней. Если станет ясно, что учетная запись вообще больше не понадобится, ее можно удалить.

Для блокирования учетных записей пользователей в Windows NT Server служит окно User Properties программы User Manager for Domains. Чтобы заблокировать пользователя, дважды щелкните имя его учетной записи, установите флажок Account Disabled, а затем нажмите Ok. Теперь учетная запись заблокирована.

Удаление учетной записи уничтожает информацию о пользователе в базе данных учетных записей сети. Пользователь больше не сможет получить доступ к сети.

Процесс удаления пользователя обычно несложен: надо выбрать имя учетной записи и нажать клавишу Delete. В Microsoft Windows NT Server, например, для удаления учетных записей пользователей служит программа User Manager for Domains. Выберите учетную запись, которую нужно удалить, затем нажмите клавишу Delete. В окне предупреждения щелкните Ok. В появившемся окне подтверждения операции щелкните Yes, если Вы действительно хотите удалить учетную запись.

При удалении учетной записи навсегда удаляются все связанные с ней права и привилегии. При повторном создании учетной записи с этим же именем права и привилегии восстановлены не будут. Это происходит потому, что при повторном создании учетной записи будет создан новый уникальный идентификатор защиты (SID).

После установки и запуска сети администратор должен быть уверен в том, что она работает эффективно. Для этого ему приходится следить за производительностью сети и управлять всеми факторами, которые влияют на нее.

Масштаб задач по управлению сетью зависит от:

- размера сети;
- численности и профессионализма сотрудников, которые обеспечивают поддержку сети;
- средств, выделяемых на поддержку сети;
- ожидаемой отдачи от использования сети.

Небольшую одноранговую сеть, состоящую из 10 или 12 компьютеров, может контролировать (визуально) один человек, тогда как для надлежащего мониторинга большой сети или глобальной сети (ГВС) требуется специальный персонал и соответствующее оборудование.

Самый простой метод обеспечить безотказную работу сети — ежедневно наблюдать за определенными аспектами ее функционирования. Постоянно контролируя сеть можно вовремя заметить снижение производительности на любых ее участках.

Существует широкий спектр средств сетевого администратора, позволяющих управлять ресурсами локального компьютера, общими сетевыми ресурсами, а также получать статистические данные и устранять неполадки. Ниже представлены некоторые наиболее важные средства, о которых необходимо знать каждому сетевому администратору. Некоторые из этих средств предназначены для всех пользователей, а другими должны пользоваться только системные администраторы.

Системный монитор — это средство, позволяющее получить данные об эффективности функционирования оборудования и программного обеспечения. Данное мощное средство используется для выполнения следующих задач:

- выполнение базовых замеров, с которыми будут сравнивать бузующие результаты;
- выявление эффекта изменений в конфигурации оборудования и программного обеспечения через сравнение новых показателей с предыдущими замерами;
- обоснование необходимости модернизации оборудования путем выявления «узких» мест;
- диагностика проблем быстрей действия на локальном и удаленных компьютерах.

Большинство сетевых операций складывается из совместных действий нескольких устройств. Каждое устройство на выполнение своей части операции требует некоторого времени. Если какое-либо устройство расходует заметно больше времени по сравнению с другими, возникают проблемы с производительностью системы в целом. Такое «тормозящее устройство» называют «узким местом».

Это средство используется для сбора и отображения в виде диаграмм информации о дисках, файловой системе, процессоре, ядре операционной системы, управлении памятью и сети.

Чаше всего «узкими местами» сервера являются такие устройства, как процессоры, сетевые платы, контроллеры дисков, среда передачи. Устройство может стать «узким местом» в силу того, что оно имеет недостаточную мощность для выполнения предлагаемых задач, медленно работает либо неэффективно используется, расходует больше системных ресурсов чем следует. Хороший мониторинг распознает эти недостатки и выдает информацию, которая облегчает поиск проблемных компонент.

Инспектор сети — это средство, позволяющее легко создавать, управлять и следить за удаленными общими сетевыми ресурсами. Благодаря ему можно сделать ресурс общим в сети, прекратить совместное использование ресурса, а также отобразить список всех общих ресурсов, открытых файлов и подключенных пользователей. Также можно принудительно закрывать файлы и отключать пользователей, если возникнет необходимость удалить общий ресурс. Все эти действия выполняются удаленно через сеть.

Программное обеспечение управления сетью, как и большинство сетевых компонентов, подчиняется стандартам, созданным производителями сетевого оборудования. Один из таких стандартов — простой протокол управления сетью — SNMP (Simple Network Management Protocol).

При использовании SNMP программы, называемые агентами, загружаются на каждое управляемое устройство. Агенты собирают статистические данные, контролируя сетевой трафик и функционирование компонентов сети. Собранные сведения хранятся в базе данных управленческой информации (Management Information Base — MIB).

К компонентам SNMP относятся: концентраторы, серверы, интерфейсные платы, маршрутизаторы и мосты, другое специальное сетевое оборудование.

Чтобы накопить информацию, специальная программа, известная как консоль управления, регулярно опрашивает агентов и загружает информацию из их MIB. Накопив необработанные данные, программа управления предоставляет информацию в форме графиков, схем и диаграмм или пересылает информацию в указанную базу данных для последующего анализа.

Если какой-либо из показателей выйдет за пределы, установленные администратором, программа управления известит администратора, выдав предупреждение на экран компьютера или отправив его на пейджер. Затем с помощью консоли управления персонал поддержки может произвести изменения в сети.

Удаленный доступ к сети позволяет вашему компьютеру из отдаленного места связаться по телефону с сетью и после соединения стать ее удаленным узлом.

При использовании аналоговой телефонной сети на каждом конце соединения необходим модем. Модем (сокращенно от «модулятор-демодулятор») преобразует цифровые сигналы от ПК в аналоговые сигналы для передачи их по телефонным линиям. Данное действие называется модуляцией. На другом конце соединения другой модем конвертирует аналоговые сигналы, поступающие по телефонной линии, в цифровые сигналы. Это называется демодуляцией.

И компьютер-клиент удаленного доступа, и сервер нуждаются в собственном модеме. Для того, чтобы передавать данные на высокой скорости, оба модема на конце соединения должны поддерживать такую скорость. Реальная скорость передачи данных зависит от качества линии и количества помех во время сеанса связи.

При реализации удаленного доступа к сети существуют два способа уменьшить количество потенциальных проблем:

1) при выборе модемов для использования, например, с Windows 95/98/NT, позаботиться о совместимости оборудования с операционной системой;

2) на обоих концах соединения лучше использовать модемы одной модели и от одного производителя. Мелкие отличия в функционировании модемов от разных производителей (или с отличающимся набором возможностей) станут источниками проблем, очень плохо поддающихся выявлению.

Рассмотрим администрирование в ЦСИО. В этих сетях большое внимание уделено средствам контроля сети, которые позволяют маршрутизировать вызовы для установления соединений с абонентом сети, а также осуществлять мониторинг и управление сетью. Управляемость сети обеспечивается интеллектуальностью коммутаторов и конечных узлов сети, поддерживающих стек протоколов, в том числе и специальных протоколов управления.

Продукты ЦСИО обслуживают потребности в удаленном доступе пользователей, работающих дома, предприятий малого бизнеса и дочерних отделений компаний. Значительную долю этого рынка составляют пользователи, которые плохо разбираются во всех сложностях и тонкостях, связанных с установкой, работой и обслуживанием локальных сетей и соответствующих операционных систем.

ISP-компании и предприятия, развертывающие ЦСИО для доступа к удаленным офисам, придерживаются в вопросах установки оборудования, настройки конфигурации в удаленных филиалах и текущего администрирования нескольких стратегий:

- 1) обучить абонентов и сотрудников работе с конкретным оборудованием и вооружить их знаниями, необходимыми для настройки конфигурации и для обслуживания удаленных локальных сетей;
- 2) заставить пользователей или персонал, отвечающих за эксплуатацию, установить оборудование в удаленной среде и подключить его к порту консоли, что позволит квалифицированным сотрудникам удаленно выполнять настройку конфигурации и проверку средств;
- 3) создать централизованную конфигурацию и управление заранее настроенным оборудованием перед установкой в удаленном офисе.

Каждый из этих методов имеет свои сложности и дает различные степени успеха. В конечном счете пользователи должны взять на себя некоторую ответственность за текущую работу и сопровождение оборудования, так как неизбежны проблемы со средствами ISDN, кабелями локальных сетей, программным обеспечением хост-систем и мостов/маршрутизаторов.

Критически важными элементами для развертывания продуктов ISDN являются системы управления конфигурацией. Лучше выбирать оборудование, предусматривающее простые в использовании системы управления конфигурацией с эффективными средствами диагностики. Диагностические средства обеспечивают доступ к информации, необходимой для локализации проблемы, а также возможности ее устранения.

По этим и многим другим причинам средства диагностики являются критически важными для продуктов удаленного доступа. Ниже перечислены наиболее полезные возможности диагностики:

- мониторинг событий ISDN. Такие уведомления, как идентификация отказа конечной точки, потеря или отсутствие сигнала передачи данных, отказ регистрации \*\*\*, позволяют определить корректность настройки конфигурации BRI-интерфейса пользователем или телефонной компанией;
- мониторинг на уровне глобальной сети. Счетчик ошибок в передаваемых и принимаемых по ISDN BRI кадрах, включая контроль с использованием циклического избыточного кода (CRC) и отброшенных кадров, позволяет определить пригодность качества сигнала телефонной компании для передачи данных. Кроме того, такие ошибки помогают пользователю локализовать причину низкой производительности;
- мониторинг локальной сети Ethernet. Счетчики передачи/приема и счетчики ошибок полезно использовать для определения неработоспособности или неверного функционирования некоторого компонента в среде локальной сети (разъема кабеля, порта концентратора и т.п.);
- мониторинг трафика. Определение загрузки ISDN полезно для выявления потребности в дополнительных каналах или в сжатии информации. Это позволяет обнаружить, что ISDN больше не отвечает потребностям локальной сети;
- клиент PING. Средство PING выполняет эхо-передачу пакетов «запрос/ответ» протокола ICMP для тестирования соединения между хост-системами и маршрутизаторами на уровне IP. PING можно использовать для тестирования каналов ISDN с коммутацией по запросу;
- трассировка маршрута. Утилита трассировки маршрута (TRA-CEROUTE) посылает последовательность пакетов IP целевой хост-системе или маршрутизатору, инициируя ответ от каждого маршрутизатора на всем пути до этой хост-системы. На основе всех полученных IP-адресов строится маршрут к целевой хост-системе. Трассировку полезно использовать для определения корректности конфигурации маршрутизатора IP;
- протокол двухточечной связи (PPP) и мониторинг пакетов в реальном времени на более высоком уровне. Предоставляет возможность наблюдать за установлением связи по протоколу PPP. Это помогает определить, соответствует ожидаемому варианту обмен информацией аутентификации по протоколам PPP, LCP, IPCP;
- мониторинг пакетов более высокого уровня. Полезно применять в тех ситуациях, когда линия функционирует корректно, но наблюдаются другие проблемы межсетевое взаимодействия.

Продукты ISDN предлагают четыре типа интерфейсов настройки конфигурации:

- 1) для внешних устройств применяются системы настройки конфигурации, управляемые с помощью меню и форм. Эти устройства обращаются к устройству непосредственно через порт консоли и работают в режиме эмуляции терминала VT100 (к примеру TERMINAL в Windows, Zterm для Macintosh);
- 2) для внешних устройств применяется интерпретатор, работающий в режиме командной строки. Для доступа используется порт консоли (порт управления) или сеть Ethernet (через Telnet);
- 3) для конфигурирования внешних и встроенных устройств применяется графический интерфейс на рабочей станции Unix или на ПК с соответствующей системой, поддерживающей работу с окнами (Windows 9x, Windows 3.x, X Windows System и т.п.);

4) для настройки конфигурации внешних мостов и маршрутизаторов используется интерфейс браузера на базе языка HTML. Браузеры доступны на ПК с клиентским приложением Web и со стек протоколов TCP/IP.

## ГЛАВА 11 МОНИТОРИНГ И АНАЛИЗ СЕТЕЙ

Постоянный контроль за работой локальной сети необходим для поддержания ее в работоспособном состоянии. Ввиду важности этой функции ее часто отделяют от других функций систем управления и реализуют специальными средствами. Такое разделение функций контроля и управления полезно для небольших сетей, для которых установка интегрированной системы управления экономически нецелесообразна. Использование автономных средств контроля помогает администратору сети выявить проблемные участки и устройства сети. Их отключение или реконфигурацию он может выполнять в этом случае вручную. Процесс контроля работы сети обычно делат на два этапа: мониторинг и анализ. На этапе мониторинга выполняется процедура сбора первичных данных о работе сети: статистики о количестве циркулирующих в сети кадров и пакетов различных протоколов, состоянии портов концентраторов, коммутаторов и маршрутизаторов и т.п.

Далее выполняется этап анализа, под которым понимается более сложный и интеллектуальный процесс осмысления собранной на этапе мониторинга информации, сопоставления ее с данными, полученными ранее, и выработки предположений о возможных причинах замедленной или ненадежной работы сети.

Задачи мониторинга решаются программными и аппаратными измерителями, тестерами, сетевыми анализаторами, встроенными средствами мониторинга коммуникационных устройств, а также агентами систем управления. Задача анализа требует более активного участия человека и использования таких сложных средств, как экспертные системы, аккумулирующие практический опыт многих сетевых специалистов.

### 11.1. Диагностика сетей с применением протоколов SNMP и CMIP

Обслуживание и диагностирование больших многосегментных, многопротокольных сетей, размещенных на большой территории, а в некоторых случаях и в нескольких городах, представляет собой сложную проблему.

Большая часть работы по управлению сетями состоит из слежения за работой устройств, контроля производительности компьютерной сети, диагностики проблем и устранения их причин. Для этого были разработаны два практически аналогичных протокола управления сетями: простой протокол для управления вычислительной сетью SNMP (Simple Network Management Protocol), который разработан для решения коммуникационных проблем TCP/IP, и протокол общего управления информацией CMIP (Common Management Information Protocol), разработанный как часть стандартной модели OSI и являющийся продуктом международного комитета по стандартизации.

Каждый из этих протоколов имеет свои преимущества, и производители сетевых систем разрабатывают средства управления сетями, объединяющие оба протокола.

Протоколы SNMP и CMIP имеют общую цель, состоящую в облегчении задач управления и диагностики при работе в сетях. Оба протокола используют концепцию MIB (Management Information Base). В базе MIB хранятся не только данные о состоянии устройства, но и управляющая информация, воздействующая на это устройство. MIB состоит из набора переменных, тестовых точек и контрольных параметров, которые поддерживаются всеми устройствами сети и могут контролироваться администратором сети. Оба протокола поддерживают также расширения MIB, вводимые различными производителями с целью сбора большего количества служебной информации при запросах в сетях. Основными расширениями MIB являются стандарты MIB-I и MIB-II, а также версия базы данных для удаленного управления RMON MIB. Стандарт MIB-I разрабатывался с жесткой ориентацией на управление маршрутизаторами, поддерживающими протоколы стека TCP/IP. Стандарт MIB-II ориентирован на контроль и управление. Стандарт RMON MIB специально ориентирован на сбор детальной статистики по протоколу Ethernet, кроме того, он поддерживает функцию построения агентом зависимостей статистических характеристик от времени.

При разработке систем управления компьютерными сетями производители сочетают возможности протоколов SNMP и CMIP. Совместимость различных реализаций протоколов MIB позволяет производителям создавать системы управления сетями, которые смогут принимать информацию как от SNMP, так и от CMIP, и хранить ее в общем формате.

Различие между протоколами SNMP и CMIP состоит в способах, при помощи которых они извлекают и выдают данные о вычислительных сетях. Эти протоколы предлагают различные функции, требуют разных затрат вычислительной мощности и используют разное количество памяти. Каждый из этих протоколов использует собственный набор протоколов низкого уровня для передачи и приема информации, необходимой для управления сетями. Оба протокола поддерживаются различными комитетами по стандартизации.

Протоколы SNMP и CMIP имеют одинаковые функции извлечения данных, но делают это разными способами. Протокол SNMP предназначен для получения сведений о конкретных устройствах, тогда как CMIP больше ориентирован на извлечение наборов данных. При использовании SNMP необходима точная формулировка запроса об интересующем устройстве. В случае CMIP можно сделать общий запрос и затем уточнить его. Протокол CMIP рассчитан на интеллектуальных агентов, которые могут по одной команде от менеджера выполнить сложную последовательность действий.

Протокол SNMP работает через опросы, т.е. центральное устройство управления периодически опрашивает каждое устройство в ЛВС для определения его статуса. В протоколе CMIP используются отчеты, в которых устройства информируют центральную управляющую станцию об изменениях в своем статусе. При большом числе устройств протокол SNMP может вызвать большой трафик ЛВС и замедлить ее работу, но он может работать с любыми устройствами, включая самые примитивные, которые не могут сами определить свою неисправность.

Система управления ЛВС на базе протокола SNMP может быть меньших размеров, более быстройдействующей и менее дорогостоящей по сравнению с CMIP. Система CMIP требует более быстройдействующего компьютера и большей памяти.

Протокол SNMP легко реализуется на DOS-машине в виде резидентной программы. Это возможно для протокола CMIP, который имеет большие возможности и характеристики, но часто не все его возможности используются в полной мере.

Использование в протоколе CMIP сеансового обмена информацией делает его более удобным при необходимости получения большого количества данных. Однако это может затруднить управление сетью при возникновении неполадок. Если ЛВС выйдет из строя или практически перестанет функционировать, SNMP, действующий на уровне дейтаграмм, будет продолжать посылать управляющие запросы до тех пор, пока один из них не пройдет.

### 11.2. Классификация средств мониторинга и анализа

Все многообразие средств, применяемых для анализа и диагностики вычислительных сетей, можно разделить на несколько крупных классов:

- агенты систем управления, поддерживающие функции одной из стандартных MIB и поставляющие информацию по протоколу SNMP или CMIP. Для получения данных от агентов обычно требуется наличие системы управления, собирающей данные от агентов в автоматическом режиме;

- встроенные системы диагностики и управления. Эти системы выполняются в виде программно-аппаратных модулей, устанавливаемых в коммуникационное оборудование, а также в виде программных модулей, встроенных в операционные системы. Они выполняют функции диагностики и управления только одним устройством, и в этом их основное отличие от централизованных систем управления. Примером средств этого класса может служить модуль управления многосегментным повторителем Ethernet, реализующий функции автосегментации портов при обнаружении неисправностей, присписывания портов внутренним сегментам повторителя и некоторые другие. Как правило, встроенные модули управления «по совместительству» выполняют роль SNMP-агентов, поставляющих данные о состоянии устройства для систем управления;

- анализаторы протоколов (Protocol analyzers). Представляют собой программные или аппаратно-программные системы, которые ограничиваются в отличие от систем управления лишь функциями мониторинга и анализа трафика в сетях. Хороший анализатор протоколов может захватывать и декодировать пакеты большого количества протоколов, применяемых в сетях, — обычно несколько десятков. Анализаторы протоколов позволяют установить некоторые логические условия для захвата отдельных пакетов и выполняют полное декодирование захваченных пакетов, то есть показывают в удобной для специалиста форме вложенность пакетов протоколов разных уровней друг в друга с расшифровкой содержания отдельных полей каждого пакета;

- экспертные системы. Этот вид систем аккумулирует знания технических специалистов о выявлении причин аномальной работы сетей и возможных способах приведения сети в работоспособное состояние. Экспертные системы часто реализуются в виде отдельных подсистем различных средств мониторинга и анализа сетей: систем управления сетями, анализаторов протоколов, сетевых анализаторов. Простейшим вариантом экспертной системы является контекстно-зависимая система помощи. Более сложные экспертные системы представляют собой, так называемые базы знаний, обладающие элементами искусственного интеллекта. Примерами таких систем являются экспертные системы, встроенные в систему управления Spectrum компании Cabletron и анализатора протоколов Sniffer компании Network General. Работа экспертных систем состоит в анализе большого числа событий для выдачи пользователю краткого диагноза о причине неисправности сети;

- оборудование для диагностики и сертификации кабельных систем. Условно это оборудование можно поделить на пять основных групп: сетевые мониторы, сетевые анализаторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры.

Сетевые мониторы предназначены для тестирования кабелей различных категорий. Сетевые мониторы собирают также данные о статистических показателях трафика — средней интенсивности общего трафика сети, средней интенсивности потока пакетов с определенным типом ошибки и т.п.

Сетевые анализаторы выполняют анализ трафика в реальном времени, захват, преобразование, передачу пакетов, а также устранение неполадок в сети.

Устройства для сертификации кабельных систем выполняют сертификацию в соответствии с требованиями одного из международных стандартов на кабельные системы.

Кабельные сканеры используются для диагностики медных кабельных систем.

Тестеры предназначены для проверки кабелей на отсутствие физического разрыва;

- многофункциональные портативные устройства анализа и диагностики. В связи с развитием технологии больших интегральных схем появилась возможность производства портативных приборов, которые совмещали бы функции нескольких устройств: кабельных сканеров, сетевых мониторов и анализаторов протоколов.

### **11.2.1. Анализаторы протоколов**

Анализатор протоколов представляет собой либо специализированное устройство, либо персональный компьютер, обычно переносной (Notebook), оснащенный специальной сетевой картой и соответствующим программным обеспечением. Применяемые сетевая карта и программное обеспечение должны соответствовать технологии сети (Ethernet, Token Ring, FDDI, Fast Ethernet). Анализатор подключается к сети точно так же, как и обычный узел. Отличие состоит в том, что анализатор может принимать все пакеты данных, передаваемые по сети, в то время как обычная станция — только адресованные ей. Для этого сетевой адаптер анализатора протоколов переводится в режим «беспорядочного» захвата (promiscuous mode).

Программное обеспечение анализатора состоит из ядра, поддерживающего работу сетевого адаптера и программного обеспечения, декодирующего протокол канального уровня, с которым работает сетевой адаптер, а также наиболее распространенные протоколы верхних уровней (IP, TCP, ftp, telnet, HTTP, IPX, NCP, NetBEUI, DECnet и т.п.) В состав некоторых анализаторов может также входить экспертная система, которая позволяет выдавать пользователю рекомендации о том, какие эксперименты следует проводить в данной ситуации, что могут означать те или иные результаты измерений, как устранить некоторые виды неисправности сети.

Анализаторы протоколов имеют некоторые общие свойства:

- возможность (кроме захвата пакетов) измерения среднестатистических показателей трафика в сегменте локальной сети, в котором установлен сетевой адаптер анализатора. Обычно измеряется коэффициент использования сегмента, матрицы перекрестного трафика узлов, количество нормальных и испорченных кадров, прошедших через сегмент;

- возможность работы с несколькими агентами, поставляющими захваченные пакеты из разных сегментов локальной сети. Эти агенты чаще всего взаимодействуют с анализатором протоколов по собственному протоколу прикладного уровня, отличному от SNMP или CMIP;

- наличие развитого графического интерфейса, позволяющего представить результаты декодирования пакетов с разной степенью детализации;

- фильтрация захватываемых и отображаемых пакетов. Условия фильтрации задаются в зависимости от значения адресов назначения и источника, типа протокола или значения определенных полей пакета. Пакет либо игнорируется, либо записывается в буфер захвата. Использование фильтров значительно ускоряет и упрощает анализ, так как исключает захват или просмотр ненужных в данных момент пакетов;

- использование триггеров. Триггеры — это задаваемые администратором некоторые условия начала и прекращения процесса захвата данных из сети. Такими условиями могут быть: время суток, продолжительность процесса захвата, появление определенных значений в кадрах данных. Триггеры могут использоваться совместно с фильтрами, позволяя более детально и тонко проводить анализ, а также продуктивнее расходовать ограниченный объем буфера захвата;

- многоканальность. Некоторые анализаторы протоколов позволяют проводить одновременную запись пакетов от нескольких сетевых адаптеров, что удобно для сопоставления процессов, происходящих в разных сегментах сети;

- возможности анализа проблем сети на физическом уровне у анализаторов протоколов минимальные, поскольку всю информацию они получают от стандартных сетевых адаптеров. Поэтому они передают и обобщают информацию физического уровня, которую сообщает им сетевой адаптер, а она во многом зависит от типа сетевого адаптера. Некоторые сетевые адаптеры сообщают более детальные данные об ошибках кадров и интенсивности коллизий в сегменте, а некоторые вообще не передают такую информацию верхним уровням протоколов, на которых работает анализатор протоколов.

### **11.2.2. Сетевые мониторы**

Сетевые мониторы представляют собой эталонные измерительные приборы для диагностики и сертификации кабелей и кабельных систем. Они могут с высокой точностью измерить все электрические параметры кабельных систем, а также работают на более высоких уровнях стека протоколов. Сетевые мониторы генерируют синусоидальные сигналы в широком диапазоне частот, что позволяет измерять на приемной паре амплитудно-частотную характеристику и перекрестные наводки, затухание и суммарное затухание. Сетевой монитор представляет собой лабораторный прибор больших размеров, достаточно сложный в обращении.

Многие производители дополняют сетевые мониторы функциями статистического анализа трафика — коэффициента использования сегмента, уровня широковещательного графика, процента ошибочных кадров, а также функциями анализатора протоколов, которые обеспечивают захват пакетов разных протоколов в соответствии с условиями фильтров и декодирование пакетов.

Сетевыми мониторами также часто называют компьютеры, подключаемые к сети для контроля трафика всей сети или выделенной ее части. С помощью проверки данных в каждом пакете информации, сетевые мониторы могут создавать статистические сообщения об использовании сети, типах пакетов, числе переданных и

принятых пакетов сообщений каждым узлом сети и другую важную информацию. Сетевые мониторы на основе обыкновенных компьютеров относительно недороги и могут использоваться по одному на каждый сегмент в больших компьютерных сетях. Они обычно работают непрерывно, набирая информацию и контролируя неполадки в сети.

### **11.2.3. Сетевые анализаторы**

Сетевые анализаторы выполняют те же функции, что и сетевые мониторы, но, кроме того, задачей сетевых анализаторов является выяснение причин неполадок в сети и их устранение. Сетевые анализаторы предназначены для анализа трафика в реальном масштабе времени и имеют средства для перехватывания и декодирования пакетов, а также могут передавать собственные сообщения. Некоторые из них включают набор средств для экспертизы на определенные типы неполадок и имеют встроенные средства для проведения рефлектометрии. Наиболее сложные сетевые анализаторы снабжены специальными аппаратными средствами для обнаружения неполадок, незаметных на уровне обычных сетевых адаптеров. В последнее время разработчики этих систем стали включать элементы искусственного интеллекта в свои изделия.

Сетевые анализаторы являются сложными, дорогостоящими инструментами для обнаружения определенного сорта проблем в сетях. Эти приборы обладают гораздо более широкими возможностями, чем кабельные тестеры или различные программные средства, и могут применяться для идентификации неисправных устройств, обнаружения ошибок в конфигурации и «узких мест» сетей.

Сетевые анализаторы могут прослушивать пакеты, проходящие через сеть для анализа работы компьютерной сети. Анализатор также может выделять только те пакеты, которые удовлетворяют определенным критериям, перехватывать их и суммировать в файл для последующего разбора их содержания. Критерии отбора пакетов устанавливаются пользователем и могут быть направленными на выделение только ошибочных кадров, кадров от определенных рабочих станций и серверов, кадров больших размеров или содержащих определенный набор данных и т.п. Некоторые анализаторы позволяют увеличивать трафик сети, симулируя дополнительные узлы. Таким образом, пользователю остается только точно определить, какого рода ошибки нужно искать, а сетевой анализатор определит их с указанием устройства, вызывающего эти ошибки. Однако это не означает, что сетевые анализаторы способны заменить опытного специалиста. Напротив, только очень квалифицированные специалисты могут эффективно пользоваться этим прибором.

### **11.2.4. Различные типы инструментов для мониторинга**

Контрольно-измерительные приборы включают: рефлектометры, осциллографы, детекторы разрывов, измерители мощности, кабельные сканеры и тестеры и другие аналогичные продукты.

Рефлектометр — устройство для обнаружения обрывов, коротких замыканий и некачественных участков кабеля, которые могут влиять на производительность сети. Принцип работы рефлектометров состоит в посылке в кабель короткого импульса и анализе отраженного от конца кабеля сигнала (наподобие акустического локатора). Если на пути импульса встречается некачественный участок, рефлектометр анализирует отраженный сигнал и выдает результат. Хорошие рефлектометры находят место разрыва с точностью до нескольких десятков сантиметров. Рефлектометры часто используются при установке сети, но и также незаменимы и при решении проблем в уже установленных сетях.

Кабельные сканеры. Основное назначение кабельных сканеров — измерение электрических и механических параметров кабелей: длины кабеля, параметра NEXT, затухания, импеданса, схемы разводки пар проводников, уровня электрических шумов в кабеле. Точность измерений, произведенных этими устройствами, ниже, чем у сетевых анализаторов, но вполне достаточна для оценки соответствия кабеля стандарту.

Для определения местоположения неисправности кабельной системы (обрыва, короткого замыкания, неправильно установленного разъема и т.д.) используется метод «отраженного импульса» — TDR (Time Domain Reflectometry). Суть этого метода состоит в том, что сканер излучает в кабель короткий электрический импульс и измеряет время задержки до прихода отраженного сигнала. По полярности отраженного импульса определяется характер повреждения кабеля (короткое замыкание или обрыв). В правильно установленном и подключенном кабеле отраженный импульс почти отсутствует.

Точность измерения расстояния зависит от того, насколько точно известна скорость распространения электромагнитных волн в кабеле. В различных кабелях она будет разной. Скорость распространения электромагнитных волн в кабеле — NVP (Nominal Velocity of Propagation) обычно задается в процентах от скорости света в вакууме. Современные сканеры содержат в себе электронную таблицу данных о NVP для всех основных типов кабелей, что дает возможность пользователю устанавливать эти параметры самостоятельно после предварительной калибровки.

Кабельные сканеры — это портативные приборы, которые обслуживающий персонал может постоянно носить с собой.

Кабельные тестеры — это универсальный электроизмерительный прибор. Кабельные тестеры наиболее простые и дешевые приборы для диагностики кабеля. Они позволяют определить непрерывность кабеля, однако, в отличие от кабельных сканеров, не дают ответа на вопрос о том, в каком месте произошел сбой.

Расширенные тестеры кабеля работают над физическим уровнем. Эти тестеры способны отображать информацию о состоянии физического кабеля, а также информацию о количестве кадров, избытке коллизий, последних коллизиях, количестве ошибочных кадров, перегрузках, испускании маяка.

Тестеры могут отслеживать весь сетевой трафик, отдельные виды ошибок или трафик конкретного компьютера. Они проинформируют, какой именно сегмент кабеля или плата сетевого адаптера является причиной проблемы.

### 11.2.5. Многофункциональные портативные приборы мониторинга

В последнее время начали выпускаться многофункциональные портативные приборы, которые объединяют в себе возможности кабельных сканеров, анализаторов протоколов и даже некоторые функции систем управления, сохраняя в то же время такое важное свойство, как портативность. Многофункциональные приборы мониторинга имеют специализированный физический интерфейс, позволяющий выявлять проблемы и тестировать кабели на физическом уровне, который дополняется микропроцессором с программным обеспечением для выполнения высокоуровневых функций.

Рассмотрим типичный набор функций и свойств такого прибора, который оказывается очень полезным для диагностики причин разнообразных неполадок в сети, происходящих на всех уровнях стека протоколов, от физического до прикладного.

Интерфейс пользователя

Прибор обычно предоставляет пользователю удобный и интуитивно понятный интерфейс, основанный на системе меню. Графический интерфейс пользователя реализован на многострочном жидкокристаллическом дисплее и индикаторах состояния на светодиодах, извещающих пользователя о наиболее общих проблемах наблюдаемых сетей. Имеется обширный файл подсказок оператору с уровнем доступа в соответствии с контекстом. Информация о состоянии сети представляется таким образом, что пользователи любой квалификации могут ее быстро понять.

Функции проверки аппаратуры и кабелей

Многофункциональные приборы сочетают наиболее часто используемые на практике функции кабельных сканеров с рядом новых возможностей тестирования:

- сканирование кабеля позволяет измерять длину кабеля, расстояние до самого серьезного дефекта и распределение импеданса по длине кабеля. При проверке неэкранированной витой пары могут быть выявлены следующие ошибки: расщепленная пара, обрывы, короткое замыкание и другие виды нарушения соединения. Для сетей Ethernet на коаксиальном кабеле эти проверки могут быть осуществлены на работающей сети;

- функция определения распределения кабельных жил осуществляет проверку правильности подсоединения жил, наличие промежуточных разрывов и перемычек на витых парах. На дисплее выводится перечень связанных между собой контактных групп;

- функция определения карты кабелей используется для составления карты основных кабелей и кабелей, отходящих от центрального помещения;

- автоматическая проверка кабеля. В зависимости от конфигурации возможно определить длину, импеданс, схему подключения жил, затухание и параметр NEXT на частоте до 100 МГц. Автоматическая проверка выполняется для коаксиальных кабелей, экранированной витой пары с импедансом 150 Ом, неэкранированной витой пары с импедансом 100 Ом;

- целостность цепи при проверке постоянным током. Эта функция используется при проверке коаксиальных кабелей для верификации правильности используемых терминаторов и их установки;

- определение номинальной скорости распространения. Функция вычисляет номинальную скорость распространения (NVP) по кабелю известной длины и дополнительно сохраняет полученные результаты в файле для определяемого пользователем типа кабеля (User Defined cable type) или стандартного кабеля.

- комплексная автоматическая проверка пары «сетевой адаптер-концентратор». Этот комплексный тест позволяет последовательно подключить прибор между конечным узлом сети и концентратором. Тест дает возможность автоматически определить местонахождение источника неисправности — кабель, концентратор, сетевой адаптер или программное обеспечение станции;

- автоматическая проверка сетевых адаптеров. Проверяет правильность функционирования вновь установленных или «подозрительных» сетевых адаптеров. Для сетей Ethernet по итогам проверки сообщаются: MAC-адрес, уровень напряжения сигналов (а также присутствие и полярность импульсов Link Test для 10BASE-T). Если сигнал не обнаружен на сетевом адаптере, то тест автоматически сканирует соединительный разъем и кабель для их диагностики.

Функции сбора статистики

Эти функции позволяют в реальном масштабе времени проследить за изменением наиболее важных параметров, характеризующих «здоровье» сегментов сети. Статистика обычно собирается с разной степенью детализации по разным группам.

- Сетевая статистика

В этой группе собраны наиболее важные статистические показатели: коэффициент использования сегмента (utilization), уровень коллизий, уровень ошибок и уровень широковещательного графика. Превышение этими показателями определенных порогов в первую очередь говорят о проблемах в том сегменте сети, к которому подключен многофункциональный прибор.

- Статистика ошибочных кадров

Эта функция позволяет отслеживать все типы ошибочных кадров для определенной технологии. Например, для технологии Ethernet характерны следующие типы ошибочных кадров:

- укороченные кадры (Short frames). Это кадры, имеющие длину, меньше допустимой, то есть меньше 64 байт. Иногда этот тип кадров дифференцируют на два класса — просто короткие кадры (short), у которых имеется корректная контрольная сумма, и «коротышки» (runts), не имеющие корректной контрольной суммы. Наиболее вероятными причинами появления укороченных кадров являются неисправные сетевые адаптеры и их драйверы;

- удлиненные кадры (Jabbers). Это кадры, имеющие длину, превышающую допустимое значение в 1518 байт с хорошей или плохой контрольной суммой. Удлиненные кадры являются следствием затянувшейся передачи, которая появляется из-за неисправностей сетевых адаптеров;

- кадры нормальных размеров, но с плохой контрольной суммой (Bad FCS) и кадры с ошибками выравнивания по границе байта. Кадры с неверной контрольной суммой являются следствием множества причин — плохих адаптеров, помех на кабелях, плохих контактов, некорректно работающих портов повторителей, мостов, коммутаторов и маршрутизаторов. Ошибка выравнивания всегда сопровождается ошибкой по контрольной сумме, поэтому некоторые средства анализа трафика не делают между ними различий. Ошибка выравнивания может быть следствием прекращения передачи кадра при распознавании коллизии передающим адаптером;

- кадры-призраки (ghosts) являются результатом электромагнитных наводок на кабеле. Они воспринимаются сетевыми адаптерами как кадры, не имеющие нормального признака начала кадра — 10101011. Кадры-призраки имеют длину более 72 байт, в противном случае они классифицируются как удаленные коллизии. Количество обнаруженных кадров-призраков в большой степени зависит от точки подключения сетевого анализатора. Причинами их возникновения являются петли заземления и другие проблемы с кабельной системой.

Знание процентного распределения общего количества ошибочных кадров по их типам может многое подсказать администратору о возможных причинах неполадок в сети. Даже небольшой процент ошибочных кадров может привести к значительному снижению полезной пропускной способности сети, если протоколы, восстанавливающие искаженные кадры, работают с большими тайм-аутами ожидания квитанций. Считается, что в нормально работающей сети процент ошибочных кадров не должен превышать 0,01 %, то есть не более 1 ошибочного кадра из 10 000.

- Статистика по коллизиям

Эта группа характеристик дает информацию о количестве и видах коллизий, отмеченных на сегменте сети, позволяет определить наличие и местонахождение проблемы. Анализаторы протоколов обычно не могут дать дифференцированной картины распределения общего числа коллизий по их отдельным типам, в то же время знание преобладающего типа коллизий может помочь понять причину плохой работы сети.

Ниже приведены основные типы коллизий сети Ethernet:

- локальная коллизия (Local Collision). Является результатом одновременно передачи двух или более узлов, принадлежащих к тому сегменту, в котором производятся измерения. Если многофункциональный прибор не генерирует кадры, то в сети на витой паре или волоконно-оптическом кабеле локальной коллизии не фиксируются. Слэшом высокий уровень локальных коллизий является следствием проблем с кабельной системой;

- удаленная коллизия (Remote Collision). Эти коллизии происходят на другой стороне повторителя (по отношению к тому сегменту, в котором установлен измерительный прибор). В сетях, построенных на многопортовых повторителях (10Base-T, 10Base-FL/FB, 10Base-TX/FX/T4, Gigabit Ethernet). Все измеряемые коллизии являются удаленными (кроме тех случаев, когда анализатор сам генерирует кадры и может быть виновником коллизии). Не все анализаторы протоколов и средства мониторинга одинаковым образом фиксируют удаленные коллизии. Это происходит из-за того, что некоторые измерительные средства и системы не фиксируют коллизии, происходящие при передаче преамбулы;

- поздняя коллизия (Late Collision). Это коллизия, которая происходит после передачи первых 64 байт кадра (по протоколу Ethernet коллизия должна обнаруживаться при передаче первых 64 байт кадра). Результатом поздней коллизии будет кадр, который имеет длину более 64 байт и содержит неверное значение контрольной суммы. Чаще всего это указывает на то, что сетевой адаптер, являющийся источником конфликта, оказывается не в состоянии правильно прослушивать линию и поэтому не может вовремя остановить передачу. Другой причиной поздней коллизии является слишком большая длина кабельной системы или слишком большое количество промежуточных повторителей, приводящее к превышению максимального значения времени двойного оборота сигнала.

Средняя интенсивность коллизий в нормально работающей сети должна быть меньше 5 %. Большие всплески (более 20 %) могут быть индикатором кабельных проблем.

- Распределение используемых сетевых протоколов

Эта статистическая группа относится к протоколам сетевого уровня. На дисплее отображается список основных протоколов в убывающем порядке относительно процентного соотношения кадров, содержащих пакеты данного протокола к общему числу кадров в сети.

- Основные отправители (Top Senders)

Функция позволяет отслеживать наиболее активные передающие узлы локальной сети. Прибор можно настроить на фильтрацию по единственному адресу и выявить список основных отправителей кадров для данной станции. Данные отражаются на дисплее в виде диаграммы вместе с перечнем основных отправителей кадров.

- Основные получатели (Top Receivers)

Функция позволяет следить за наиболее активными узлами-получателями сети. Информация отображается в виде, аналогичном приведенному выше.

- Основные генераторы широковещательного графика (Top Broadcasters)

Функция выявляет станции сети, которые больше остальных генерируют кадры с широковещательными и групповыми адресами.

- Генерирование трафика (Traffic Generation)

Прибор может генерировать трафик для проверки работы сети при повышенной нагрузке. Трафик может генерироваться параллельно с активизированными функциями «Сетевая статистика», «Статистика ошибочных кадров» и «Статистика по коллизиям».

Пользователь может задать такие параметры генерируемого графика, как интенсивность и размер кадров. Для тестирования мостов и маршрутизаторов прибор может автоматически создавать заголовки IP- и IPX-пакетов. Все, что требуется от оператора - внести адреса источника и назначения.

В ходе испытаний пользователь может увеличить размер и частоту следования кадров с помощью клавиш управления курсором. Это особенно ценно при поиске источника проблем производительности сети и условий возникновения отказов.

Функции анализа протоколов

Обычно портативные многофункциональные приборы поддерживают декодирование и анализ только основных протоколов локальных сетей, таких как протоколы стеков TCP/IP, Novell NetWare, NetBIOS и Banyan VINES.

В некоторых многофункциональных приборах отсутствует возможность декодирования захваченных пакетов, как в анализаторах протоколов. Вместо этого собирается статистика о наиболее важных пакетах, свидетельствующих о наличии проблем в сетях. Например, при анализе протоколов стека TCP/IP собирается статистика по пакетам протокола ICMP, с помощью которого маршрутизаторы сообщают конечным узлам о возникновении разного рода ошибок. Для ручной проверки достижимости узлов сети в прибор включается поддержка утилиты IP Ping, а также аналогичных по назначению утилит NetWare Ping и NetBIOS Ping.



Рис. 5.6. Сетезависимые и сетезависимые уровни стека TCP/IP

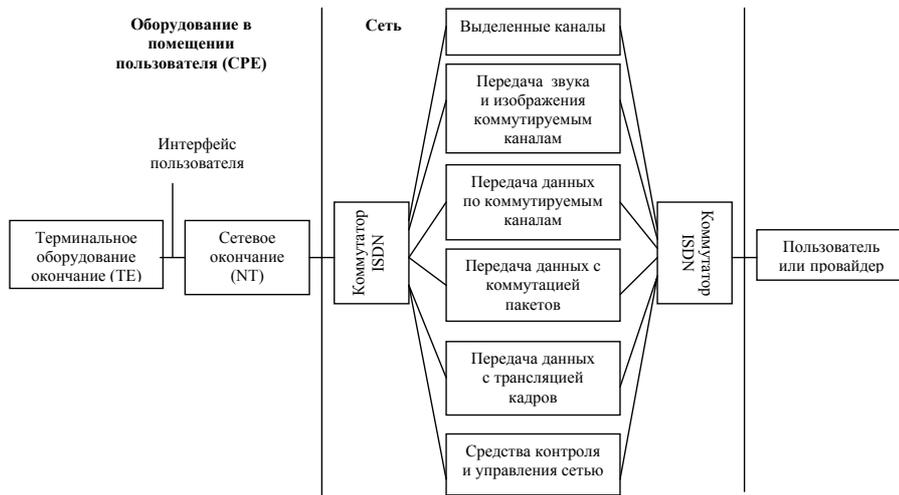


Рис. 8.2. Службы ЦСИО

Функции ISDN

Таблица 8.3

функции высоких уровней (телесервис)	7	Прикладные функции					
	6	Кодирование-декодирование		Сжатие/расширение			
4	5	Установка соединения сеанса	Освобождение соединения сеанса	Отображение сеанса в транспортное соединение		Синхронизация соединения сеанса	Управление сеансом
	4	Мультиплексирование соединения		Установка соединения	Освобождение соединения	Обнаружение ошибок/восстановление	Управление потоком
функции низких уровней (базовое обслуживание)	3	Сегментация/переключение	Установка соединений в сети	Освобождение соединений в сети	Мультиплексирование сетевых соединений	Управление сцеплением	Адресация
	2	Установка соединений звена данных	Освобождение соединений звена данных	Управление потоком	Контроль ошибок	Контроль последовательностей	Синхронизация кадров
	1	Активизация соединений физического уровня		Деактивизация соединений физического уровня		Передача битов	Мультиплексирование структуры канала

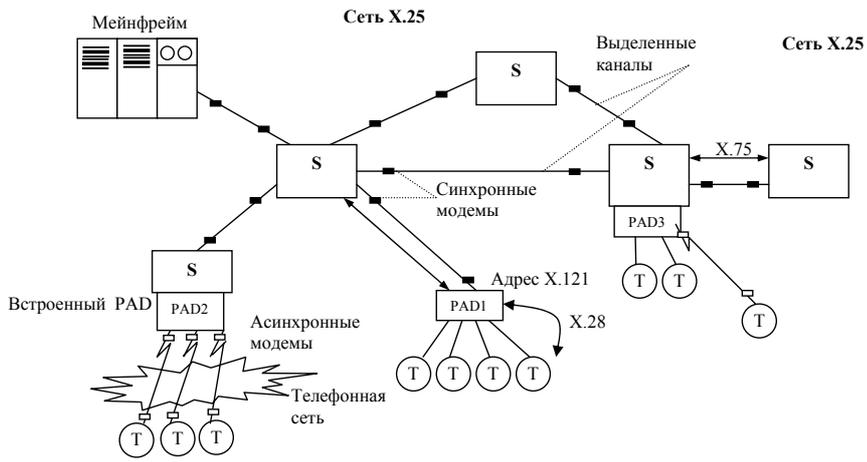


Рис. 6.3. Структура сети X.25

## ЗАКЛЮЧЕНИЕ

Современное общество стоит на рубеже «эпохи информации». Информация стала основным производственным ресурсом и товаром, от которой зависит жизнеспособность крупнейших промышленных и социальных комплексов, и даже отдельно взятый человек. Информационные коммуникации, это кровеносные сосуды, по которым перекачиваются огромные объемы информации. Недостаток современных сетей заключается в их гетерогенности, потому что существующие коммуникации построены на вчерашних стереотипах. Огромное количество различных информационных каналов опутывают нашу планету: телефонные сети, спутниковая связь, оптические кабели, радиоканалы, коаксиальные кабели. Множество протоколов, различные типы коммуникационного оборудования приводят к сложным системам передачи разнородного трафика. Все эти системы существуют независимо друг от друга. И для того, чтобы подключиться к какой-либо из них или объединить их требуется масса усилий и затрат.

Также разнородны и пользователи информации: в первую очередь это групповые пользователи — разнобразные организации, ВУЗы, бизнес-центры, многоквартирные жилые дома и офисы, фирмы, расположенные в одном здании и имеющие локальные сети.

Второе — это корпоративные клиенты, которым необходимо большое число телефонных линий, высокоскоростной доступ в Интернет, системы аудио- и видеоконференц-связи, сигнализации и телеметрии.

К третьей категории пользователей относятся распределенные корпорации, имеющие территориально удаленные офисы, филиалы, автоматические терминалы. Это банкоматы, торговые автоматы и т. п. Помимо всего вышеперечисленного, им требуется построение виртуальных частных сетей с достаточной высокой степенью защиты от несанкционированного доступа. Такая сеть может содержать как постоянные, так и временные элементы. Последними становятся, скажем, банкоматы или кассовые аппараты, соединяющиеся с сетью соответствующего банка для осуществления операций по платежным картам. Другой пример временного элемента — портативный терминал врача, посещающего пациента на дому. Подключив его к сетевой розетке и войдя в сеть со своими реквизитами, врач сможет автоматически внести в электронную карту пациента обычные медицинские показатели, данные кардиограммы, оперативно заказать в аптеке нужное лекарство, а при необходимости — провести видеоконсилиум с другими специалистами. Наконец, распределенными являются и системы сотовой связи, базовые станции которых также будут подключаться к единой мультисервисной сети. С их помощью мобильный абонент, вооруженный портативным мультимедиа-терминалом, сможет получать весь комплекс услуг, доступных стационарному пользователю.

Постепенно становится ясно, что такое широкое разнообразие различных сетей становится очень неудобно в процессе ее эксплуатации. Предлагается альтернатива прокладыванию новых проводов и умножению «коробок». Этой альтернативой является построение интеллектуальных мультисервисных (интегральных) сетей общего пользования. Телекоммуникационной структурой, позволяющей оказывать пользователям разнообразные услуги, различающиеся по качественным и количественным характеристикам.

Предполагается, что мультисервисная сеть должна одновременно обеспечивать передачу всего разнородного трафика.

Поэтому в мультисервисной сети не должно быть различий между пользователями. Любой ее абонент должен пользоваться любым типом услуг, ограничениями будут лишь его платежеспособность, условия контракта и наличие соответствующего оконечного оборудования. Необходимо, чтобы в любой момент он мог потребовать ту или иную услугу и в любой момент отказаться от нее, перейдя на работу в более экономичном режиме. Именно в удовлетворении этих требований заключается одна из основных проблем функционирования таких сетей.

Пользователь мультисервисной сети должен иметь средства для удаленного выбора услуг, оснащенные простым и интуитивно понятным интерфейсом. На сегодняшний день таким оптимальным средством можно считать интерфейс Web-браузера, хотя, возможно, завтра в этой области появятся какие-то другие идеи и тенденции.

Интерфейс должен быть доступен всем, как пожилым людям, так и современной молодежи. Например, пользователь захотел выбрать для просмотра какой-то канал. Это должно быть необременительно. Для этого достаточно дать установку путем выбора той или иной кнопки, и на этом работа пользователя заканчивается. Телевизор сам посылает сигнал в сеть для установления необходимой связи для выполнения заказа.

Для выбора скорости доступа в Интернет достаточно иметь на экране всего один орган управления: «медленнее, дешевле - быстрее, дороже». Что же касается специализированных аудио, видео и других терминалов и контроллеров, то они должны автоматически заказывать соответствующие коммуникационные услуги.

Также иметь доступ к контролю качества заказываемых услуг. В настоящее время эти функции осуществляет программа-монитор, использующая механизмы для измерения полосы пропускания, времени задержки пакетов и т.п. и выводящая информацию в виде пиктограммы на экран.

Если используются телевизор или телефон, то они должны самостоятельно контролировать параметры услуг и при необходимости оповещать пользователя соответствующим сигналом об каких-либо отклонения параметров от заданных значений. Для универсализации этого процесса предлагается установить специальный тестер в телекоммуникационную розетку, который будет предоставлять интерфейсы для подключения абонентских устройств. Он должен регистрировать все запросы на установление соединений, проходящие через него со стороны абонента, и контролировать параметры каждого канала, предоставляемого в ответ на эти запросы.

Также пользователь должен иметь интерактивный доступ к своему личному счету и полную статистику о его использовании. Эта актуальная проблема, поскольку стоимость услуг и объем их потребления будет изменяться также, как технические характеристики.

При любом сколько-нибудь значительном числе пользователей в мультисервисной сети требуется сложная и интеллектуальная система управления трафиком. Чисто количественное наращивание пропускной способности сети в данном случае бессмысленно, поскольку теоретический максимальный объем трафика, генерируемого всеми пользователями одновременно, выходит далеко за все мыслимые границы. Традиционные статистические методы расчета телефонных сетей в этом случае тоже малоприменимы, поскольку предназначены для однородного трафика и дают лишь вероятностный результат. В мультисервисной сети обычная постановка задачи типа «вероятность получения сигнала “занято” не более столько-то процентов» принципиально неприемлема: если клиент заключил контракт, предусматривающий гарантированное соединение, то сеть обязана предоставить ему такое соединение любой ценой, пусть даже за счет отключения кого-нибудь из низкоприоритетных пользователей. В мультисервисной сети существует множество разнотипных и неравномерных потоков одновременно, причем для каждого из них требуется безусловное соблюдение одних параметров и допускаются более или менее серьезные уступки по другим. Такая структура трафика не может не приводить к периодическому возникновению перегрузок, сеть же должна самостоятельно

устранять их, автоматически решая, чем можно пожертвовать: для одного соединения — полосой пропускания (сбросить все пакеты и не принимать следующие), для другого — временем доставки (задержать пакеты в промежуточных буферах до устранения перегрузки), для третьего — целостностью информации.

В принципе намечаются два подхода: революционный и эволюционный.

Революционный подход основан на применении новой технологии ATM, передачу с коммутацией микропакетов и с гарантированным предоставлением услуг по качеству передачи. Но при этом требуются большие затраты, связанные с обновлением всего программно-аппаратного парка сетевых коммуникаций. Выгоды очевидны в дальнейшем. Однородность сетевой среды и качество передачи.

Наиболее развитые средства управления трафиком предоставляет технология ATM, которая с самого начала разрабатывалась именно для передачи мультимедийной информации. Развитая система категорий обслуживания и приоритетов, интеллектуальные механизмы устранения и предупреждения перегрузок создают все условия для предоставления на основе инфраструктуры ATM самых разнообразных телекоммуникационных услуг — не только тех, что известны нам сегодня, но и тех, которые, возможно, появятся завтра. Опыт построения сетей ATM показывает, что сегодня эта технология предоставляет готовую базу для создания мультисервисных сетей общего пользования. В ближайшем будущем ожидается серьезный прорыв в этом направлении.

Эффективные средства управления трафиком позволяют существенно изменить работу пользователей. Например, работая на скорости 16 Кбит/с, экономный пользователь сможет на некоторое время заказать для себя полосу пропускания 2 Мбит/с, чтобы загрузить большой файл, а затем возвратиться в обычный режим. Когда же он не работает в сети, его почтовый клиент сможет один раз в час автоматически подключаться в самом медленном (дешевом) режиме, чтобы принять и передать новые письма.

Аналогичные решения для статических ресурсов уже предлагают крупные Интернет-провайдеры: пользователь может самостоятельно с помощью браузера изменить объем дискового пространства для персональной Web-страницы, перейти на другой тарифный план, создать дополнительные почтовые ящики и т. п. То же самое можно будет делать и с транспортными сетевыми ресурсами, причем в режиме реального времени.

С другой стороны существует эволюционный подход, основанный на использовании уже имеющихся средств, в частности это также технология пакетов, но с использованием широко известного протокола IP новой версии, и вместо протокола TCP, протоколов RTP и RSVP, а также новых способов компрессии информации и физического и логического кодирования (технологии xDSL).

Технология IP, в принципе также может стать той основой, которая обеспечит универсализацию средств передачи интегрального трафика. Причем объединение аналоговых и цифровых сетей неминуемо, и произойдет оно на базе технологии IP. Постоянно расширяющиеся сети передачи данных стремятся включить в себя передачу речи, изображения, высококачественного звука, что сближает телекоммуникационные и компьютерные возможности. Объемы данных, передаваемых по телефонным линиям в виде IP-пакетов, неуклонно растут, и нет смысла сохранять сети с коммутацией каналов, оптимизированных для передачи речи.

Объединенная на основе IP протоколов инфраструктура, способная передавать интегрированный трафик, имеет множество преимуществ. Это упрощенное управление, единый обслуживающий персонал, отсутствие дублирующих линий, возможность использования высокопроизводительных приложений и др. Линии ISDN, применяются для объединенной передачи речи и данных, но это дорого. Технология ATM также имеет большие возможности по передаче интегральной информации, но это потребует замены большинства существующих аппаратных сетевых средств. В то же время технология IP, возраст которой перевалил уже за тридцать лет и которая создавалась для совершенно других задач, сегодня становится основой для слияния передачи речи и данных.

Направленные на IP и Интернет инвестиции и интеллектуальные усилия специалистов по разработке приложений достигли критической массы. Возможно, IP — не лучшая технология, но она распространена повсеместно, стала стандартом связи между организациями и вполне позволяет объединить речь и данные".

Быстродействие оборудования для коммутации пакетов удваивается примерно каждые 10 месяцев, а вот аппаратура для коммутации каналов требуется в четыре раза больше времени, чтобы добиться таких же резуль-

татов. Если учесть, что объем трафика, передаваемого по Internet, удваивается через каждые шесть месяцев, то становится очевидным: только у технологии коммутации пакетов есть шансы справиться с перегрузкой линий. Коммутация каналов обречена. Новое поколение маршрутизирующих коммутаторов позволяет обрабатывать значительное количество IP-пакетов с такой же скоростью и при таком уровне же затрат. Только за прошедший год цены на оборудование для IP-сетей снизились в 10 раз, в то время как его быстродействие выросло примерно во столько же раз.

Сети с коммутацией пакетов являются и более гибкими, чем сети с коммутацией каналов. Современная офисная АТС в IP-сети может следить за уровнем трафика и использовать механизмы компрессии в режиме реального времени, если сеть перегружена. Качество связи при этом несколько снижается, но каждый абонент по-прежнему способен получить доступ к сети.

Таким образом, как показывает практика, эволюционный подход более предпочтителен. В то же время требования пользователей по интеграции услуг в любом случае будут реализовываться в виде мультисервисных сетей интегрального обслуживания.

Для эффективного управления услугами оператор мультисервисной сети должен располагать развитыми программными и аппаратными средствами, позволяющие быстро и гибко предоставлять любую мультимедиа-услугу для любого абонента. Рассматривая механизм предоставления таких услуг более подробно, нетрудно увидеть, что каждый запрос абонента порождает в сети оператора множество процессов. С одной стороны, необходимо аутентифицировать пользователя, проверить его платежеспособность, наличие данной услуги в его контракте и условия ее предоставления. При этом вопрос оптимального составления абонентских договоров и тарифных планов сам по себе — это огромный край работ для маркетинговых служб. С другой стороны, сеть должна проверить собственные ресурсы и определить, достаточно ли их для предоставления запрошенной услуги с требуемым качеством. Если ответ окажется отрицательным, а контракт предусматривает гарантированное предоставление услуги, оператор должен будет предпринять дополнительные меры для выполнения условий контракта — в противном случае клиент имеет полное право потребовать выплаты неустойки, а также подать в суд за некачественное обслуживание. Поскольку услуги заказываются и предоставляются в реальном времени, сеть сама должна оперативно решить, что делать: уменьшить объем ресурсов, выделенных другим клиентам сверх гарантированных им квот, перемаршрутизировать часть трафика на другие магистральные каналы, задействовать резервные каналы связи или предпринять какие-либо другие действия.

Существенным является то, что все взаимоотношения между оператором и абонентом сети должны сниться в терминах услуг, а не на языке малопонятных простому пользователю технических параметров. Пользователю необходимо предоставить возможность выбора требуемого типа соединения из нескольких предлагаемых, например: «телефон», «радиоточка», «Hi-Fi Stereo». Еще лучше, чтобы абонентское оборудование делало это автоматически. Система управления услугами сама должна транслировать кодовое название канала и соответствующий набор технических параметров. Например, канал «голос» может подразумевать выделение полосы пропускания 8 Кбит/с с максимальным временем задержки 300 мс, а соединение типа «видео» — полосы пропускания 2 Мбит/с с задержкой не более 500 мс.

Для мультисервисной сети общего пользования требуется более сложная система управления, чем для традиционных сетей. Она должна обеспечить одновременное предоставление множества разнообразных сетевых услуг и «мирное сосуществование» разнотипного трафика. Решение задач управления такой сетью можно разделить на четыре этапа: сбор информации непосредственно с сетевых устройств; ее анализ и структурирование; статистический учет; моделирование и планирование трафика. Классические системы сетевого управления, существующие на сегодняшний день, охватывают первые два этапа. Биллинговые системы осуществляют анализ и статистическую обработку, но они не предназначены для моделирования и планирования трафика. В целом же законченных систем для полноценного мультисервисными сетями, и особенно для моделирования и планирования трафика, пока не существует. Очевидно, это связано с относительной новизной поставленных задач. Для построения мультисервисных сетей интегрального обслуживания предстоит решить еще немало сложных технических задач.

## ПЕРЕЧЕНЬ ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. — СПб: Изд-во «Питер», 2000. — 672 с.
2. Блэк Ю. Сети ЭВМ: Протоколы, стандарты, интерфейсы: Пер. с англ. — М.: Мир, 1990. — 506 с.
3. Назаров А.Н., Симонов М.В. АТМ: Технология высокоскоростных сетей. — М.: ЭКО-ТРЕНДЗ, 1998.
4. Толковый словарь по вычислительным системам / Под ред. В. Иллингорта и др.; Пер. с англ. А. К. Белоцкого и др.; Под ред. Е.К. Масловского. — М.: Машиностроение, 1990. — 560 с.
5. Компьютерные сети. Учебный курс: Официальное пособие Microsoft для самостоятельной подготовки. — М.: Издательско-торговый дом «Русская редакция», 1999.
6. Компьютерные сети. Учебный курс: Официальное пособие Microsoft для самостоятельной подготовки: — М.: Издательско-торговый дом «Русская редакция», 1997.
7. Кеннет Грег. Основы сетей Windows.
8. Эд Титтель и др. ISDN просто и доступно: — М.: Изд-во «Лори», 1997.
9. В.П. Косарев и др. Компьютерные системы и сети.
10. Бакланов И. Г. Технология измерений в современных телекоммуникациях. - М.: ЭКО-ТРЕНДЗ, 1998.
11. Бэрри Нанс. Компьютерные сети: Пер. с англ. — М.: Восточная Книжная Компания, 1996. — 400 с.
12. Компьютерные сети. Уч. курс: Официальное пособие Microsoft для самостоятельной подготовки: Пер. с англ. — 2-е изд., испр. и доп. — М.: Издательско-торговый дом «Русская Редакция», 1999. — 586 с.
13. Семенов Ю. А. Сети Интернет: архитектура и протоколы. — М.: «Радио и связь», 1998.
14. Бертсекас В. Сети передачи данных. Пер. с англ. — М.: Мир, 1989.
15. Шварц М. Сети ЭВМ. Анализ и проектирование. — М.: Радио и связь, 1981. — 334 с.