Кузин А.В.

компьютерные сети

УДК 004.6(075.32)
ББК 32.973я723
К89

Рецензенты:
профессор Московского государственного социального университета, доктор технических наук *Ю. П. Кораблин*;
профессор МВТУ им. Баумана, доктор технических наук *А. С. Чижов*

Кузин А. В.

К89 Компьютерные сети: учебное пособие / А. В. Кузин. — 3-е изд., перераб. и доп. — М.: ФОРУМ: ИНФРА-М, 2011. — 192 с.: ил. — (Профессиональное образование).

ISBN 978-5-91134-476-4 (ФОРУМ)
ISBN 978-5-16-004609-9 (ИНФРА-М)

Рассматриваются общие вопросы построения компьютерных сетей: сетевые архитектуры, аппаратные компоненты, линии связи, сетевые модели, задачи и функции по уровням сетевой модели OSI, различия и особенности распространенных протоколов разных уровней, принципы адресации в сети, методы доступа к среде передачи данных. Приводятся особенности основных операционных систем, структура и информационные услуги территориальных сетей.

Для студентов средних специальных учебных заведений, обучающихся по специальностям «Автоматизированные системы обработки информации и управления», «Программное обеспечение вычислительной техники и автоматизированных систем».

УДК 004.6(075.32)
ББК 32.973я723

ISBN 978-5-91134-476-4 (ФОРУМ)
ISBN 978-5-16-004609-9 (ИНФРА-М)
© Кузин А. В., 2010
© Издательство «ФОРУМ», 2010

Введение

Компьютерные информационно-вычислительные сети (ИВС) и телекоммуникации — сравнительно новая, стремительно развивающаяся область науки и техники. Работы по проектированию и созданию ИВС и телекоммуникаций ведутся одновременно во многих передовых странах мира.

Для изучения принципов организации и функционирования информационно-вычислительных сетей и телекоммуникаций необходимо обладать знаниями в достаточно широкой области, включающей основы электротехники и электроники, информатики и вычислительной техники, и дополнить их знаниями сетевых технологий, техники электрической связи и других.

Учитывая специфику среднего профессионального обучения, материал предлагаемого учебного пособия излагается последовательно, начиная с рассмотрения общих вопросов построения ИВС, а затем с углубленным описанием основных компонентов сетей и телекоммуникаций.

Основой книги послужили тексты лекций и практических занятий, проводимых автором в Красногорском оптико-электронном колледже, а также на факультете информационных систем Российского государственного социального университета.

Глава 1
ОСНОВНЫЕ ПОНЯТИЯ О КОМПЬЮТЕРНЫХ СЕТЯХ

1.1. Классификация информационно-вычислительных сетей (ИВС). Локальные, городские и глобальные сети

Коммуникационная сеть — система, состоящая из объектов, называемых пунктами (узлами) сети и осуществляющих функции генерации, преобразования, хранения и потребления некоторого продукта, а также линий передачи (связей, коммуникаций, соединений), осуществляющих передачу продукта между пунктами. В качестве продукта может фигурировать информация, энергия, масса. Соответственно различают группы сетей информационных, энергетических, вещественных. В группах сетей возможно разделение на подгруппы. Так, среди вещественных сетей могут быть выделены сети транспортные, водопроводные, производственные и др.

Информационно-вычислительная сеть — коммуникационная сеть, в которой продуктом генерирования, переработки, хранения и использования является информация, а узлами сети — вычислительное оборудование. Компонентами ИВС могут быть электронные вычислительные машины (ЭВМ) и периферийные устройства, являющиеся источниками и приемниками данных, передаваемых по сети. В качестве периферийных устройств могут выступать ЭВМ, принтеры, плоттеры и другое вычислительное, измерительное и исполнительное оборудование автоматических и автоматизированных систем. Собственно пересылка информации происходит с помощью средств, объединяемых под названием среда передачи данных.

Существует множество причин для объединения отдельных компьютеров в сеть, например:

1) в сети можно организовать доступ всех пользователей к единому информационному ресурсу (например, базе данных), расположенному на одном компьютере. При этом возрастает мобильность и оперативность работы, упрощаются процессы обеспечения целостности информационного ресурса и его резервного копирования;

2) при объединении компьютеров в сеть снижаются затраты на аппаратное обеспечение в расчете на одного пользователя. Это достигается за счет совместного использования дискового пространства, дорогих внешних устройств (лазерных принтеров, сканеров, плоттеров). При этом правильная организация совместного доступа повышает надежность системы в целом, поскольку при поломке одного устройства исполнение его функций может взять на себя другое;

3) совместное использование дискового пространства позволяет разместить сетевые версии прикладного программного обеспечения на диске одного компьютера, что, кроме значительной экономии места на дисках, позволяет снизить затраты на программное обеспечение (ПО).

ИВС **классифицируются** по ряду признаков. В зависимости от расстояний между связываемыми узлами различают вычислительные сети:

- **территориальные**, охватывающие значительное географическое пространство. Среди территориальных сетей можно выделить сети **региональные** и **глобальные**, имеющие соответственно региональные или глобальные масштабы; региональные сети иногда называют сетями MAN (Metropolitan Area Network), а общее англоязычное название для территориальных сетей — WAN (Wide Area Network);
- **локальные** вычислительные сети (ЛВС), охватывающие ограниченную территорию (обычно в пределах удаленности узлов сети не более чем на несколько десятков или сотен метров друг от друга, реже — на несколько километров). Локальные сети также обозначают сокращением LAN (Local Area Network);
- **корпоративные** сети (масштаба предприятия) — совокупность связанных между собой ЛВС, охватывающих территорию, на которой размещено одно предприятие или учреждение.

Среди глобальных сетей следует выделить единственную в своем роде глобальную сеть Internet и реализованную в ней информационную службу World Wide Web (WWW) (переводится на русский язык как всемирная паутина).

Различают интегрированные сети, неинтегрированные сети и подсети. **Интегрированная вычислительная сеть (интерсеть)** представляет собой взаимосвязанную совокупность многих вычислительных сетей, которые в интерсети называются подсетями. Обычно интерсети приспособлены для различных видов связи: телефонии, электронной почты, передачи видеоинформации, цифровых данных и т. п. В этом случае они называются **сетями интегрального обслуживания.**

В зависимости от топологии соединений узлов различают **сети шинной (магистральной), кольцевой, звездной, ячеистой, комбинированной, произвольной структуры.**

В зависимости от способа управления различают сети:

«клиент/сервер» или сети с выделенным сервером. В них выделяется один или несколько узлов (их название — серверы), выполняющих в сети управляющие или специальные обслуживающие функции, а остальные узлы (клиенты) являются терминальными, в них работают пользователи. Сети клиент/сервер различаются по характеру распределения функций между серверами, другими словами, по типам серверов (например, файл-серверы, серверы баз данных). При специализации серверов по определенным приложениям получается **сеть распределенных вычислений**. В рамках одной локальной сети может использоваться несколько выделенных серверов. По своему функциональному назначению различают несколько типов серверов:

- файловый сервер;
- сервер печати;
- сервер приложений;
- сервер базы данных;
- коммуникационный сервер и т. д.

Файловый сервер — компьютер, который выполняет функции управления локальной сетью, отвечает за коммуникационные связи, хранит файлы, разделяемые в сети, и предоставляет доступ к совместно используемому дисковому пространству.

Сервер печати — компьютер, программа или специальное устройство, обеспечивающее доступ станциям сети к центральному разделяемому принтеру. Запросы на печать поступают от каждой рабочей станции к серверу печати, который разделяет их

на индивидуальные задания принтеру, создает очередь печати. Задания обычно обрабатываются в порядке их поступления. В функции сервера печати входит также управление принтером.

Коммуникационный сервер (сервер удаленного доступа — Access Server) позволяет работать с различными протоколами (правилами передачи информации в сети) и позволяет станциям разделять модем или узел связи с большой ЭВМ. Это дает возможность получить информацию, хранящуюся в сети, практически с любого места, где есть телефон, модем и компьютер.

Довольно часто сервер совмещает функции коммуникационного сервера и сервера приложений.

Сервер приложений выполняет одну или несколько прикладных задач, которые запускают пользователи со своих терминалов, включенных в данную сеть. Принцип действия сервера приложений совпадает с принципом действия многотерминальной системы (системы совместной обработки). Задача пользователя выполняется непосредственно на сервере приложений, а по низкоскоростной телефонной линии на удаленный компьютер (терминал) передается только изображение экрана терминала пользователя, а обратно — только информация о нажимаемых пользователем клавишах. Поэтому нагрузка по передаче информации (например, при работе с базами данных (БД)) ложится на высокоскоростной кабель сети, к которой подключен сервер приложений.

Сервер БД — специализированная программа или компьютер, обеспечивающий станции записями из базы данных. При использовании обычного файл-сервера все данные из БД передаются через сеть в пользовательский компьютер так, чтобы он мог выбрать информацию, необходимую работающей прикладной программе. В отличие от этого, сервер БД сам выбирает необходимые данные и посылает через сеть только информацию, запрашиваемую программой пользователя (эта программа производит обработку информации и представление ее пользователю). Таким образом, в подобных системах (называемых системами «клиент/сервер») совмещаются преимущества систем совместной и распределенной обработки.

Технология клиент/сервер является реализацией распределенной обработки данных. С точки зрения баз данных под распределенной обработкой понимается выполнение операций с базами данных на одной машине и приложений на другой. В системе архитектуры клиент/сервер обработка данных разделена между компьютером-клиентом и компьютером-сервером, связь

между которыми происходит по сети. Основная функция компьютера-клиента состоит в выполнении приложения (интерфейса с пользователем и логики представления) и осуществлении связи с сервером, когда этого требует приложение. Компьютер-клиент может быть как простой машиной типа персонального компьютера, так и мощной рабочей станцией с многозадачной и многопользовательской операционной системой типа UNIX. Таким образом, выбор компьютера, операционной системы, оперативной и дисковой памяти, другого оборудования определяется требованиями приложения. Главная функция компьютера-сервера заключается в обслуживании потребностей клиента. Связь с клиентом, анализ и выполнение запроса к базе данных, включая возврат клиенту результата запроса (набора строк из базы данных), управление одновременным доступом к базе данных многих пользователей, перенаправление запросов к другим серверам сети, обеспечение защиты — таковы некоторые основные функции компьютера-сервера.

К рассмотренным выше серверам можно добавить сервер электронной почты и факс-сервер. Главной их характеристикой является степень защиты конфиденциальной информации от несанкционированного доступа.

Один выделенный компьютер в сети может одновременно выполнять функции файл-сервера, сервера печати, приложений и т. д.

Одноранговые — в них все узлы равноправны. Поскольку в общем случае под клиентом понимается объект (устройство или программа), запрашивающий некоторые услуги, а под сервером — объект, предоставляющий эти услуги, поэтому каждый узел в одноранговых сетях может выполнять функции и клиента, и сервера.

Сети также различают в зависимости от используемых в них протоколов и по способам коммутации.

Протоколы — это набор семантических и синтаксических правил, определяющий поведение функциональных блоков сети при передаче данных. Другими словами, протокол — это совокупность соглашений относительно способа представления данных, обеспечивающего их передачу в нужных направлениях и правильную интерпретацию данных всеми участниками процесса информационного обмена.

Поскольку информационный обмен — процесс многофункциональный, то протоколы делятся на уровни. К каждому уров-

ню относится группа родственных функций. Для правильного взаимодействия узлов различных вычислительных сетей их архитектура должна быть открытой. Этим целям служат унификация и стандартизация в области телекоммуникаций и вычислительных сетей.

Унификация и стандартизация протоколов выполняются рядом международных организаций, что наряду с разнообразием типов сетей породило большое число различных протоколов. Наиболее широко распространенными являются протоколы, разработанные и применяемые в глобальной сети Internet, протоколы открытых систем Международной организации по стандартизации (ISO — Intrenational Standard Organization), протоколы Международного телекоммуникационного союза (International Telecommunication Union — ITU) и протоколы Института инженеров по электротехнике и электронике (IEEE — Institute of Electrical and Electronics Engineers).

Протоколы ISO являются семиуровневыми и известны как протоколы **базовой эталонной модели взаимосвязи открытых систем**.

1.2. Программные и аппаратные средства ИВС

Вычислительная сеть (ВС) — это сложный комплекс взаимосвязанных и согласованно функционирующих программных и аппаратных компонентов, основными элементами которого являются:

- компьютеры;
- коммуникационное оборудование;
- операционные системы;
- сетевые приложения.

В основе любой сети лежит стандартизованная аппаратная платформа. В настоящее время в сетях широко и успешно применяются компьютеры различных классов — от персональных компьютеров до мэйнфреймов и суперЭВМ. Набор компьютеров в сети должен соответствовать набору разнообразных задач, решаемых сетью.

Второй элемент — это коммуникационное оборудование. Хотя компьютеры и являются центральными элементами обработки данных в сетях, в последнее время не менее важную роль

стали играть коммуникационные устройства. Кабельные системы, повторители, мосты, коммутаторы, маршрутизаторы и модульные концентраторы из вспомогательных компонентов сети превратились в основные наряду с компьютерами и системным программным обеспечением как по влиянию на характеристики сети, так и по стоимости. Сегодня коммуникационное устройство может представлять собой сложный специализированный мультипроцессор, который нужно конфигурировать, оптимизировать и администрировать. Изучение принципов работы коммуникационного оборудования требует знакомства с большим количеством протоколов, используемых как в локальных, так и глобальных сетях.

Третьей составляющей, образующей программную платформу сети, являются операционные системы (ОС). От того, какие концепции управления локальными и распределенными ресурсами положены в основу сетевой ОС, зависит эффективность работы всей сети. При проектировании сети важно учитывать, насколько просто данная операционная система может взаимодействовать с другими ОС сети, насколько она обеспечивает безопасность и защищенность данных, до какой степени она позволяет наращивать число пользователей, можно ли перенести ее на компьютер другого типа и многие другие соображения.

Последней составляющей сетевых средств являются различные сетевые приложения, такие как сетевые базы данных, почтовые системы, средства архивирования данных, системы автоматизации коллективной работы и др. Очень важно представлять диапазон возможностей, предоставляемых приложениями для различных областей применения, а также знать, насколько они совместимы с другими сетевыми приложениями и операционными системами.

1.3. Сети одноранговые и «клиент/сервер»

Локальные, глобальные и территориальные сети могут быть одноранговыми сетями, сетями типа «клиент/сервер» (они также называются сетями с выделенным сервером) или смешанными сетями (в которых используются как одноранговые технологии, так и технологии с выделенным сервером).

Компьютеры в **одноранговых сетях** могут выступать как в роли клиентов, так и в роли серверов. Так как все компьютеры в этом типе сетей равноправны, одноранговые сети не имеют централизованного управления разделением ресурсов. Любой из компьютеров может разделять свои ресурсы с любым компьютером в той же сети.

Одноранговые взаимоотношения также означают, что ни один компьютер не имеет ни высшего приоритета на доступ, ни повышенной ответственности за предоставление ресурсов в совместное пользование.

Каждый пользователь в одноранговой сети является одновременно сетевым администратором. Это означает, что каждый пользователь в сети управляет доступом к ресурсам, расположенным на его компьютере. Он может дать всем остальным неограниченный доступ к локальным ресурсам, дать ограниченный доступ, а может не дать вообще никакого доступа другим пользователям. Каждый пользователь также решает, дать другим пользователям доступ просто по их запросу или защитить эти ресурсы паролем.

Основной проблемой в одноранговых сетях является безопасность, так как отсутствуют средства обеспечения безопасности в масштабе сети. При этом отдельные ресурсы отдельных компьютеров могут быть защищены системой паролей, и только те пользователи, которые знают пароль, могут получить доступ к ресурсам.

Этот тип сети может быть работоспособным в малых сетях, но также требует, чтобы пользователи знали и помнили различные пароли для каждого разделенного ресурса в сети. С ростом количества пользователей и ресурсов одноранговая сеть становится неработоспособной. Это происходит не потому, что сеть не может функционировать правильно, а потому, что пользователи не в состоянии справиться со сложностью сети.

К тому же большинство одноранговых сетей состоит из набора типичных персональных компьютеров, связанных общим сетевым носителем. Эти типы компьютеров не были разработаны для работы в качестве сетевых серверов, поэтому производительность сети может упасть, когда много пользователей попытаются одновременно получить доступ к ресурсам какого-то одного компьютера. Кроме того, пользователь, к чьей машине происходит доступ по сети, сталкивается с падением производительности в то время, когда компьютер выполняет затребованные сетевые

службы. Например, если к компьютеру пользователя подключен принтер, к которому осуществляется доступ по сети, компьютер будет замедлять свою работу каждый раз, когда пользователи посылают задание на этот принтер. Это может раздражать того, кто работает на данной машине.

В одноранговой сети также трудно организовывать хранение и учет данных. Когда каждый сетевой компьютер может служить сервером, пользователям трудно отслеживать, на какой машине лежит интересующая их информация. Децентрализованная природа такого типа сети делает поиск ресурсов чрезвычайно сложным с ростом числа узлов, на которых должна происходить проверка. Децентрализация также затрудняет процедуру резервного копирования данных — вместо копирования централизованного хранилища данных требуется осуществлять резервное копирование на каждом сетевом компьютере, чтобы защитить разделенные данные.

Однако одноранговые сети имеют серьезные преимущества перед сетями с выделенным сервером, особенно для малых организаций и сетей. Одноранговые сети являются наиболее легким и дешевым типом сетей для установки. Большинство одноранговых сетей требует наличия на компьютерах, кроме сетевой карты и сетевого носителя (кабеля), только операционной системы. Как только компьютеры соединены, пользователи немедленно могут начинать предоставление ресурсов и информации в совместное пользование.

Преимущества одноранговых сетей:

- легкость в установке и настройке;
- независимость отдельных машин от выделенного сервера;
- возможность пользователем контролировать свои собственные ресурсы;
- сравнительная дешевизна в приобретении и эксплуатации;
- отсутствие необходимости в дополнительном программном обеспечении, кроме операционной системы;
- отсутствие необходимости иметь отдельного человека в качестве выделенного администратора сети.

Недостатки одноранговых сетей:

- необходимость помнить столько паролей, сколько имеется разделенных ресурсов;
- необходимость производить резервное копирование отдельно на каждом компьютере, чтобы защитить все совместные данные;

- падение производительности при доступе к разделенному ресурсу на компьютере, где этот ресурс расположен;
- отсутствие централизованной организационной схемы для поиска и управления доступом к данным.

Сети с выделенным сервером или сети типа «клиент/сервер» опираются на специализированные компьютеры, называемые серверами, представляющими собой централизованные хранилища сетевых ресурсов и объединяющими централизованное обеспечение безопасности и управления доступом. В отличие от сетей с выделенным сервером, одноранговые сети не имеют централизованного обеспечения безопасности и управления. Сервер представляет собой сочетание специализированного программного обеспечения и оборудования, которое предоставляет службы в сети для остальных клиентских компьютеров (рабочих станций) или других процессов (рис. 1.1).

Рис. 1.1. Сети типа клиент/сервер

Имеется несколько причин для реализации сети с выделенным сервером, включающих централизованное управление сетевыми ресурсами путем использования сетевой безопасности и управление посредством установки и настройки сервера. С точки зрения оборудования, серверные компьютеры обычно имеют более быстрый центральный процессор, больше памяти, большие жесткие диски и дополнительные периферийные устройства, например накопители на магнитной ленте и приводы ком-

пакт-дисков, по сравнению с клиентскими машинами. Серверы также ориентированы на то, чтобы обрабатывать многочисленные запросы на разделяемые ресурсы быстро и эффективно. Серверы обычно выделены для обслуживания сетевых запросов клиентов. В дополнение, физическая безопасность — доступ к самой машине — является ключевым компонентом сетевой безопасности. Поэтому важно, чтобы серверы располагались в специальном помещении с контролируемым доступом, отделенном от помещений с общим доступом.

Сети с выделенным сервером также предоставляют централизованную проверку учетных записей пользователей и паролей. Например, Windows Server использует доменную концепцию для управления пользователями, группами и машинами и для контроля над доступом к сетевым ресурсам. Прежде чем пользователь сможет получить доступ к сетевым ресурсам, он должен сообщить свое регистрационное имя и пароль контроллеру домена — серверу, который проверяет имена учетных записей и пароли в базе данных с такой информацией. Контроллер домена позволит доступ к определенным ресурсам только в случае допустимой комбинации регистрационного имени и пароля. Изменять связанную с безопасностью информацию в базе данных контроллера домена может только сетевой администратор. Этот подход обеспечивает централизованную безопасность и позволяет управлять ресурсами с изменяющейся степенью контроля в зависимости от их важности и расположения.

В отличие от одноранговой модели сеть с выделенным сервером обычно требует только один пароль для доступа к самой сети, что уменьшает количество паролей, которые пользователь должен помнить. Кроме того, сетевые ресурсы типа файлов и принтеров легче найти, потому что они расположены на определенном сервере, а не на чьей-то машине в сети. Концентрация сетевых ресурсов на небольшом количестве серверов также упрощает резервное копирование и поддержку данных.

Сети с выделенным сервером лучше масштабируются в сравнении с одноранговыми сетями. С ростом размера одноранговые сети сильно замедляют свою работу и становятся неуправляемыми. Сети с выделенным сервером, наоборот, могут обслуживать от единичных пользователей до десятков тысяч пользователей и географически распределенных ресурсов. Другими словами, сеть с выделенным сервером может расти с ростом использующей ее организации.

Подобно одноранговой модели, сеть с выделенным сервером также имеет недостатки. Первой в этом списке стоит необходимость дополнительных расходов на такие сети. Сеть с выделенным сервером требует наличия одного или нескольких более мощных (и, соответственно, более дорогих) компьютеров для запуска специального (и тоже дорогого) серверного программного обеспечения. Вдобавок, серверное программное обеспечение требует квалифицированного персонала для его обслуживания. Подготовка персонала для овладения необходимыми для обслуживания сети с выделенным сервером навыками или наем на работу подготовленных сетевых администраторов также увеличивают стоимость такой сети.

Есть и другие негативные аспекты сетей с выделенным сервером. Централизация ресурсов и управления упрощает доступ, контроль и объединение ресурсов, но при этом приводит к появлению точки, которая может привести к неполадкам во всей сети. Если сервер вышел из строя, не работает вся сеть. В сетях с несколькими серверами потеря одного сервера означает потерю всех ресурсов, связанных с этим сервером. Также если неисправный сервер является единственным источником информации о правах доступа определенной части пользователей, эти пользователи не смогут получить доступ к сети.

Преимущества сетей с выделенным сервером:

- обеспечение централизованного управления учетными записями пользователей, безопасностью и доступом, что упрощает сетевое администрирование;
- использование более мощного серверного оборудования означает и более эффективный доступ к сетевым ресурсам;
- пользователям для входа в сеть нужно помнить только один пароль, что позволяет им получить доступ ко всем ресурсам, к которым имеют права.

Недостатки сетей с выделенным сервером:

- неисправность сервера может сделать сеть неработоспособной, что в лучшем случае означает потерю сетевых ресурсов;
- сети требуют квалифицированного персонала для сопровождения сложного специализированного программного обеспечения, что увеличивает общую стоимость сети;
- стоимость также увеличивается благодаря потребности в выделенном оборудовании и специализированном программном обеспечении.

1.4. Способы коммутации

Назначение любой сети — обмен данными (информацией) между компьютерами.

Любые сети связи поддерживают некоторый способ коммутации своих абонентов между собой. Этими абонентами могут быть удаленные компьютеры, локальные сети, факс-аппараты или просто собеседники, общающиеся с помощью телефонных аппаратов. Практически невозможно предоставить каждой паре взаимодействующих абонентов свою собственную некоммутируемую физическую линию связи, которой они могли бы монопольно «владеть» в течение длительного времени. Поэтому в любой сети всегда применяется какой-либо способ коммутации абонентов, который обеспечивает доступность имеющихся физических каналов одновременно для нескольких сеансов связи между абонентами сети.

Под **коммутацией данных** понимается их передача, при которой канал передачи данных может использоваться попеременно для обмена информацией между различными пунктами информационной сети в отличие от связи через некоммутируемые каналы, обычно закрепленные за определенными абонентами.

Различают следующие способы коммутации данных:

- **коммутация каналов** — осуществляется соединение двух или более станций данных и обеспечивается монопольное использование канала передачи данных до тех пор, пока соединение не будет разомкнуто;
- **коммутация сообщений** — характеризуется тем, что создание физического канала между оконечными узлами необязательно, и пересылка сообщений происходит без нарушения их целостности; вместо физического канала имеется виртуальный канал, состоящий из физических участков, и между участками возможна буферизация сообщения;
- **коммутация пакетов** — сообщение передается по виртуальному каналу, но оно разделяется на пакеты, при этом канал передачи данных занят только во время передачи пакета (без нарушения его целостности) и по ее завершении освобождается для передачи других пакетов.

Коммутация каналов может быть пространственной и временно́й.

Пространственный коммутатор размера N*M представляет собой сетку (матрицу), в которой N входов подключены к горизонтальным шинам, а M выходов — к вертикальным (рис. 1.2).

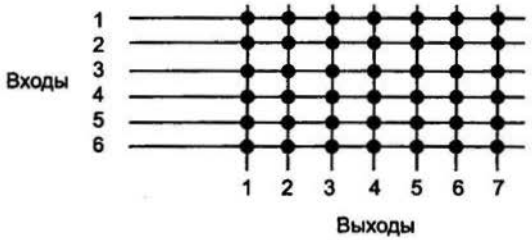

Рис. 1.2. Пространственный коммутатор

В узлах сетки имеются коммутирующие элементы, причем в каждом столбце сетки может быть открыто не более чем по одному элементу. Если $N < M$, то коммутатор может обеспечить соединение каждого входа с не менее чем одним выходом; в противном случае коммутатор называется блокирующим, т. е. не обеспечивающим соединения любого входа с одним из выходов. Обычно применяются коммутаторы с равным числом входов и выходов $N \times N$.

Недостаток рассмотренной схемы — большое число коммутирующих элементов в квадратной матрице, равное N^2. Для устранения этого недостатка применяют многоступенчатые коммутаторы.

Временно́й коммутатор строится на основе буферной памяти, запись производится в ее ячейки последовательным опросом входов, а коммутация осуществляется благодаря считыванию данных на выходах из нужных ячеек памяти. При этом происходит задержка на время одного цикла «запись—чтение». В настоящее время преимущественно используются временная или смешанная коммутация.

При **коммутации сообщений** осуществляется передача единого блока данных между транзитными компьютерами сети с временной буферизацией этого блока на диске каждого компьютера. Сообщение в отличие от пакета имеет произвольную длину, которая определяется не технологическими соображениями, а содержанием информации, составляющей сообщение. Например, сообщением может быть текстовый документ, файл с кодом программы, электронное письмо.

Транзитные компьютеры могут соединяться между собой как сетью с коммутацией пакетов, так и сетью с коммутацией каналов. Сообщение хранится в транзитном компьютере на диске, причем время хранения может быть достаточно большим, если компьютер загружен другими работами или сеть временно перегружена.

По такой схеме обычно передаются сообщения, не требующие немедленного ответа, чаще всего сообщения электронной почты.

Количество транзитных компьютеров стараются по возможности уменьшить. Если компьютеры подключены к сети с коммутацией пакетов, то число промежуточных компьютеров обычно уменьшается до двух. Например, пользователь передает почтовое сообщение своему серверу исходящей почты, а тот сразу старается передать сообщение серверу входящей почты адресата. Но если компьютеры связаны между собой телефонной сетью, то часто используется несколько промежуточных серверов, так как прямой доступ к конечному серверу может быть невозможен в данный момент из-за перегрузки телефонной сети (абонент занят) или экономически невыгоден из-за высоких тарифов на дальнюю телефонную связь.

Техника коммутации сообщений появилась в компьютерных сетях раньше техники коммутации пакетов, но потом была вытеснена последней, как более эффективной по критерию пропускной способности сети. Запись сообщения на диск занимает достаточно много времени, кроме того, наличие дисков предполагает специализированные компьютеры в качестве коммутаторов, что удорожает сеть.

Во многих случаях наиболее эффективной оказывается **коммутация пакетов**. Во-первых, ускоряется передача данных в сетях сложной конфигурации за счет того, что возможна параллельная передача пакетов одного сообщения на разных участках сети; во-вторых, при появлении ошибки требуется повторная передача короткого пакета, а не всего длинного сообщения. Кроме того, ограничение сверху на размер пакета позволяет обойтись меньшим объемом буферной памяти в промежуточных узлах на маршрутах передачи данных в сети.

Любой пакет состоит из трех обязательных компонентов:

- заголовка;
- данных;
- информации для проверки ошибок передачи.

Заголовок содержит:

- адрес источника, идентифицирующий компьютер-отправитель;
- адрес местоназначения, идентифицирующий компьютер-получатель;
- инструкции сетевым компонентам о дальнейшем маршруте данных;
- информация компьютеру-получателю о том, как объединить передаваемый пакет с остальными, чтобы получить данные в исходном виде.

Данные — это часть пакета, представляющая передаваемые данные. В зависимости от типа сети ее размер составляет от 512 байтов до 4 Кб. Так как обычно размер исходных данных гораздо больше 4 Кб, для помещения в пакет их необходимо разбивать на мелкие блоки. При передаче объемного файла может потребоваться много пакетов.

Информация для проверки ошибок обеспечивает корректность передачи. Эта информация носит название циклический избыточный код. Это число, получаемое в результате математических преобразований над пакетом с исходной информацией. Когда пакет достигает местоназначения, эти преобразования повторяются. Если результат совпадает с циклическим избыточный кодом, пакет принят без ошибок. В противном случае необходимо повторить передачу пакета, поскольку при передаче данные изменились.

В сетях коммутации пакетов различают два режима работы: режим виртуальных каналов (другое название — связь с установлением соединения) и дейтаграммный режим (связь без установления соединения).

В **режиме виртуальных каналов** пакеты одного сообщения передаются в естественном порядке по устанавливаемому маршруту. При этом в отличие от коммутации каналов линии связи могут разделяться многими сообщениями, когда попеременно по каналу передаются пакеты разных сообщений (это так называемый режим временного мультиплексирования, иначе TDM — Time Division Method), или задерживаться в промежуточных буферах. Предусматривается контроль правильности передачи данных путем посылки от получателя к отправителю подтверждающего сообщения. Этот контроль возможен как во всех промежуточных узлах маршрута, так и только в конечном узле. Он может осуществляться **старт-стопным** способом, при котором отправи-

тель до тех пор не передает следующий пакет, пока не получит подтверждения о правильной передаче предыдущего пакета, или способом **передачи «в окне»**. Окно может включать *N* пакетов, и возможны задержки в получении подтверждений на протяжении окна. Так, если произошла ошибка при передаче, т. е. отправитель получает ошибку о передаче пакета с номером *K*, то нужна повторная передача, и она начинается с пакета *K*.

В **дейтаграммном режиме** сообщение делится на дейтаграммы. Дейтаграмма — часть информации, передаваемая независимо от других частей одного и того же сообщения в вычислительных сетях с коммутацией пакетов. Дейтаграммы одного и того же сообщения могут передаваться в сети по разным маршрутам и поступать к адресату в произвольной последовательности, что может послужить причиной блокировок сети. На внутренних участках маршрута контроль правильности передачи не предусмотрен, и надежность связи обеспечивается лишь контролем на оконечном узле.

Блокировкой сети в дейтаграммном режиме называется такая ситуация, когда в буферную память узла вычислительной сети поступило столько пакетов разных сообщений, что эта память оказывается полностью занятой. Следовательно, она не может принимать другие пакеты и не может освободиться от уже принятых, так как это возможно только после поступления всех дейтаграмм сообщения.

1.5. Топология сетей

При организации компьютерной сети в первую очередь необходимо выбрать способ организации физических связей, т. е. топологию. Под **топологией вычислительной сети** понимается конфигурация графа, вершинам которого соответствуют компьютеры сети (иногда и другое оборудование, например концентраторы), а ребрам — физические связи между ними. Компьютеры, подключенные к сети, часто называют **станциями** или **узлами сети**.

Заметим, что конфигурация физических связей определяется электрическими соединениями компьютеров между собой и может отличаться от конфигурации логических связей между узлами сети. **Логические связи** представляют собой маршруты переда-

чи данных между узлами сети и образуются путем соответствующей настройки коммуникационного оборудования.

Выбор топологии электрических связей существенно влияет на многие характеристики сети. Например, наличие резервных связей повышает надежность сети и делает возможным балансирование загрузки отдельных каналов. Простота присоединения новых узлов, свойственная некоторым топологиям, делает сеть легко расширяемой. Экономические соображения часто приводят к выбору топологий, для которых характерна минимальная суммарная длина линий связи. Рассмотрим некоторые, наиболее часто встречающиеся топологии.

Существуют четыре основных топологии: шина (Bus), кольцо (Ring), звезда (Star) и ячеистая топология (Mesh). Другие топологии обычно являются комбинацией двух и более главных типов. Выбор типа физической топологии для сети является одним из первых шагов планирования сети. Выбор топологии основывается на множестве факторов, в число которых входят цена, расстояния, вопросы безопасности, предполагаемая сетевая операционная система, а также будет ли новая сеть использовать существующее оборудование, проводку и т. п.

Физическая топология **«шина»** (Bus), именуемая также линейной шиной (Linear Bus), состоит из единственного кабеля, к которому присоединены все компьютеры сегмента (рис. 1.3). Сообщения посылаются по линии всем подключенным станциям вне зависимости от того, кто является получателем. Каждый компьютер проверяет каждый пакет в проводе, чтобы определить получателя пакета. Если пакет предназначен для другой

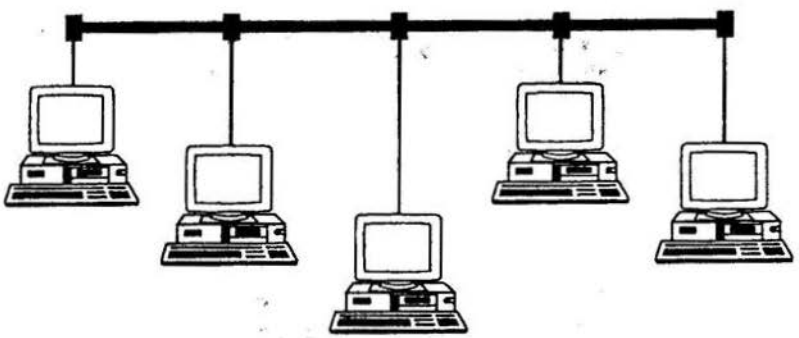

Рис. 1.3. Топология «шина»

станции, компьютер отвергнет его. Соответственно, компьютер получит и обработает любой пакет на шине, адресованный ему.

Главный кабель шины, известный как магистраль (backbone), имеет на обоих концах заглушки (terminator) для предотвращения отражения сигнала. Без правильно установленных заглушек работа шины будет ненадежной или вообще невозможной.

Шинная топология представляет собой быстрейший и простейший способ установки сети. Она требует меньше оборудования и кабелей, чем другие топологии, и ее легче настраивать. Это хороший способ быстрого построения временной сети. Это обычно лучший выбор для малых сетей (не более 10 компьютеров).

Имеется несколько недостатков, о которых надо знать при решении вопроса об использовании шинной топологии для сети. Неполадки станции или другого компонента сети трудно изолировать. Кроме того, неполадки в магистральном кабеле могут привести к выходу из строя всей сети.

Топология **«кольцо»** (Ring) обычно используется в сетях Token Ring и FDDI (волоконно-оптических). В физической топологии Ring линия передачи данных фактически образует логическое кольцо, к которому подключены все компьютеры сети (рис. 1.4). В отличие от шинной топологии, которая использует конкурентную схему, чтобы позволить станциям получать доступ к сетевому носителю, доступ к носителю в кольце осуществляется посредством логических знаков — «маркеров» (token), которые пускаются по кругу от станции к станции, давая им возмож-

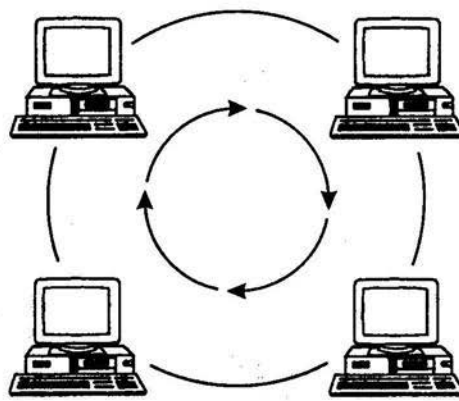

Рис. 1.4. Топология «кольцо»

ность переслать пакет, если это нужно. Это дает каждому компьютеру в сети равную возможность получить доступ к носителю и, следовательно, переслать по нему данные. Компьютер может посылать данные только тогда, когда владеет маркером.

Так как каждый компьютер при этой топологии является частью кольца, он имеет возможность пересылать любые полученные им пакеты данных, адресованные другой станции. Получающаяся регенерация делает сигнал сильным и позволяет избежать необходимости в применении повторителей. Так как кольцо формирует бесконечный цикл, заглушки не требуются. Кольцевая топология относительно легка для установки и настройки, требуя минимального аппаратного обеспечения.

Топология физического кольца имеет несколько недостатков. Как и в случае линейной шины, неполадки на одной станции могут привести к отказу всей сети. Поддерживать логическое кольцо трудно, особенно в больших сетях. Кроме того, в случае необходимости настройки и переконфигурации любой части сети придется временно отключить всю сеть.

Кольцевая топология даст всем компьютерам равные возможности доступа к сетевому носителю.

В топологии **«звезда»** (Star) все компьютеры в сети соединены друг с другом с помощью центрального концентратора (рис. 1.5). Все данные, которые посылает станция, направляются прямо на концентратор, который затем пересылает пакет в направлении

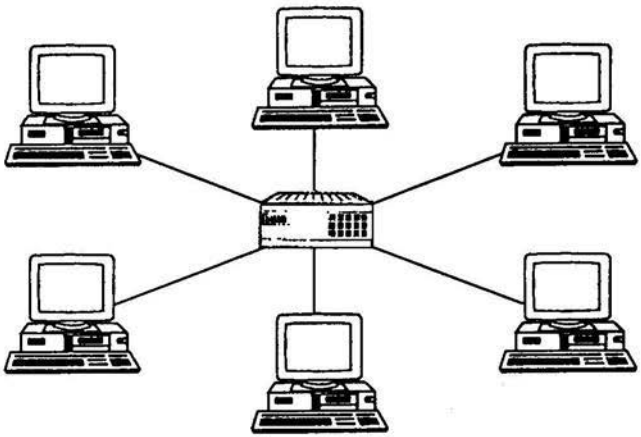

Рис. 1.5. Топология «звезда»

получателя. Как и при шинной топологии, компьютер в сети типа «звезда» может пытаться послать данные в любой момент. Однако на деле только один компьютер может в конкретный момент времени производить посылку. Если две станции посылают сигналы на концентратор точно в одно время, обе посылки окажутся неудачными и каждому компьютеру придется подождать случайный период времени, прежде чем снова пытаться получить доступ к носителю. Сети с топологией Star обычно лучше масштабируются, чем другие типы.

Главное преимущество внедрения топологии «звезда» заключается в том, что в отличие от линейной шины неполадки на одной станции не выведут из строя всю сеть. В сетях с этой топологией проще находить обрывы кабеля и прочие неисправности. Это облегчает обнаружение обрыва кабеля и других неполадок. Кроме того, наличие центрального концентратора в топологии «звезда» облегчает добавление нового компьютера и реконфигурацию сети.

Топологии «звезда» присуще несколько недостатков. Во-первых, этот тип конфигурации требует больше кабеля, чем большинство других сетей, вследствие наличия отдельных линий, соединяющих каждый компьютер с концентратором. Кроме того, центральный концентратор выполняет большинство функций сети, так что выход из строя одного этого устройства отключит всю сеть.

Ячеистая топология (Mesh) соединяет все компьютеры попарно (рис. 1.6). Сети ячеистой топологии используют значительно

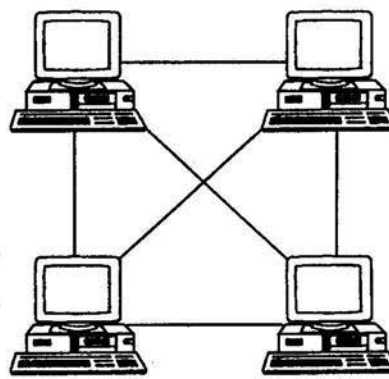

Рис. 1.6. Ячеистая топология

большее количество кабеля, чем любая другая топология, что делает их дороже. Кроме того, такие сети значительно сложнее устанавливать, чем другие топологии. Однако ячеистая топология устойчива к сбоям (fault tolerance). Устойчивость к сбоям заключается в способности работать при наличии повреждений. В сети с поврежденным сегментом это означает обход сегмента. Каждый компьютер имеет множество возможных путей соединения с другим компьютером по сети, так что отдельный обрыв кабеля не приведет к потере соединения между любыми двумя компьютерами.

Многие организации используют комбинации главных сетевых топологий, называемые смешанные сети.

Смешанная топология **звезда на шине** (Star Bus), показанная на рис. 1.7, объединяет топологии «шина» и «звезда». Преимущество этой топологии заключается в том, что никакие неполадки на отдельном компьютере или в сегменте не могут вывести из строя всю сеть. Также в случае неисправности отдельного концентратора не смогут взаимодействовать по сети только те компьютеры, которые присоединены к этому концентратору, а остальные компьютеры эта проблема не затронет.

Топология «звезда на кольце» (Star Ring) известна также под названием Star-wired Ring, поскольку сам концентратор выпол-

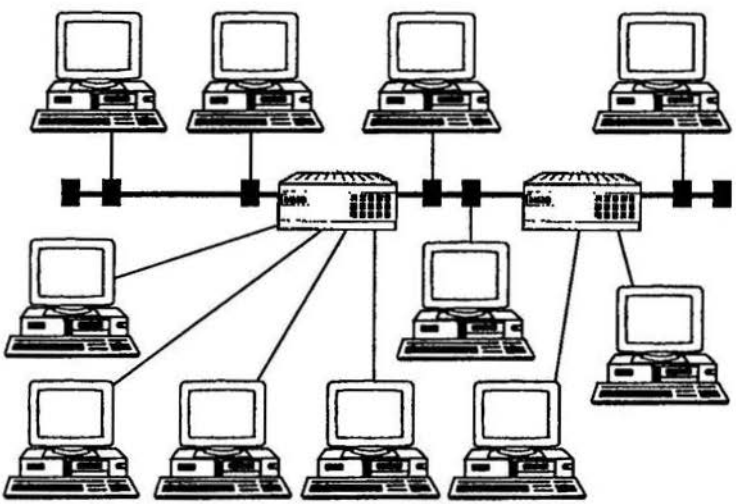

Рис. 1.7. Топология «звезда на шине»

нен как кольцо. Сеть «звезда на кольце» внешне идентична топологии «звезда», но на самом деле концентратор соединен проводами как логическое кольцо (рис. 1.8). Эта топология популярна для сетей Token Ring, поскольку легче в реализации, чем физическое кольцо, но дает возможность посылать «токены» внутри концентратора так же, как и в случае физического кольца. Почти так же, как при топологии «кольцо», компьютеры имеют равный доступ к сетевому носителю за счет посылки «токенов». Повреждение отдельного компьютера не может привести к остановке всей сети, но если выходит из строя концентратор, кольцо, которым управляет концентратор, тоже отключается.

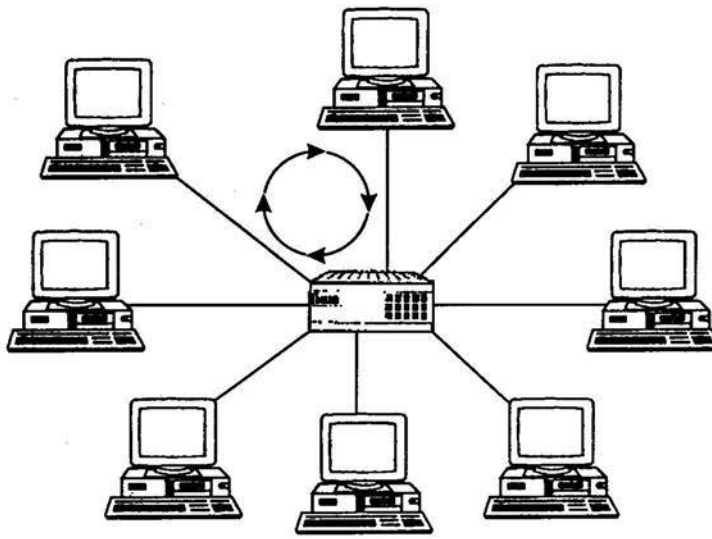

Рис. 1.8. Топология «звезда на кольце»

Реализация настоящей ячеистой топологии в крупных сетях может быть дорогой, требующей времени и непростой. Сеть **«гибридной ячеистой топологии»** (Hybrid Mesh) может предоставить некоторые из существенных преимуществ настоящей сети ячеистой топологии без необходимости использования большого количества кабеля. В большинстве крупных организаций критически важные данные хранятся не на всех компьютерах сети. Вместо этого они хранятся на сетевых серверах. Компании, которые хотят обеспечить защиту от сбоев для своих сетей на уровне кабелей, могут ограничиться только компьютерами с крити-

чески важными данными. Это означает, что ячеистая топология существует только на части сети (рис. 1.9). Этот тип ячеистой топологии по-прежнему обеспечивает защиту от сбоев для серверов с важной информацией, но не добавляет защиты для отдельных клиентов сети. Гибридная ячеистая топология должна стоить меньше, чем сеть, полностью построенная на ячеистой топологии, но будет не столь защищенной от сбоев.

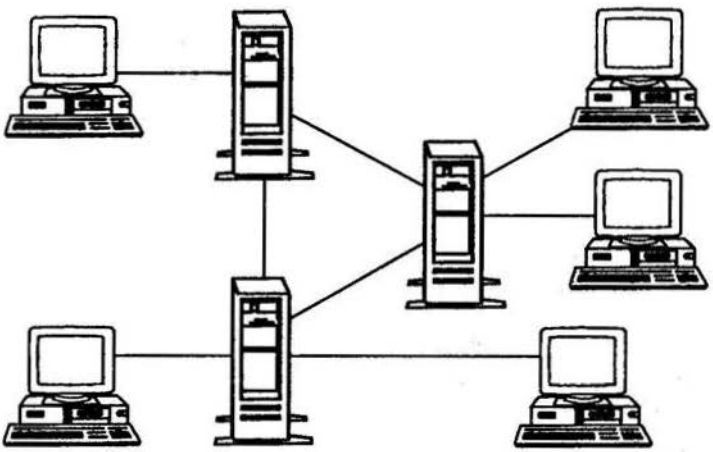

Рис. 1.9. Гибридная ячеистая топология

Физическая структуризация сети полезна во многих отношениях, однако, в ряде случаев, обычно относящихся к сетям большого и среднего размера, невозможно обойтись без логической структуризации сети. Наиболее важной проблемой, не решаемой путем физической структуризации, остается проблема перераспределения передаваемого трафика между различными физическими сегментами сети.

Сегментом сети называется часть сети с общим пространством доступа к среде передачи данных и обнаружения коллизий. При этом под **коллизией** понимается отказ в доступе к среде передачи данных из-за совпадения во времени моментов генерации заявок на ее использование, поступающих от различных станций сети.

Основные недостатки сети на одной разделяемой среде начинают проявляться при превышении некоторого порога количества узлов, подключенных к разделяемой среде, и состоят в

следующем. Даже та доля пропускной способности разделяемой среды, которая должна в среднем доставаться одному узлу (т. е., например, 10/*N* Мбит/с для сети Ethernet с *N* компьютерами), очень часто узлу не достается. Причина заключается в случайном характере метода доступа к среде, используемого во всех технологиях локальных сетей.

Локальные сети, состоящие из одного или двух серверов и небольшого количества рабочих станций, объединяются в корпоративные системы — сложные среды, состоящие из множества серверов различных типов, а также многочисленных рабочих групп, нуждающихся в связи друг с другом. В такой среде несегментированная сеть способна привести к снижению производительности, уменьшению надежности и ухудшению безопасности сети.

Обычно крупные сети имеют высокоскоростную магистраль, но если, например, весь сетевой трафик направляется туда, то он может запросто исчерпать доступную пропускную способность, сводя на нет все преимущества в производительности, которая организация могла бы извлечь при другом подходе. Ввиду того, что рабочие станции взаимодействуют в основном с локальными серверами, имеет смысл сегментировать сеть в соответствии с рабочими группами, в которых большая часть трафика не выходит за пределы локального сегмента. Такой подход позволяет разным группам выделить разную пропускную способность. Например, разработчикам и инженерам выделяется собственный сегмент на 10 Мбит/с, пользователям из отдела маркетинга — другой.

Сегментирование повышает также и надежность сети за счет изолирования проблем в данном сегменте. Например, если разработчики выведут из строя свой собственный сегмент сети, то на других пользователях это никак не скажется.

Сегментирование предполагает, что пакеты не выходят за пределы текущего сегмента (принимаются только узлами сегмента). Для передачи информации из одного сегмента в другой (объединения сегментов) используют специальные устройства: маршрутизаторы, коммутируемые концентраторы (коммутаторы), мосты.

В качестве примера несовпадения физической и логической топологии рассмотрим сеть на рис. 1.3. Физически компьютеры соединены по топологии общая шина. Предположим, что доступ к шине происходит не по алгоритму случайного доступа, применяемому в технологии Ethernet, а путем передачи маркера в коль-

цевом порядке: от компьютера А — компьютеру В, от компьютера В — компьютеру С и т. д. Здесь порядок передачи маркера уже не повторяет физические связи, а определяется логическим конфигурированием драйверов сетевых адаптеров. Ничто не мешает настроить сетевые адаптеры и их драйверы так, чтобы компьютеры образовали кольцо в другом порядке, например: В, А, С... При этом физическая структура сети никак не изменяется.

1.6. Многоуровневые ИВС и эталонная модель взаимосвязи открытых систем

Основу компьютерной сети составляет соединение различного оборудования, где одной из наиболее острых проблем является проблема совместимости. Без принятия всеми производителями общепринятых правил (стандартов) создания сетевого оборудования построение сетей в целом было бы невозможно. В компьютерных сетях идеологической основой стандартизации является многоуровневый подход к разработке средств сетевого взаимодействия. Именно на основе этого подхода была разработана стандартная семиуровневая модель взаимодействия открытых систем, ставшая своего рода универсальным языком сетевых специалистов.

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 термином **«спецификация»** (в вычислительной технике) понимают формализованное описание аппаратных или программных компонентов, способов их функционирования, взаимодействия с другими компонентами, условий эксплуатации, ограничений и особых характеристик. Понятно, что не всякая спецификация является стандартом. В свою очередь, под открытыми спецификациями понимаются опубликованные, общедоступные спецификации, соответствующие стандартам и принятые в результате достижения согласия после всестороннего обсуждения всеми заинтересованными сторонами.

Использование при разработке систем открытых спецификаций позволяет третьим сторонам разрабатывать для этих систем различные аппаратные или программные средства расширения и

модификации, а также создавать программно-аппаратные комплексы из продуктов разных производителей.

Организация взаимодействия между устройствами в сети является сложной задачей, которая разбивается на несколько более простых задач-модулей. Процедура разбиения (декомпозиции) включает в себя четкое определение функций каждого модуля, решающего отдельную задачу, и интерфейсов между ними. В результате достигается логическое упрощение задачи, а также появляется возможность модификации отдельных модулей без изменения остальной части системы.

При декомпозиции часто используют многоуровневый подход. Он заключается в следующем. Все множество модулей разбивают на уровни. Уровни образуют иерархию, т. е. имеются вышележащие и нижележащие уровни (рис. 1.10). Множество модулей, составляющих каждый уровень, сформировано таким образом, что для выполнения своих задач они обращаются с запросами только к модулям непосредственно примыкающего нижележащего уровня. С другой стороны, результаты работы всех модулей, принадлежащих некоторому уровню, могут быть переданы только модулям соседнего вышележащего уровня. Такая иерархическая декомпозиция задачи предполагает четкое определение функции каждого уровня и интерфейсов между уровнями. Интерфейс определяет набор функций, которые нижележащий уровень предоставляет вышележащему. В результате иерархической декомпозиции достигается относительная независимость уровней, а значит, и возможность их легкой замены.

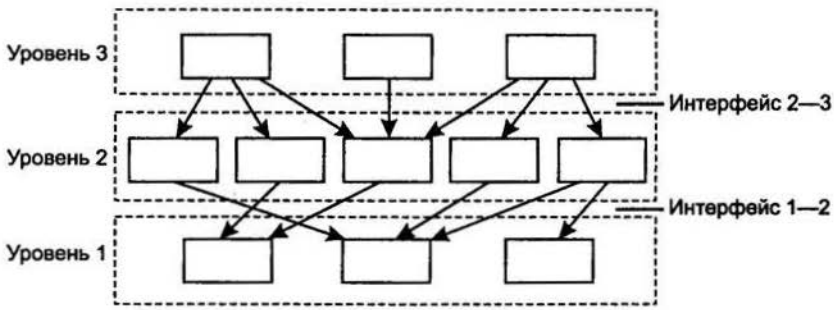

Рис. 1.10. Многоуровневый подход к созданию ИВС

Средства сетевого взаимодействия также могут быть представлены в виде иерархически организованного множества модулей.

При этом модули нижнего уровня могут, например, решать все вопросы, связанные с надежной передачей электрических сигналов между двумя соседними узлами. Модули более высокого уровня организуют транспортировку сообщений в пределах всей сети, пользуясь для этого средствами упомянутого нижележащего уровня. А на верхнем уровне работают модули, предоставляющие пользователям доступ к различным службам — файловой, печати и т. п.

Многоуровневое представление средств сетевого взаимодействия имеет свою специфику, связанную с тем, что для организации обмена сообщениями между двумя компьютерами необходимо принять множество соглашений для всех уровней, начиная от самого низкого уровня передачи битов и до самого высокого уровня, реализующего сервис для пользователей сети.

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

Модули, реализующие протоколы соседних уровней и находящиеся в одном узле, также взаимодействуют друг с другом в соответствии с четко определенными правилами и с помощью стандартизованных форматов сообщений, которые называются **интерфейсом**. Таким образом, протоколы определяют правила взаимодействия модулей одного уровня в разных узлах, а интерфейсы определяют правила взаимодействия модулей соседних уровней в одном узле.

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, чисто программными средствами. На эффективность взаимодействия устройств в сети влияет качество всей совокупности протоколов, составляющих стек, в частности, насколько рационально распределены функции между протоколами разных уровней и насколько хорошо определены интерфейсы между ними.

Протоколы реализуются не только компьютерами, но и другими сетевыми устройствами — концентраторами, мостами, коммутаторами, маршрутизаторами и т. д. Действительно, в об-

щем случае связь компьютеров в сети осуществляется не напрямую, а через различные коммуникационные устройства. В зависимости от типа устройства в нем должны быть встроенные средства, реализующие тот или иной набор протоколов.

В начале 1980-х годов ряд международных организаций по стандартизации — ISO, ITU и некоторые другие — разработали модель, которая сыграла значительную роль в развитии сетей. Эта модель называется **моделью взаимодействия открытых систем** или моделью OSI (**Open System Interconnection**). Модель OSI определяет различные уровни взаимодействия систем, дает им стандартные имена и указывает, какие функции должен выполнять каждый уровень. Модель OSI была разработана на основании большого опыта, полученного при создании компьютерных сетей, в основном глобальных, в 1970-е годы. Полное описание этой модели занимает более 1000 страниц текста.

В модели OSI (рис. 1.11) 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.

Физический уровень (Physical layer) имеет дело с передачей битов по физическим каналам связи, таким, например, как коаксиальный кабель, витая пара, оптоволоконный кабель или цифровой территориальный канал. К этому уровню имеют отношение характеристики физических сред передачи данных, такие как полоса пропускания, помехозащищенность, волновое сопротивление и другие. 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 стандартизуются типы разъемов и назначение каждого контакта.

Функции физического уровня реализуются во всех устройствах, подключенных к сети. Со стороны компьютера функции физического уровня выполняются сетевым адаптером или последовательным портом.

В некоторых сетях линии связи используются (разделяются) попеременно несколькими парами взаимодействующих компьютеров, и физическая среда передачи может быть занята. Поэтому одной из задач **канального уровня** (Data Link layer) является проверка доступности среды передачи. Другой задачей канального

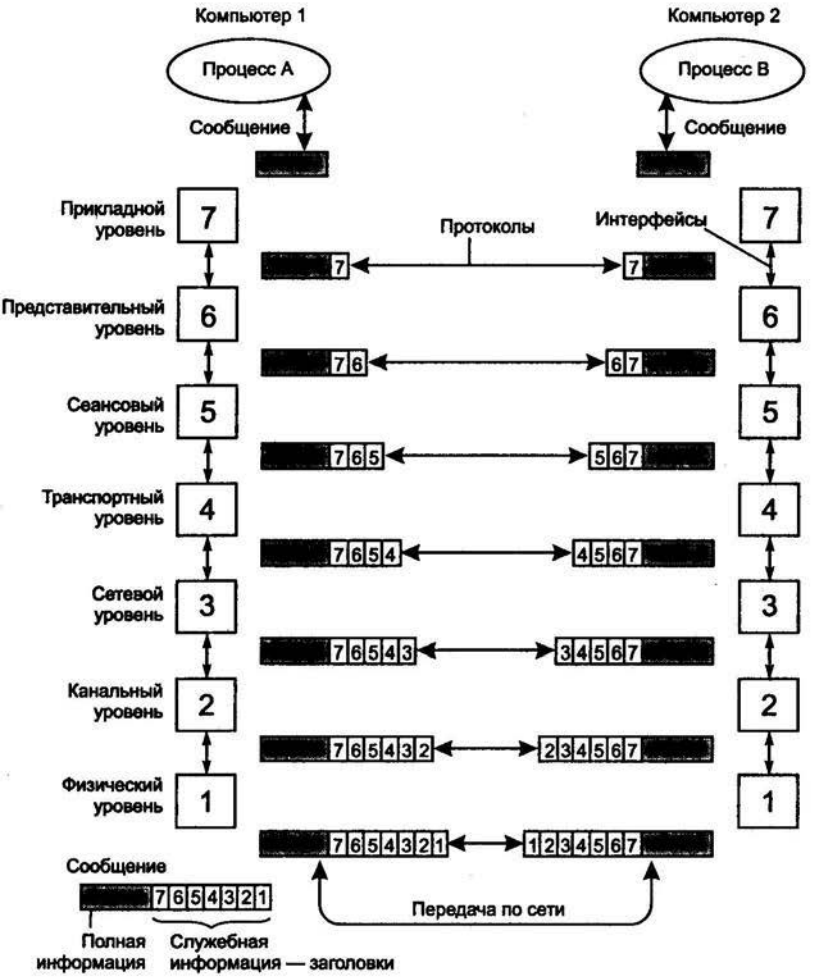

Рис. 1.11. Модель взаимодействия открытых систем ISO/OSI

ровня является реализация механизмов обнаружения и коррек-ии ошибок. Для этого на канальном уровне биты группируются наборы, называемые **кадрами**. Канальный уровень обеспечива-т корректность передачи каждого кадра, помещая специальную оследовательность бит в начало и конец каждого кадра для его ыделения, а также вычисляет контрольную сумму, обрабатывая се байты кадра определенным способом и добавляя контроль-ую сумму к кадру. Когда кадр приходит по сети, получатель

снова вычисляет контрольную сумму полученных данных и сравнивает результат с контрольной суммой из кадра. Если они совпадают, кадр считается правильным и принимается. Если же контрольные суммы не совпадают, то фиксируется ошибка. Канальный уровень может не только обнаруживать ошибки, но и исправлять их за счет повторной передачи поврежденных кадров. Необходимо отметить, что функция исправления ошибок не является обязательной для канального уровня, поэтому в некоторых протоколах этого уровня она отсутствует.

К типовым топологиям, поддерживаемым протоколами канального уровня локальных сетей, относятся общая шина, кольцо и звезда, а также структуры, полученные из них с помощью мостов и коммутаторов. Примерами протоколов канального уровня являются протоколы Ethernet, Token Ring, FDDI.

В локальных сетях протоколы канального уровня используются компьютерами, мостами, коммутаторами и маршрутизаторами. В компьютерах функции канального уровня реализуются совместными усилиями сетевых адаптеров и их драйверов.

В глобальных сетях, которые редко обладают регулярной топологией, канальный уровень часто обеспечивает обмен сообщениями только между двумя соседними компьютерами, соединенными индивидуальной линией связи.

Для обеспечения качественной транспортировки сообщений в сетях любых топологий и технологий функций канального уровня оказывается недостаточно, поэтому в модели OSI решение этой задачи возлагается на два следующих уровня — сетевой и транспортный.

Сетевой уровень (Network layer) 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.

На сетевом уровне сам термин **сеть** наделяют специфическим значением. В данном случае под сетью понимается совокупность компьютеров, соединенных между собой в соответствии с одной из стандартных типовых топологий и использующих для передачи данных один из протоколов канального уровня, определенный для этой топологии.

Внутри сети доставка данных обеспечивается соответствующим канальным уровнем, а вот доставкой данных между сетями занимается сетевой уровень, который и поддерживает возмож-

ность 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.

Сетевой уровень решает также задачи согласования разных технологий, упрощения адресации в крупных сетях и создания надежных и гибких барьеров на пути нежелательного трафика между сетями.

Сообщения сетевого уровня принято называть **пакетами** (packets). 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 сети должны иметь одну и ту же старшую часть адреса, поэтому термину «сеть» на сетевом уровне можно дать и другое, более формальное определение: сеть — это совокупность узлов, сетевой адрес которых содержит один и тот же номер сети.

Транспортный уровень (Transport layer) обеспечивает приложениям или верхним уровням стека — прикладному и сеансовому — передачу данных с той степенью надежности, которая им требуется. 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, а главное — способностью к обнаружению и исправлению ошибок передачи, таких как искажение, потеря и дублирование пакетов.

Сеансовый уровень (Session layer) обеспечивает управление диалогом: фиксирует, какая из сторон является активной в настоящий 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.

Представительный уровень (Presentation layer) 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 кодов ASCII и EBCDIC. На этом уровне может выполняться шифрование и дешифрование данных, благодаря которому секретность обмена данными обеспечивается сразу для всех прикладных служб. Примером такого протокола является протокол SSL (Secure Socket Layer), который обеспечивает секретный обмен сообщениями для протоколов прикладного уровня стека TCP/IP.

Прикладной уровень (Application layer) — это набор разнообразных протоколов, с помощью которых пользователи сети получают доступ к разделяемым ресурсам, таким как файлы, принтеры или гипертекстовые Web-страницы, а также организуют свою совместную работу, например, с помощью протокола электронной почты. Единица данных, которой оперирует прикладной уровень, обычно называется **сообщением** (message).

Сетезависимые и сетенезависимые 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 приложениями.

Три нижних уровня — физический, канальный и сетевой — являются сетезависимыми, т. е. протоколы этих уровней тесно связаны с технической реализацией сети и используемым коммуникационным оборудованием. Например, переход на оборудование FDDI означает полную смену протоколов физического и канального уровней во всех узлах сети.

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. Так, переход от Ethernet на высокоскоростную технологию 100VG-AnyLAN не потребует никаких изменений в программных средствах, реализующих функции прикладного, представительного и сеансового уровней.

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. Компьютер с установленной на нем сетевой ОС взаимодействует с другим компьютером с помощью протоколов всех семи уровней. Это взаимодействие компьютеры осуществляют опосредованно через различные коммуникационные устройства: концентраторы, модемы, мосты, коммутаторы, маршрутизаторы, мультиплексоры. В зависимости от типа коммуникационное устройство 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).

В модели OSI различаются два основных типа протоколов. В протоколах с **установлением соединения** (connection-oriented) 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 это соединение.

Вторая группа протоколов — протоколы **без предварительного установления соединения** (connectionless). Отправитель просто передает сообщение, когда оно готово. При взаимодействии компьютеров используются протоколы обоих типов.

Модель OSI касается только 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.

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, это позволяет сети развиваться с минимальными затратами;
- возможность легкого сопряжения одной сети с другой;
- простота освоения и обслуживания сети.

Примером открытой системы является международная сеть Internet. Эта сеть развивалась в полном соответствии с требованиями, предъявляемыми к открытым системам. В разработке ее стандартов принимали участие тысячи специалистов-пользователей этой сети из различных университетов, научных организаций и фирм-производителей вычислительной аппаратуры и программного обеспечения, работающих в разных странах.

1.7. Стандартные стеки коммуникационных протоколов

Важнейшим направлением стандартизации в области вычислительных 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 стандартизованные протоколы Ethernet, Token Ring, FDDI и некоторые другие, которые позволяют использовать во всех сетях одну и ту же аппаратуру. Зато на верхних уровнях все стеки работают по своим собственным протоколам. Эти протоколы часто не соответствуют рекомендуемому моделью OSI разбиению на уровни. В частности, функции сеансового и представительного уровня, как правило, объединены с прикладным уровнем. Такое несоответствие связано с тем, что модель OSI появилась как результат обобщения уже существующих и реально используемых стеков, а не наоборот.

Следует четко различать модель OSI и стек OSI. В то время как модель OSI является концептуальной схемой взаимодействия открытых систем, стек OSI представляет собой набор вполне конкретных спецификаций протоколов. В отличие от других стеков протоколов стек OSI полностью соответствует модели OSI, он включает 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, — т. е. 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.

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.

Стек TCP/IP был разработан по инициативе Министерства обороны США более 20 лет назад для связи экспериментальной сети ARPAnet с другими сетями как набор общих протоколов для разнородной вычислительной среды. Сегодня этот стек используется для связи компьютеров всемирной информационной 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, давшими ему название, являются протоколы 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, почтовый протокол SMTP, исполь-

зуемый в электронной почте сети Internet, гипертекстовые сервисы службы WWW и многие другие.

В табл. 1.1 показано соответствие некоторых, наиболее популярных протоколов уровням модели OSI. Часто это соответствие весьма условно, так как модель OSI — это только руководство к действию, причем достаточно общее, а конкретные протоколы разрабатывались для решения специфических задач, причем многие из них появились до разработки модели OSI. В большинстве случаев разработчики стеков отдавали предпочтение скорости работы сети в ущерб модульности — ни один стек, кроме стека OSI, не разбит на семь уровней. Чаще всего в стеке явно выделяются 3—4 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.

Таблица 1.1. **Соответствие стеков протоколов модели OSI**

<table>
<tr><th>Модель OSI</th><th>IBM/Microsoft</th><th>TCP/IP</th><th>Novell</th><th>Стек OSI</th></tr>
<tr><td>Прикладной</td><td rowspan="2">SMB</td><td rowspan="2">Telnet, FTP, SNMP, SMTP, WWW</td><td rowspan="3">NCP, SAP</td><td>X/400
X500
FTAM</td></tr>
<tr><td>Представительный</td><td>Представительный протокол OSI</td></tr>
<tr><td>Сеансовый</td><td rowspan="2">NetBIOS</td><td rowspan="2">TCP</td><td>Сеансовый протокол OSI</td></tr>
<tr><td>Транспортный</td><td>SPX</td><td>Транспортный протокол OSI</td></tr>
<tr><td>Сетевой</td><td></td><td>IP, RIP, OSPF</td><td>IPX, RIP, NLSP</td><td>ES-ES
IS-IS</td></tr>
<tr><td>Канальный</td><td colspan="4">802.3 (Ethernet), 802.5 (Token Ring), FDDI, Fast Ethernet, SLIP, 100VG-AnyLAN, X.25, ATM, LAP-B, LAP-D, PPP</td></tr>
<tr><td>Физический</td><td colspan="4">Коаксиал, экранированная и неэкранированная витые пары, оптоволокно, радиоволны</td></tr>
</table>

В 1980 г. в институте IEEE был организован комитет 802 по стандартизации локальных сетей, в результате работы которого было принято семейство стандартов IEEE 802-х, которые содер-

жат рекомендации по проектированию нижних уровней локальных сетей.

Стандарты семейства IEEE 802.X охватывают только два нижних уровня семиуровневой модели OSI — физический и канальный. Это связано с тем, что именно эти уровни в наибольшей степени отражают специфику локальных сетей. Старшие же уровни, начиная с сетевого, в значительной степени имеют общие черты как для локальных, так и для глобальных сетей.

Специфика локальных сетей также нашла свое отражение в разделении канального уровня на два подуровня, которые часто называют также уровнями. Канальный уровень (Data Link Layer) делится в локальных сетях на два подуровня:

- логической передачи данных (Logical Link Control — LLC);
- управления доступом к среде (Media Access Control — MAC).

Уровень MAC появился из-за существования в локальных сетях разделяемой среды передачи данных. Именно этот уровень обеспечивает корректное совместное использование общей среды, предоставляя ее в соответствии с определенным алгоритмом в распоряжение той или иной станции сети. После того как доступ к среде получен, ею может пользоваться более высокий уровень — уровень LLC, организующий передачу логических единиц данных, кадров информации, с различным уровнем качества транспортных услуг. В современных локальных сетях получили распространение несколько протоколов уровня MAC, реализующих различные алгоритмы доступа к разделяемой среде. Эти протоколы полностью определяют специфику таких технологий, как Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI, 100VG-AnyLAN.

Уровень LLC отвечает за передачу кадров данных между узлами с различной степенью надежности, а также реализует функции интерфейса с прилегающим к нему сетевым уровнем. Именно через уровень LLC сетевой протокол запрашивает у канального уровня нужную ему транспортную операцию с нужным качеством. На уровне LLC существует несколько режимов работы, отличающихся наличием или отсутствием на этом уровне процедур восстановления кадров в случае их потери или искажения, т. е. отличающихся качеством транспортных услуг этого уровня.

Протоколы уровней MAC и LLC взаимно независимы — каждый протокол уровня MAC может применяться с любым протоколом уровня LLC, и наоборот.

Стандарты IEEE 802 имеют достаточно четкую структуру:

- 802.1 — Internetworking — объединение сетей;
- 802.2 — Logical Link Control, LLC — управление логической передачей данных;
- 802.3 — Ethernet с методом доступа CSMA/CD;
- 802.4 — Token Bus LAN — локальные сети с методом доступа Token Bus;
- 802.5 — Token Ring LAN — локальные сети с методом доступа Token Ring;
- 802.6 — Metropolitan Area Network, MAN — сети мегаполисов;
- 802.7 — Broadband Technical Advisory Group — техническая консультационная группа по широкополосной передаче;
- 802.8 — Fiber Optic Technical Advisory Group — техническая консультационная группа по волоконно-оптическим сетям;
- 802.9 — Integrated Voice and data Networks — интегрированные сети передачи голоса и данных;
- 802.10 — Network Security — сетевая безопасность;
- 802.11 — Wireless Networks — беспроводные сети;
- 802.12 — Demand Priority Access LAN, 100VG-AnyLAN — локальные сети с методом доступа по требованию с приоритетами.

1.8. Сетевые компоненты

Существует множество сетевых устройств, которые возможно использовать для создания, сегментирования и усовершенствования сети. Основными из них являются сетевые адаптеры, повторители, усилители, мосты, маршрутизаторы, коммутаторы и шлюзы.

Сетевые адаптеры (карты), или NIC (Network Interface Card), являются теми устройствами, которые физически соединяют компьютер с сетью. Сетевые адаптеры — это сетевое оборудование, обеспечивающее функционирование сети на физическом и канальном уровнях.

Сетевые адаптеры производят следующие основные операции при приеме или передаче сообщения:

1) *гальваническая развязка* с коаксиальным кабелем или витой парой. Для этой цели используются импульсные трансформаторы. Иногда для развязки используются оптроны;

2) *прием (передача) данных.* Данные передаются из ОЗУ ПК в адаптер или из адаптера в память ПК через программируемый канал ввода/вывода, канал прямого доступа или разделяемую память;

3) *буферизация.* Для согласования скоростей пересылки данных в адаптер или из него со скоростью обмена по сети используются буфера. Во время обработки в сетевом адаптере данные хранятся в буфере. Буфер позволяет адаптеру осуществлять доступ ко всему пакету информации. Использование буферов необходимо для согласования между собой скоростей обработки информации различными компонентами ЛВС;

4) *формирование пакета.* Сетевой адаптер должен разделить данные на блоки в режиме передачи (или соединить их в режиме приема) данных и оформить в виде кадра определенного формата. Кадр включает несколько служебных полей, среди которых имеется адрес компьютера назначения и контрольная сумма кадра, по которой сетевой адаптер станции назначения делает вывод о корректности доставленной по сети информации;

5) *доступ к каналу связи.* Набор правил, обеспечивающих доступ к среде передачи. Выявление конфликтных ситуаций и контроль состояния сети;

6) *идентификация своего адреса* в принимаемом пакете. Физический адрес адаптера может определяться установкой переключателей, храниться в специальном регистре или прошиваться в ППЗУ;

7) *преобразование* параллельного кода в последовательный код при передаче данных и из последовательного кода в параллельный при приеме. В режиме передачи данные передаются по каналу связи в последовательном коде;

8) *кодирование и декодирование данных.* На этом этапе должны быть сформированы электрические сигналы, используемые для представления данных. Большинство сетевых адаптеров для этой цели используют манчестерское кодирование. Этот метод не требует передачи синхронизирующих сигналов для распознавания единиц и нулей по уровням сигналов, а вместо этого для представления 1 и 0 используется перемена полярности сигнала;

9) *передача или прием импульсов.* В режиме передачи закодированные электрические импульсы данных передаются в кабель (при приеме импульсы направляются на декодирование).

Сетевой адаптер относится к периферийному устройству компьютера, непосредственно взаимодействующему со средой

передачи данных, которая прямо или через другое коммуникационное оборудование связывает его с другими компьютерами. Это устройство решает задачи надежного обмена двоичными данными, представленными соответствующими электромагнитными сигналами, по внешним линиям связи. Как и любой контроллер компьютера, сетевой адаптер работает под управлением драйвера операционной системы, и распределение функций между сетевым адаптером и драйвером может изменяться от реализации к реализации.

Компьютер, будь то сервер или рабочая станция, подключается к сети с помощью внутренней платы — сетевого адаптера (хотя бывают и внешние сетевые адаптеры, подключаемые к компьютеру через параллельный порт). Сетевой адаптер вставляется в гнездо материнской платы. Карты сетевых адаптеров устанавливаются на каждой рабочей станции и на файловом сервере. Рабочая станция отправляет запрос к файловому серверу и получает ответ через сетевой адаптер, когда файловый сервер готов. Сетевые адаптеры преобразуют параллельные коды, используемые внутри компьютера и представленные маломощными сигналами, в последовательный поток мощных сигналов для передачи данных по внешней сети. Сетевые адаптеры должны быть совместимы с кабельной системой сети, внутренней информационной шиной ПК и сетевой операционной системой. Простота или сложность этой установки и настройки зависит от типа сетевого адаптера, который предполагается использовать. Для некоторых конфигураций достаточно просто вставить адаптер в подходящий слот материнской платы компьютера. Автоматически конфигурирующиеся адаптеры, а также адаптеры, отвечающие стандарту Plug and Play (Вставь и работай), автоматически производят свою настройку. Если сетевой адаптер не отвечает стандарту Plug and Play, требуется настроить его запрос на прерывание IRQ (Interrupt Request) и адрес ввода/вывода (Input/Output address). IRQ представляет собой логическую коммуникационную линию, которую устройство использует для связи с процессором. Адрес ввода/вывода — это трехзначное шестнадцатеричное число, которое идентифицирует коммуникационный канал между аппаратными устройствами и центральным процессором. Чтобы сетевой адаптер функционировал правильно, должны быть правильно настроены как IRQ, так и адрес ввода/вывода.

Обычно плата адаптера использует адреса портов ввода/вывода, которые выбираются перемычками или переключателями на

плате. Прежде чем выбрать значения адресов адаптера, необходимо проверить, чтобы в данном компьютере эти адреса были свободны, иначе возможны конфликты. Кроме того, адаптер, как правило, использует одно из аппаратных прерываний компьютера. Номер канала прерывания, используемого адаптером, чаще всего выбирается перемычками или переключателями. Прежде чем выбрать номер используемого прерывания необходимо проверить, чтобы это прерывание не использовалось другими устройствами. Иногда адаптер использует режим прямого доступа к памяти (ПДП или DMA — Direct Memory Access), номер которого выбирается перемычками или переключателями. В этом случае выбирать номер канала ПДП надо таким образом, чтобы не было конфликтов с другими устройствами компьютера. Информацию о свободных адресах, номерах каналов прерывания и ПДП можно получить из тестовых программ.

В последнее время появились адаптеры, в которых выбор адресов и каналов прерываний и ПДП производится не переключателями, а с помощью специальной программы установки (jumperless-адаптеры). Это, конечно, гораздо удобнее. При запуске программы пользователю предлагается установить конфигурацию аппаратуры с помощью простого меню: выбрать адреса ввода/вывода, помер канала прерывания, ПДП, адреса загрузочного ППЗУ и тип используемого внешнего разъема (тип среды передачи). Эта же программа позволяет произвести самотестирование адаптера.

Повторители и усилители

Сигнал при перемещении по сети ослабевает. Чтобы противодействовать этому ослаблению, можно использовать повторители и/или усилители, которые усиливают сигналы, проходящие через них по сети.

Повторители (repeater) используются в сетях с цифровым сигналом для борьбы с ослаблением сигнала. Повторители обеспечивают надежную передачу данных на большие расстояния, нежели обычно позволяет тип носителя. Когда повторитель получает ослабленный входящий сигнал, он очищает сигнал, увеличивает его мощность и посылает этот сигнал следующему сегменту.

Усилители (amplifier), хоть и имеют сходное назначение, используются для увеличения дальности передачи в сетях, использующих аналоговый сигнал. Аналоговые сигналы могут перено-

сить как голос, так и данные одновременно — носитель делится на несколько каналов, так что разные частоты могут передаваться параллельно.

Повторители и усилители действуют на физическом уровне сетевой модели OSI.

Концентратор (hub) представляет собой сетевое устройство, служащее в качестве центральной точки соединения в сетевой конфигурации «звезда» (star) и действует на физическом уровне сетевой модели OSI. Концентратор также может быть использован для соединения сетевых сегментов. Существуют три основных типа концентраторов: пассивные (passive), активные (active) и интеллектуальные (intelligent). Пассивные концентраторы, не требующие электроэнергии, действуют просто как физическая точка соединения, ничего не добавляя к проходящему сигналу. Активные концентраторы требуют энергии, которую они используют для восстановления и усиления сигнала, проходящего через них. Интеллектуальные концентраторы могут предоставлять такие сервисы, как переключение пакетов (packet switching) и перенаправление трафика (traffic routing). Напомним, что переключение пакетов позволяет не поддерживать постоянный физический канал между двумя устройствами. Информация при этом способе коммутации делится на части, называющиеся пакетами, и каждый пакет передается отдельно по свободным в данный момент каналам связи. При этом каждый пакет может проходить по своему маршруту.

Перенаправление трафика осуществляется при перегрузках и отказах оборудования.

Мост (bridge) представляет собой устройство, используемое для соединения сетевых сегментов.

В соответствии с базовой эталонной моделью взаимодействия открытых систем мост описывается протоколами физического и канального уровней, над которыми располагаются канальные процессы. Мост опирается на пару связываемых им физических средств соединения, которые в этой модели представляют физические каналы.

Логический сегмент образуется путем объединения нескольких физических сегментов (отрезков кабеля) с помощью одного или нескольких концентраторов. Каждый логический сегмент подключается к отдельному порту моста/коммутатора. При поступлении кадра на какой-либо из портов мост/коммутатор повторяет этот кадр, но не на всех портах, как это делает концен-

тратор, а только на том порту, к которому подключен сегмент, содержащий компьютер-адресат.

Мост функционирует в первую очередь как повторитель, он может получать данные из любого сегмента, однако он более разборчив в передаче этих сигналов, чем повторитель. Если получатель пакета находится в том же физическом сегменте, что и мост, то мост знает, что этот пакет достиг цели и, таким образом, больше не нужен. Однако, если получатель пакета находится в другом физическом сегменте, мост знает, что его надо переслать. Эта обработка помогает уменьшить загрузку сети. Например, сегмент не получает сообщений, не относящихся к нему.

Мосты могут соединять сегменты, которые используют разные типы носителей (кабелей). Они могут соединять сети с разными схемами доступа к носителю — например, сеть Ethernet и сеть Token Ring. Примером таких устройств являются мосты-трансляторы (translating bridge), которые осуществляют преобразование между различными методами доступа к носителю, позволяя связывать сети разных типов. Другой специальный тип моста, прозрачный (transparent bridge), или интеллектуальный мост (learning bridge), периодически «изучает», куда направлять получаемые им пакеты. Он делает это посредством непрерывного построения специальных таблиц, добавляя в них по мере необходимости новые элементы.

Возможным недостатком мостов является то, что они передают данные дольше, чем повторители, так как проверяют адрес сетевой карты получателя для каждого пакета. Они также сложнее в управлении и дороже, нежели повторители.

Маршрутизатор (router) представляет собой сетевое коммуникационное устройство, которое может связывать два и более сетевых сегментов (или подсетей). Маршрутизатор реализует протоколы физического, канального и сетевого уровней. Специальные сетевые процессы соединяют части коммутатора в единое целое. Физический, канальный и сетевой протоколы в разных сетях различны. Поэтому соединение пар коммуникационных сетей осуществляется через маршрутизаторы, которые осуществляют необходимое преобразование указанных протоколов. Сетевые процессы выполняют взаимодействие соединяемых сетей.

Маршрутизатор работает с несколькими каналами, направляя в какой-нибудь из них очередной блок данных.

Маршрутизаторы обмениваются информацией об изменениях структуры сетей, трафике и их состоянии. Благодаря этому

выбирается оптимальный маршрут следования блока данных в разных сетях от абонентской системы-отправителя к системе-получателю.

Маршрутизатор для фильтрации трафика использует не адрес сетевой карты компьютера, а информацию о сетевом адресе, передаваемую в относящейся к сетевому уровню части пакета. После получения этой информации об адресе маршрутизатор использует таблицу маршрутизации (routing table), содержащую сетевые адреса, чтобы определить, куда направить пакет. Он делает это посредством сравнения сетевого адреса в пакете с элементами в таблице маршрутизации — если совпадение найдено, пакет направляется по указанному маршруту. Если же совпадение не найдено, обычно пакет отбрасывается.

Маршрут по умолчанию (default route) используется, если не подходит ни один из других маршрутов. Требуемый маршрут сначала ищется в таблицах, а если он не найден, пакет посылается в узел, специально выбранный для данного случая. Маршруты по умолчанию используются обычно тогда, когда маршрутизатор имеет ограниченный объем памяти или по какой-то иной причине не имеет полной таблицы маршрутизации. Маршрут по умолчанию может помочь реализовать связь даже при ошибках в маршрутной таблице, однако для региональных сетей с ограниченной пропускной способностью такое решение может повлечь серьезные последствия. Например, из-за такого рода ошибки пакеты внутри локальной сети могут пересылаться через сеть другой страны.

Существуют два типа маршрутизирующих устройств: статические и динамические. Статические маршрутизаторы (static router) используют таблицы маршрутизации, которые должен создать и вручную обновлять сетевой администратор. С другой стороны, динамические маршрутизаторы (dynamic router) создают и обновляют свои собственные таблицы маршрутизации. Они используют информацию как найденную на своих собственных сегментах, так и полученную от других динамических маршрутизаторов. Динамические маршрутизаторы всегда содержат свежую информацию о возможных маршрутах по сети, а также информацию об узких местах и задержках в прохождении пакетов. Эта информация позволяет им определить наиболее эффективный путь, доступный в данный момент, для перенаправления пакетов данных к их получателям. Более подробно алгоритмы маршрутизации рассматриваются в параграфе 5.2.

Поскольку маршрутизаторы могут осуществлять интеллектуальный выбор пути и отфильтровывать пакеты, которые им не нужно получать, они помогают уменьшить загрузку сети, сохранить ресурсы и увеличить пропускную способность. Кроме того, они повышают надежность доставки данных, поскольку маршрутизаторы могут выбрать для пакетов альтернативный путь, если маршрут по умолчанию недоступен.

Термин «маршрутизатор» (router) может обозначать элемент электронной аппаратуры, сконструированной специально для маршрутизации. Он также может означать компьютер (обеспеченный таблицей маршрутизации), подключенный к другим сегментам сети с помощью нескольких сетевых карт и, следовательно, способный выполнять функции маршрутизации между связанными сегментами.

Маршрутизаторы превосходят мосты своей способностью фильтровать и направлять пакеты данных по сети. И в отличие от мостов для них можно отключить пересылку широковещательных сообщении, что уменьшает сетевой широковещательный трафик.

Другое важное преимущество маршрутизатора как соединительного устройства заключается в том, что, поскольку он работает на сетевом уровне, он может соединять сети, использующие различную сетевую архитектуру, методы доступа к устройствам или протоколы. Например, маршрутизатор может соединять подсеть Ethernet и сегмент Token Ring. Он может связывать несколько небольших сетей, использующих различные протоколы, если используемые протоколы поддерживают маршрутизацию.

Маршрутизаторы по сравнению с повторителями дороже и сложнее в управлении. У них меньшая пропускная способность, чем у мостов, поскольку они должны производить дополнительную обработку пакетов данных. Кроме того, динамические маршрутизаторы могут добавлять излишний трафик в сети, поскольку для обновления таблиц маршрутизации постоянно обмениваются сообщениями.

Английский термин «Brouter» (**мост-маршрутизатор**) представляет собой комбинацию слов «bridge» (мост) и «router» (маршрутизатор). Из этого можно сделать вывод, что мост-маршрутизатор сочетает функции моста и маршрутизатора. Когда мост-маршрутизатор получает пакет данных, он проверяет, послан пакет с использованием маршрутизируемого протокола или нет. Если это пакет маршрутизируемого протокола, мост-маршрути-

затор выполняет функции маршрутизатора, посылая при необходимости пакет получателю вне локального сегмента.

Если же пакет содержит немаршрутизируемый протокол, мост-маршрутизатор выполняет функции моста, используя адрес сетевой карты для поиска получателя на локальном сегменте. Для выполнения этих двух функций мост-маршрутизатор может поддерживать как таблицы маршрутизации, так и таблицы мостов.

Коммутаторы. В отличие от концентраторов, которые полностью воплощают в себе идеологию общей разделяемой среды и превращают сеть в единый домен, коммутаторы — это более интеллектуальные устройства, способные анализировать адрес назначения кадра и передавать его не всем станциям сети, а только адресату.

До появления коммутаторов задача разбиения сети на сегменты решалась с помощью мостов, которые в настоящее время практически не используются. Основной же принцип действия мостов и коммутаторов остался неизменным. Именно поэтому коммутаторы иногда называют многопортовыми мостами.

Конструктивно коммутатор представляет собой многопортовое устройство, предназначенное для деления сети на множество сегментов. В сетях Ethernet коммутаторы используют в своей работе алгоритм прозрачного моста (transparent bridge), регламентированного в стандарте IEEE 802.1D. Алгоритм прозрачного моста подразумевает, что коммутатор «обучается» в процессе своей работы. Коммутатор строит свою адресную таблицу на основании пассивного наблюдения за трафиком, циркулирующим в сети. В начальный момент времени коммутатор ничего не знает об адресах подключенных к его портам компьютеров или сегментах сети. По мере того как подключенные к портам коммутатора узлы начинают проявлять активность, коммутатор анализирует содержимое адресов отправителя кадров, что позволяет делать вывод о принадлежности того или иного узла к тому или иному порту коммутатора. Адреса отправителей кадров заносятся в таблицу адресов коммутатора.

В начальный момент времени коммутатор работает в неразборчивом режиме, передавая полученные кадры на все порты. Построив таблицу адресов, коммутатор может передавать полученные кадры не на все порты, а только по адресу назначения. Если на порт коммутатора поступает кадр с адресом назначения, приписанным к другому порту коммутатора, то кадр передается между портами. Такой процесс называется продвижением кадра

(forwarding). Если же коммутатор определяет, что адрес назначения приписан к тому порту, на который поступил данный кадр, то кадр отбрасывается или отфильтровывается, т. е. удаляется из буфера порта. Такой процесс называется фильтрацией (filtering).

Коммутаторы позволяют создавать изолированные друг от друга локальные сети. Изоляция виртуальных сетей друг от друга происходит на канальном уровне. Это означает, что передача кадров между различными виртуальными сетями на основании адреса канального уровня невозможна.

Конечно, построить несколько изолированных друг от друга сетей можно, использовав нескольких коммутаторов, но использование одного коммутатора не только снижает стоимость таких сетей, но и позволяет более гибко и рационально использовать порты коммутатора. К примеру, одна локальная сеть может быть построена из двух сегментов, подключенных к двум портам коммутатора, а другая сеть может состоять из пяти сегментов, для чего потребуется пять портов коммутатора. При использовании для этих сетей двух различных коммутаторов несколько портов останутся неиспользованными.

Поскольку узлы различных виртуальных сетей изолированы друг от друга на канальном уровне, для объединения таких сетей в единую сеть требуется привлечение сетевого, или 3-го уровня. Понятие 3-го уровня соответствует градации уровней сетевой модели OSI. Для обеспечения таких связей могут быть использованы маршрутизаторы либо коммутаторы, обеспечивающие функции маршрутизатора. Такие коммутаторы получили название коммутаторов 3-го уровня. По аналогии коммутаторы, работающие только на канальном уровне, иногда называются коммутаторами 2-го уровня.

Шлюз (gateway) является наиболее сложной ретрансляционной системой, обеспечивающей взаимодействие сетей с различными наборами протоколов всех семи уровней. В свою очередь, наборы протоколов могут опираться на различные типы физических средств соединения.

Шлюзы оперируют на верхних уровнях модели OSI (сеансовом, представительском и прикладном) и представляют наиболее развитый метод подсоединения сетевых сегментов и компьютерных сетей. Необходимость в сетевых шлюзах возникает при объединении двух систем, имеющих различную архитектуру. Например, шлюз приходится использовать для соединения сети с протоколом TCP/IP и большой ЭВМ со стандартом SNA. Эти две

архитектуры не имеют ничего общего, и потому требуется полностью переводить весь поток данных, проходящих между двумя системами.

В качестве шлюза обычно выступает выделенный компьютер, на котором запущено программное обеспечение шлюза и производятся преобразования, позволяющие взаимодействовать несходным системам в сети. Например, при использовании шлюза персональные компьютеры на базе Intel-совместимых процессоров на одном сегменте могут связываться и разделять ресурсы с компьютерами Macintosh.

Другой функцией шлюзов является преобразование протоколов. Шлюз может получить сообщение IPX/SPX, направленное клиенту, использующему другой протокол, например TCP/IP, на удаленном сетевом сегменте. После того как шлюз определяет, что получателем сообщения является станция TCP/IP, он действительно преобразует данные сообщения в протокол TCP/IP. (В этом состоит отличие от моста, который просто пересылает сообщение, используя один протокол внутри формата данных другого протокола, — преобразование при необходимости происходит у получателя.) Почтовые шлюзы производят сходные операции по преобразованию почтовых сообщений и других почтовых передач из формата приложения электронной почты в более универсальный почтовый протокол, например SMTP, который может быть затем использован для направления сообщения в Internet.

Хотя шлюзы имеют много преимуществ, нужно учитывать несколько факторов, которые должны учитываться при принятии решения об использовании шлюзов в сети. Шлюзы сложны в установке и настройке. Они также дороже других коммуникационных устройств. Вследствие лишнего этапа обработки, связанного с процессом преобразования, шлюзы работают медленнее, чем маршрутизаторы и подобные устройства.

Контрольные вопросы

1. Дайте определение сети.
2. В чем сходство и различие между локальными и глобальными телекоммуникационными сетями?
3. Сформулируйте достоинства и недостатки одноранговых сетей.
4. Сформулируйте достоинства и недостатки сетей с выделенным сервером.

5. Охарактеризуйте сетевую модель OSI.
6. Какие способы коммутации вы знаете? Охарактеризуйте их.
7. Какие топологии сетей вы знаете? Охарактеризуйте их.
8. Какие основные сетевые устройства вы знаете? Охарактеризуйте их.
9. Охарактеризуйте назначение сетевых карт (адаптеров).
10. Охарактеризуйте назначение и случаи применения повторителей и усилителей.
11. В чем назначение концентраторов? Приведите случаи применения концентраторов.
12. Охарактеризуйте назначение и случаи применения мостов.
13. В чем назначение маршрутизаторов? Приведите случаи применения маршрутизаторов.
14. Охарактеризуйте назначение и случаи применения шлюзов.
15. Сформулируйте достоинства и недостатки беспроводных сетевых технологий.

Глава 2
ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ И КАЧЕСТВО КОМПЬЮТЕРНЫХ СЕТЕЙ И ТЕЛЕКОММУНИКАЦИОННЫХ КАНАЛОВ

2.1. Показатели качества информационно-вычислительных сетей

Согласно Серии Международных Стандартов ISO 9000, **качество** — это совокупность свойств системы, позволяющих удовлетворять потребностям и ожиданиям потребителя. Рассмотрим основные показатели качества информационно-вычислительных сетей.

1. **Полнота выполняемых функций**. Сеть должна обеспечивать выполнение всех предусмотренных для нее функций по доступу ко всем ресурсам, по совместной работе узлов и по реализации всех протоколов и стандартов работы.

2. **Производительность** — среднее количество запросов пользователей сети, исполняемых за единицу времени.

3. **Пропускная способность** — важная характеристика производительности сети, определяется объемом данных, передаваемых через сеть (или ее звено — сегмент) за единицу времени.

4. **Надежность** сети — важная ее техническая характеристика, чаще всего характеризующаяся средним временем наработки на отказ.

5. **Достоверность** информации — важная потребительская характеристика сети.

6. **Безопасность информации** в сети является важнейшим ее параметром, поскольку современные сети имеют дело с конфиденциальной информацией. Способность сети защитить инфор-

мацию от несанкционированного доступа и определяет степень ее безопасности.

7. **Прозрачность сети** — еще одна ее потребительская характеристика, означающая невидимость особенностей внутренней архитектуры сети для пользователя, он должен иметь возможность обращаться к ресурсам сети как к локальным ресурсам своего собственного компьютера.

8. **Масштабируемость** — это возможность расширения сети без заметного снижения ее производительности.

9. **Универсальность сети** — возможность подключения к ней разнообразного технического оборудования программного обеспечения от разных производителей.

В состав этих показателей качества сети входят важные технические характеристики, которые могут быть оценены и выражены количественными значениями измеряемых или вычисляемых величин, — производительность, пропускная способность, надежность, достоверность результатной информации, безопасность информации.

Производительность ИВС, иначе называемая **вычислительной мощностью**, определяется тремя характеристиками:

- **временем реакции** сети на запрос пользователя;
- **пропускной способностью** сети;
- **задержкой передачи**.

Время реакции системы определяется как интервал времени между возникновением запроса пользователя (ЗП) к какой-либо сетевой службе и получением ответа на этот запрос и складывается из следующих составляющих:

- времени подготовки запроса на компьютере пользователя;
- времени передачи запроса через сегменты сети и промежуточное телекоммуникационное оборудование от пользователя к узлу сети, ответственному за его исполнение;
- времени выполнения (обработки) запроса в этом узле;
- времени передачи пользователю ответа на запрос;
- времени обработки полученного от сервера ответа на компьютере пользователя.

Значение времени реакции зависит от типа службы, к которой обращается пользователь, от того, какой пользователь и к какому узлу обращается, а также от состояния элементов сети на данный момент, а именно от загруженности сервера и сегментов, коммутаторов и маршрутизаторов, через которые проходит запрос, и др. Поэтому на практике используется оценка времени

реакции сети, усредненная по пользователям, серверам, времени дня, от которого зависит загрузка сети. Эти сетевые составляющие времени реакции дают возможность оценить производительность отдельных элементов сети и выявить «узкие» места с целью модернизации сети для повышения общей производительности.

Значительную часть времени реакции составляет **время передачи** информации по телекоммуникациям сети, от длительности которого и зависит величина пропускной способности. Пропускная способность определяет скорость выполнения внутренних операций сети по передаче пакетов данных между узлами сети через коммутационные устройства и характеризует качество выполнения одной из основных функций сети — транспортировки сообщений. По этой причине при анализе производительности сети эта характеристика чаще используется, чем время реакции.

Пропускная способность, называемая в некоторых литературных источниках **скоростью передачи данных**, измеряется в Бодах (названа в честь французского ученого Э. Бодо), равных 1 бит/с, либо в пакетах в секунду и характеризует эффективность передачи данных.

Например, скорость передачи данных по кабельным линиям связи ЛВС от 10 Мбит/с, по телефонным каналам связи глобальных сетей — всего 1200 бит/с.

Используются три понятия пропускной способности — средняя, мгновенная и максимальная. **Средняя пропускная способность** вычисляется делением объема переданных данных на время их передачи за длительный интервал времени (час, день, неделя). **Мгновенная пропускная способность** — средняя пропускная способность за очень маленький интервал: 10 мс или 1 с. **Максимальная пропускная способность** — это наибольшая мгновенная пропускная способность, зафиксированная за время наблюдения.

Пропускная способность может измеряться между двумя узлами или точками сети, например, между компьютером пользователя и сервером, между входным и выходным портами маршрутизатора. Общая пропускная способность любого составного пути сети будет равна **минимальной** из пропускных способностей составляющих элементов маршрута, поскольку пакеты передаются различными элементами сети последовательно. **Общая пропускная способность сети** характеризует качество сети в целом и определяется как среднее количество информации, переданной между всеми узлами сети в единицу времени.

Задержка передачи — это задержка между моментом поступления пакета на вход какого-нибудь сетевого устройства или части сети и моментом появления его на выходе этого устройства. Эта характеристика производительности отличается от времени реакции сети тем, что включает в себя только время этапов сетевой обработки данных, без учета задержек обработки данных компьютерами сети. Практически величина задержки не превышает сотен миллисекунд, реже нескольких секунд и не влияет на качество файловой службы, служб электронной почты и печати с точки зрения пользователя. Однако такие задержки пакетов, переносящих изображение или речь, приводят к снижению качества предоставляемой пользователю информации из-за возникновения дрожания изображения, эффекта «эха», неразборчивости слов и т. п.

Задержка передачи и пропускная способность являются независимыми характеристиками, поэтому, не смотря на высокую пропускную способность, сеть может вносить значительные задержки при передаче каждого пакета.

2.2. Типы каналов связи

Данные, изначально имеющие **аналоговую**, непрерывную форму, такие как речь, фото и телевизионные изображения, телеметрическая информация, в последнее время все чаще передаются по каналам связи в дискретном виде, т. е. в виде последовательности «нулей» и «единиц». Для преобразования непрерывного сигнала в дискретную форму производится **дискретная модуляция**, называемая также **кодированием**.

Применяются два типа кодирования данных. Первый — на основе непрерывного синусоидального несущего сигнала — называется **аналоговой модуляцией**, или просто модуляцией. Кодирование осуществляется за счет изменения параметров аналогового сигнала. Второй тип кодирования называется **цифровым кодированием** и осуществляется на основе последовательности прямоугольных импульсов. Эти способы кодирования различаются шириной спектра передаваемого сигнала и сложностью аппаратуры для их реализации.

В зависимости от типа промежуточной аппаратуры все линии связи делятся на аналоговые и цифровые. Промежуточная

аппаратура используется на линиях большой протяженности и решает две задачи — улучшение качества сигнала и создание составного канала связи между двумя абонентами. В **аналоговых** линиях промежуточная аппаратура предназначена для усиления аналоговых сигналов, т. е. сигналов, которые имеют непрерывный диапазон значений. Такие линии традиционно применялись в телефонных сетях с узкой полосой частот, представителем которых является канал **тональной частоты**. Аналоговые линии используются для связи между собой телефонных станций, для создания высоскоростных каналов, которые мультиплексируют несколько низкоскоростных аналоговых абонентских каналов. При аналоговом подходе для уплотнения низкоскоростных каналов абонентов в общий высокоскоростной канал обычно используется техника **разделения частот** или частотного мультиплексирования — FDM (Frequency Division Multiplexing). FDM — разбиение средств передачи на два и более каналов путем разделения полосы частот канала на узкие «подполосы», образующие каждая отдельный канал в одной и той же физической среде.

Современные телекоммуникационные системы и сети явились синтезом развития двух исходно независимых сетей — сетей электросвязи (телефонной, телеграфной, телетайпной и радиосвязи) и вычислительных сетей. Логика развития систем связи требовала применения цифровых систем передачи данных, а также применения вычислительных средств для решения задач маршрутизации, управления трафиком, сигнализации; в свою очередь, логика развития вычислительной техники требовала все большего применения средств связи между периферийными устройствами и отдельными ЭВМ. Достигнутое в результате этих двух встречных движений совмещение техники связи с вычислительной техникой позволило усовершенствовать технологию обслуживания телефонной клиентуры и повысить эффективность отрасли связи, а также полнее использовать ресурсы вычислительных центров, вычислительных систем и сетей путем перераспределения их ресурсов и распараллеливания между ними задач и информационных потоков.

Многие сети общего пользования традиционных операторов являются в основном аналоговыми. Сети связи, создаваемые новыми операторами — цифровые, что обеспечивает внедрение современных служб и гарантирует перспективность этих сетей. В то же время существующие аналоговые сети активно используются для передачи информации как в аналоговой форме (телефония,

радиотелефония, радиовещание и телевидение), так и для передачи дискретных (цифровых) данных. Носителем информации в телекоммуникационных каналах являются электрические сигналы (непрерывные, называемые аналоговыми, и дискретные или цифровые) и электромагнитные колебания — волны.

Линия связи (ЛС) — это физическая среда, по которой передаются информационные сигналы. В одной линии связи может быть организовано несколько **каналов связи** (КС) путем временного, частотного, кодового и других видов разделения, тогда говорят о **логических (виртуальных)** каналах. Когда канал монополизирует линию связи, то он может называться физическим каналом и в этом случае совпадает с линией связи. Канал связи может быть аналоговым или цифровым; в линии, как в физической среде, могут быть образованы каналы связи разного типа.

2.3. Типы цифровых каналов

Для передачи по цифровым каналам аналогового сообщения в виде непрерывной последовательности (телеметрические, метеорологические данные, данные систем контроля и управления) она предварительно оцифровывается. Частота оцифровки обычно равна порядка 8 кГц, через каждые 125 мкс значение величины аналогового сигнала отображается 8-разрядным двоичным кодом. Таким образом, скорость передачи данных составляет 64 кбит/с. Объединение нескольких таких базовых цифровых каналов в один (**мультиплексирование**) позволяет создавать более скоростные каналы: простейший мультиплексированный канал обеспечивает скорость передачи 128 кбит/с, более сложные каналы, например, мультиплексирующие 32 базовых канала, обеспечивают пропускную способность 2048 Мбит/с. С помощью цифровых каналов подключаются к магистралям также и офисные цифровые АТС.

Цифровые абонентские каналы в режиме коммутации каналов используются в наиболее распространенной цифровой сети с интеграцией услуг ISDN (Integrated Services Digital Network). По популярности сеть ISDN уступает лишь аналоговой телефонной сети. Адресация в ISDN организована так же, как и в телефонной сети, так как сеть создавалась для объединения существующих телефонных сетей с появляющимися сетями передачи

данных. Поэтому сети ISDN позволяют объединять разнообразные виды связи (видео-, аудиопередачу данных, тексты, компьютерные данные и т. п.) со скоростями 64 кбит/с, 128 кбит/с, 2 Мбит/с и 155 Мбит/с на широкополосных каналах связи.

Заметим, что названием «ISDN» принято именовать и сеть, использующую технологию ISDN, и протокол, применяющий эту технологию.

Активно развиваются и другие типы цифровых систем, из которых следует отметить модификации технологии цифровых абонентских линий DSL (Digital Subscriber Line). HDSL (High Bit Rate DSL) — высокоскоростной вариант абонентской линии ISDN.

Конкуренцию ISDN и HDSL могут составить цифровые магистрали с синхронно-цифровой иерархией SDN (Synchronous Digital Hierarchy). В системе SDN имеется иерархия скоростей передачи данных. В магистралях SDN применяются оптоволоконные линии связи и частично радиолинии.

2.4. Цифровое кодирование дискретной информации

В цифровых линиях связи передаваемые сигналы в форме прямоугольных импульсов имеют конечное число состояний, обычно 2, 3, иногда 4. Такими сигналами передаются компьютерные данные и оцифрованная речь и изображения. За один такт работы передающей аппаратуры передается один элементарный сигнал — 1 бит. Промежуточная аппаратура улучшает форму импульсов и восстанавливает длительность периода их следования. Она также осуществляет уплотнение низкоскоростных каналов абонентов в общий высокоскоростной канал, работая по принципу их разделения во времени так называемого **временного мультиплексирования** каналов TDM (от Time Division Multiplexing), когда каждому низкоскоростному каналу выделяется определенная доля времени (квант или **тайм-слот**) высокоскоростного канала.

Рисунок 2.1 иллюстрирует способ кодирования, называемый **полярным кодированием**: положительное напряжение — логический «0», отрицательное — логическая «1». Этот метод прост и логичен, но имеет существенный недостаток — необходимость синхронизации. Когда двоичный код включает две или более

следующие друг за другом единицы (или нулей), то на протяжении двух и более бит не происходит изменения напряжения. При обмене информацией двух вычислительных систем, не имеющих синхронизированных с большой точностью таймеров, невозможно правильно определить количество переданных бит. Поэтому полярное кодирование применяется в ВС со сверхскоростной передачей информации и сопутствующим внешним синхросигналом, синхронизирующим взаимодействующие ВС.

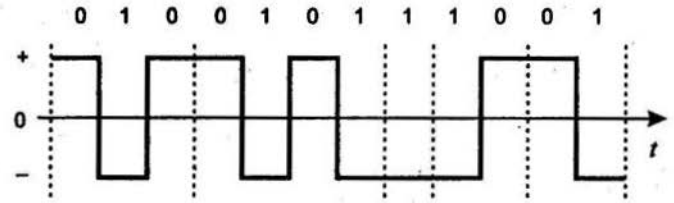

Рис. 2.1. Полярный код

Поскольку большинство информационных сетей использует узкополосную среду передачи, которая разрешает единовременную посылку только одного сигнала, то такие сети используют способ кодирования, имеющий свойство **самосинхронизации** (self-timing). Один из видов самосинхронизирующихся кодов — ***манчестерский код***, применяемый в сетях Ethernet: уровень сигнала изменяется по центру каждого бита, что позволяет принимающей ВС точно отметить границы бита (рис. 2.2). Логические 0 и 1 определяются, исходя из направления изменения полярности: нулю соответствует переход от положительного значения к отрицательному, единице — от отрицательного к положительному.

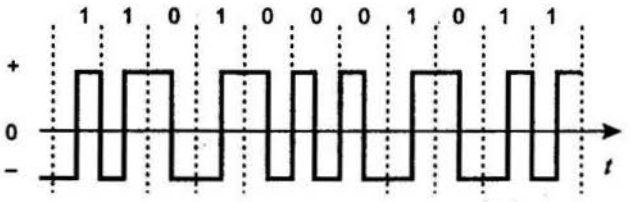

Рис. 2.2. Манчестерский код

В сетях Token Ring применяется **разностное манчестерское кодирование**: уровень сигнала изменяется также по центру бита, но направление перехода не имеет значения, его наличие требуется только для синхронизации сигнала (рис. 2.3). Значение же

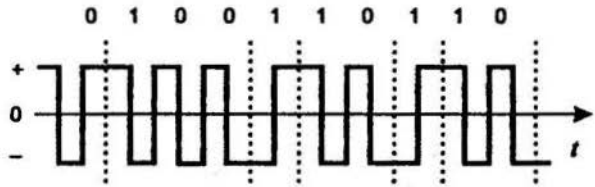

Рис. 2.3. Разностный манчестерский код

логического сигнала определяется по наличию или отсутствию перехода в начале следования бита: нулю соответствует смена полярности, единице — отсутствие смены. Смена полярности в середине бита во внимание не принимается.

По сравнению с манчестерским и разностным манчестерским кодированием более эффективно кодирование **без возврата к нулю** — NRZ (Non-Return to Zero) за счет простоты в реализации и большей помехозащищенности (рис. 2.4). Преимуществом этого кода является то, что основная гармоника спектра сигналов достаточно низка и равна $N/2$ (N — скорость передачи дискретных данных, бит/с). У сигналов, закодированных по другим методам, например, манчестерским, основная гармоника имеет более низкую частоту. Недостатком является отсутствие самосинхронизации, поэтому при высоких скоростях обмена код NRZ не применяется. Другой недостаток кода NRZ проявляется при передаче длинных последовательностей 1 и 0, тогда низкочастотная составляющая приближается к нулю, поэтому в каналах, где нет непосредственного гальванического соединения между источником и приемником информации, этот код не применяется. Однако разработаны модификации метода NRZ-кодирования, устраняющие два указанных недостатка.

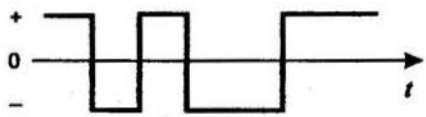

Рис. 2.4. Потенциальный код NRZ

Контрольные вопросы

1. Какими характеристиками определяется производительность ИВС?
2. Из каких составляющих состоит время реакции на запрос в вычислительной сети?
3. В каких единицах измеряется пропускная способность ИВС?

4. Чем различаются средняя, максимальная и мгновенная пропускные способности сети?
5. Чем отличается задержка передачи информации в сети от времени реакции сети?
6. Назовите причины перехода от аналоговых каналов к цифровым.
7. Поясните, как проводится оцифровка дискретизированного непрерывного сигнала и из каких соображений выбирается частота дискретизации непрерывной временной последовательности.
8. Назовите, чем отличается цифровое кодирование информации от аналоговой модуляции.
9. Назовите преимущества цифровых методов связи по сравнению с методами аналоговой модуляции.

Глава 3
ЛИНИИ СВЯЗИ СЕТЕЙ ЭВМ

3.1. Типы линий связи

Линия связи состоит в общем случае из физической среды, по которой передаются электрические информационные сигналы, аппаратуры передачи данных и промежуточной аппаратуры (рис. 3.1).

Рис. 3.1. Канал связи

Физическая среда передачи данных может представлять собой кабель, т. е. набор проводов, изоляционных и защитных оболочек и соединительных разъемов, а также земную атмосферу или космическое пространство, через которые распространяются электромагнитные волны.

В зависимости от среды передачи данных линии связи разделяются на следующие:

- проводные (воздушные);
- кабельные (медные и волоконно-оптические);
- радиоканалы наземной и спутниковой связи.

Проводные (воздушные) линии связи представляют собой провода без каких-либо изолирующих или экранирующих оплеток, проложенные между столбами и висящие в воздухе. По таким линиям связи традиционно передаются телефонные или телеграфные сигналы, но при отсутствии других возможностей эти линии используются и для передачи компьютерных данных. Скоростные качества и помехозащищенность этих линий оставляют желать много лучшего. Сегодня проводные линии связи быстро вытесняются кабельными.

Кабельные линии состоят из проводников, заключенных в несколько слоев изоляции: электрической, электромагнитной, механической. Кроме того, кабель может быть оснащен разъемами, позволяющими быстро выполнять присоединение к нему различного оборудования. В компьютерных сетях применяются три основных типа кабеля: кабели на основе скрученных пар медных проводов, коаксиальные кабели с медной жилой, а также волоконно-оптические кабели.

Скрученная пара проводов называется **витой парой**. Витая пара существует в экранированном варианте, когда пара медных проводов обертывается в изоляционный экран, и неэкранированном, когда изоляционная обертка отсутствует. Скручивание проводов снижает влияние внешних помех на полезные сигналы, передаваемые по кабелю.

Коаксиальный кабель имеет несимметричную конструкцию и состоит из внутренней медной жилы и оплетки, отделенной от жилы слоем изоляции. Существует несколько типов коаксиального кабеля, отличающихся характеристиками и областями применения — для локальных сетей, для глобальных сетей, для кабельного телевидения и т. п.

Волоконно-оптический кабель состоит из тонких (5—60 микрон) волокон, по которым распространяются световые сигналы. Это наиболее качественный тип кабеля — он обеспечивает передачу данных с очень высокой скоростью (до 10 Гбит/с и выше) и к тому же лучше других типов передающей среды обеспечивает защиту данных от внешних помех.

Радиоканалы наземной и спутниковой связи образуются с помощью передатчика и приемника радиоволн. Существует большое количество различных типов радиоканалов, отличающихся как используемым частотным диапазоном, так и дальностью канала. Диапазоны коротких, средних и длинных волн (КВ, СВ и ДВ), называемые также диапазонами амплитудной модуляции (Amplitude

Modulation — AM) по типу используемого в них метода модуляции сигнала, обеспечивают дальнюю связь, но при невысокой скорости передачи данных. Более скоростными являются каналы, работающие на диапазонах ультракоротких волн (УКВ), для которых характерна частотная модуляция (Frequency Modulation — FM), а также диапазонах сверхвысоких частот (СВЧ или microwaves). В диапазоне СВЧ (свыше 4 ГГц) сигналы уже не отражаются ионосферой Земли, и для устойчивой связи требуется наличие прямой видимости между передатчиком и приемником. Поэтому такие частоты используют либо спутниковые каналы, либо радиорелейные каналы, где это условие выполняется.

В компьютерных сетях сегодня применяются практически все описанные типы физических сред передачи данных, но наиболее перспективными являются волоконно-оптические. На них сегодня строятся как магистрали крупных территориальных сетей, так и высокоскоростные линии связи локальных сетей. Популярной средой является также витая пара, которая характеризуется отличным соотношением качества к стоимости, а также простотой монтажа. С помощью витой пары обычно подключают конечных абонентов сетей на расстояниях до 100 метров от концентратора. Спутниковые каналы и радиосвязь используются чаще всего в тех случаях, когда кабельные связи применить нельзя — например, при прохождении канала через малонаселенную местность или же для связи с мобильным пользователем сети.

3.2. Характеристики линий связи

К основным характеристикам линий связи относятся:

- амплитудно-частотная характеристика;
- полоса пропускания;
- затухание;
- помехоустойчивость;
- перекрестные наводки на ближнем конце линии;
- пропускная способность;
- достоверность передачи данных;
- удельная стоимость.

В первую очередь разработчика вычислительной сети интересуют пропускная способность и достоверность передачи дан-

ных, поскольку эти характеристики прямо влияют на производительность и надежность создаваемой сети.

Амплитудно-частотная характеристика (рис. 3.2) показывает, как затухает амплитуда синусоиды на выходе линии связи по сравнению с амплитудой на ее входе для всех возможных частот передаваемого сигнала.

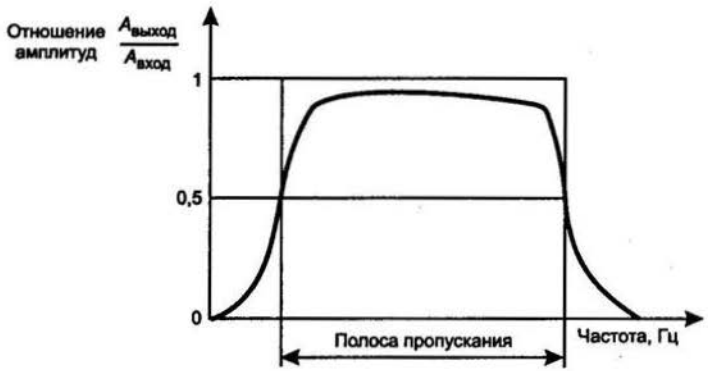

Рис. 3.2. Амплитудно-частотная характеристика

Знание амплитудно-частотной характеристики реальной линии позволяет определить форму выходного сигнала практически для любого входного сигнала. Для этого необходимо найти спектр входного сигнала, преобразовать амплитуду составляющих его гармоник в соответствии с амплитудно-частотной характеристикой, а затем найти форму выходного сигнала, сложив преобразованные гармоники.

На практике вместо амплитудно-частотной характеристики применяются другие, упрощенные характеристики, например, полоса пропускания и затухание.

Полоса пропускания (bandwidth) — это непрерывный диапазон частот, для которого отношение амплитуды выходного сигнала к входному превышает некоторый заранее заданный предел, обычно 0,5 (см. рис. 3.2). То есть полоса пропускания определяет диапазон частот синусоидального сигнала, при которых этот сигнал передается по линии связи без значительных искажений.

Затухание (attenuation) определяется как относительное уменьшение амплитуды или мощности сигнала при передаче по линии сигнала определенной частоты. Таким образом, затухание

представляет собой одну точку из амплитудно-частотной характеристики линии.

Затухание A обычно измеряется в децибелах (дБ, decibel — dB) и вычисляется по следующей формуле:

$$A = 10 \log_{10} P_{вых}/P_{вх},$$

где $P_{вых}$ — мощность сигнала на выходе линии; $P_{вх}$ — мощность сигнала на входе линии.

Так как мощность выходного сигнала кабеля без промежуточных усилителей всегда меньше, чем мощность входного сигнала, затухание кабеля всегда является отрицательной величиной.

Полоса пропускания зависит от типа линии и ее протяженности.

Пропускная способность (throughput) линии характеризует максимально возможную скорость передачи данных по линии связи.

Связь между полосой пропускания линии и ее максимально возможной пропускной способностью выражается формулой Шеннона

$$C = F \log_2(1 + P_c/P_ш),$$

где C — максимальная пропускная способность линии в битах в секунду; F — ширина полосы пропускания линии в герцах; P_c — мощность сигнала; $P_ш$ — мощность шума.

Помехоустойчивость линии определяет ее способность уменьшать уровень помех, создаваемых во внешней среде, на внутренних проводниках. Помехоустойчивость линии зависит от типа используемой физической среды, а также от экранирующих и подавляющих помехи средств самой линии. Наименее помехоустойчивыми являются радиолинии, хорошей устойчивостью обладают кабельные линии и отличной — волоконно-оптические линии, малочувствительные к внешнему электромагнитному излучению. Обычно для уменьшения помех, появляющихся из-за внешних электромагнитных полей, проводники экранируют и/или скручивают.

Перекрестные наводки на ближнем конце (Near End Cross Talk — NEXT) определяют помехоустойчивость кабеля к внутренним источникам помех, когда электромагнитное поле сигнала, передаваемого выходом передатчика по одной паре провод-

ников, наводит на другую пару проводников сигнал помехи. Если ко второй паре будет подключен приемник, то он может принять наведенную внутреннюю помеху за полезный сигнал. Показатель перекрестных наводок NEXT, выраженный в децибелах, представляется формулой

$$NEXT=10 \log P_{вых}/P_{нав},$$

где $P_{вых}$ — мощность выходного сигнала; $P_{нав}$ — мощность наведенного сигнала.

Достоверность передачи данных характеризует вероятность искажения для каждого передаваемого бита данных. Величина этого показателя для каналов связи без дополнительных средств защиты от ошибок (например, самокорректирующихся кодов или протоколов с повторной передачей искаженных кадров) составляет, как правило, 10^{-4}—10^{-6}, в оптоволоконных линиях связи — 10^{-9}. Значение достоверности передачи данных, например, в 10^{-4} говорит о том, что в среднем из 10 000 бит искажается значение одного бита.

Искажения бит происходят как из-за наличия помех на линии, так и по причине искажений формы сигнала ограниченной полосой пропускания линии. Поэтому для повышения достоверности передаваемых данных нужно повышать степень помехозащищенности линии, снижать уровень перекрестных наводок в кабеле, а также использовать более широкополосные линии связи.

3.3. Стандарты кабелей

В компьютерных сетях применяются кабели, удовлетворяющие определенным стандартам, что позволяет строить кабельную систему сети из кабелей и соединительных устройств разных производителей.

Кабели на основе неэкранированной витой пары (Unshielded Twisted Pair — UTP)

Стандартом определено пять категорий UTP. Все кабели UTP независимо от их категории выпускаются в 4-парном исполнении. Каждая из четырех пар кабеля имеет определенный цвет и шаг скрутки (рис. 3.3). Обычно две пары предназначены для передачи данных, а две — для передачи голоса.

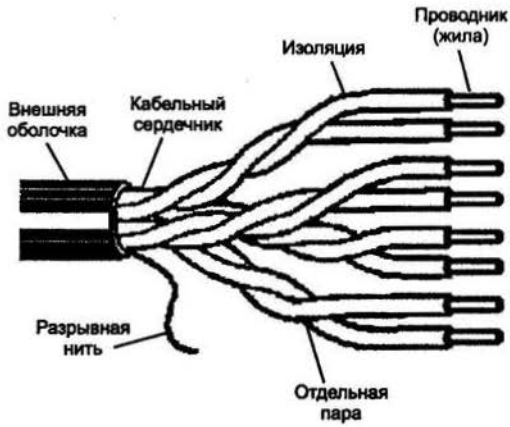

Рис. 3.3. Кабель «витая пара»

Таблица 3.1. **Категории кабелей на основе неэкранированной витой пары**

Категория	Характеристики
1	Телефонный кабель для передачи аналоговых сигналов
2	Кабель из 4 витых пар, способный передавать данные со скоростью 4 Мбит/с
3	Кабель из 4 витых пар, способный передавать данные со скоростью 10 Мбит/с
4	Кабель из 4 витых пар, способный передавать данные со скоростью 16 Мбит/с
5	Кабель из 4 витых пар, способный передавать данные со скоростью 100 Мбит/с
6	Кабель из 4 витых пар, способный передавать данные со скоростью 1 Гбит/с

Наиболее важные электромагнитные характеристики кабеля категории 5 имеют следующие значения:

- полное волновое сопротивление в диапазоне частот до 100 МГц равно 100 Ом (стандарт ISO 11801 допускает также кабель с волновым сопротивлением 120 Ом, волновое сопротивление — сопротивление переменному току);
- величина перекрестных наводок NEXT в зависимости от частоты сигнала должна принимать значения не менее 74 дБ на частоте 150 кГц и не менее 32 дБ на частоте 100 МГц;

- затухание имеет предельные значения от 0,8 дБ (на частоте 64 кГц) до 22 дБ (на частоте 100 МГц);
- активное сопротивление не должно превышать 9,4 Ом на 100 м;
- емкость кабеля не должна превышать 5,6 нФ на 100 м.

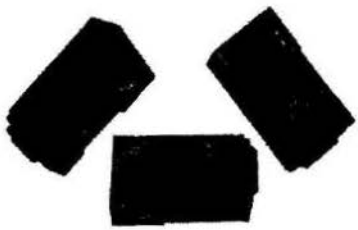

Рис. 3.4. Разъемы RJ-45

Для соединения кабелей с оборудованием используются вилки и розетки RJ-45, представляющие 8-контактные разъемы, похожие на обычные телефонные разъемы RJ-11 (рис. 3.4).

Кабели на основе экранированной витой пары (Shielded Twisted Pair — STP)

Экранированная витая пара STP хорошо защищает передаваемые сигналы от внешних помех, а также меньше излучает электромагнитных колебаний вовне, что защищает, в свою очередь, пользователей сетей от вредного для здоровья излучения. Наличие заземляемого экрана удорожает кабель и усложняет его прокладку, так как требует выполнения качественного заземления. Экранированный кабель применяется только для передачи данных, голос по нему не передают.

Основным стандартом, определяющим параметры экранированной витой пары, является фирменный стандарт IBM. В этом стандарте кабели делятся не на категории, а на типы: Type 1, Type 2, ..., Type 9.

Основным типом экранированного кабеля является кабель Type 1 стандарта IBM. Он состоит из 2-х пар скрученных проводов, экранированных проводящей оплеткой, которая заземляется. Электрические параметры кабеля Type 1 примерно соответствуют параметрам кабеля UTP категории 5, однако волновое сопротивление кабеля Type 1 равно 150 Ом.

Для присоединения экранированных кабелей к оборудованию используются разъемы конструкции IBM.

Коаксиальные кабели

Существует большое количество типов коаксиальных кабелей, используемых в сетях различного типа — телефонных, телевизионных и компьютерных.

Для организации компьютерных сетей используются два типа коаксиальных кабелей (рис. 3.5):

- тонкий коаксиальный кабель;
- толстый коаксиальный кабель.

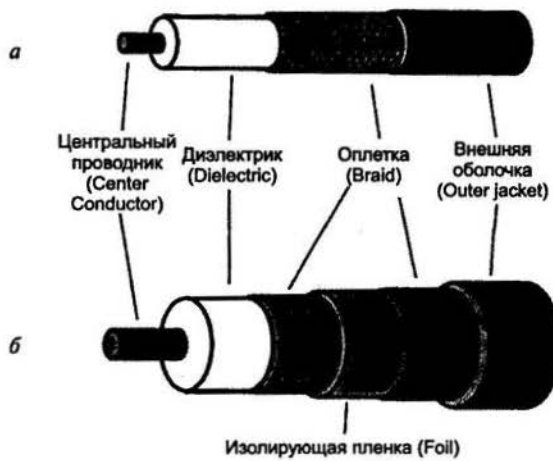

Рис. 3.5. Коаксиальные кабели:
а — тонкий; *б* — толстый

Тонкий коаксиальный кабель (табл. 3.2) — гибкий кабель диаметром примерно 0,5 см. Он способен передавать сигнал на расстояние до 185 м без его заметного искажения, вызванного затуханием. Волновое сопротивление кабеля составляет 50 Ом.

Таблица 3.2. **Таблица кодировки тонких коаксиальных кабелей**

Кабель	Характеристики кабеля
RG58 /U	Сплошная медная жила
RG58 A/U	Переплетенные провода
RG58 C/U	Военный стандарт для RG58 A/U
PK50	Отечественный аналог

Для подключения кабеля используются специальные разъемы типа BNC (Bayonet Naval Connector) (рис. 3.6).

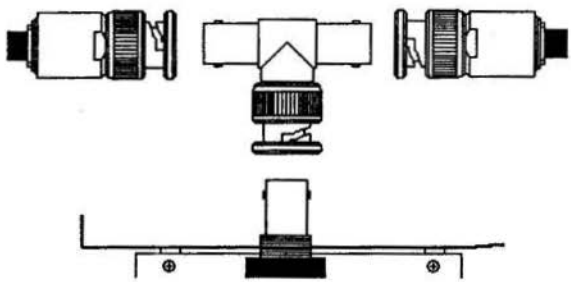

Рис. 3.6. Разъемы BNC

Кабель RG58 позволяет реализовать топологии шина и кольцо и был до последнего времени самым распространенным при построении сетей.

Толстый коаксиальный кабель — относительно жесткий кабель диаметром около 1 см. Медная жила кабеля толще, чем у тонкого коаксиального кабеля и, следовательно, сопротивление меньше. Поэтому толстый коаксиальный кабель передает сигналы дальше, чем тонкий, до 500 м.

Для подключения к толстому коаксиальному кабелю применяют специальное устройство — трансивер. Трансивер снабжен специальным коннектором, который «прокусывает» изоляционный слой и осуществляет контакт с проводящей жилой.

Волоконно-оптические кабели

Волоконно-оптические линии предназначены для перемещения больших объемов данных на высоких скоростях. Оптоволоконный кабель состоит из центрального стеклянного или пластикового проводника, окруженного другим слоем стеклянного или пластикового покрытия, и внешней защитной оболочки (рис. 3.7).

Данные передаются по кабелю с помощью лазерного (laser transmitter) или светодиодного (LED, light-emitting diode transmitter) передатчика, который посылает однонаправленные световые импульсы через центральное стеклянное волокно. Стеклянное покрытие помогает поддерживать фокусировку света во внутреннем проводнике. Сигнал принимается на другом конце фотодиодным приемником (photodiode receiver), преобразующим

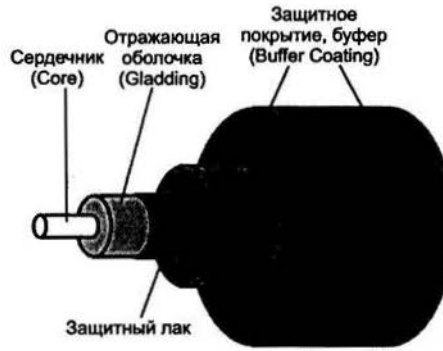

Рис. 3.7. Конструкция оптоволоконного кабеля

световые импульсы в электрический сигнал, который сможет использовать получающий компьютер.

Конструкций световодов и оптических волокон очень много, но основных типов два:

- многомодовый;
- одномодовый.

Диаметр сердцевины у многомодовых волокон в десятки раз превышает длину волны передаваемого излучения, из-за чего по волокну распространяется несколько типов волн (мод). Стандартные диаметры сердцевины многомодовых волокон — 50 и 62,5 мкм.

У одномодового волокна диаметр сердцевины находится обычно в пределах 5—10 мкм. Диаметр кварцевой оболочки световода тоже стандартизован и составляет 125 мкм.

Скорость передачи данных для оптоволоконных сетей находится в диапазоне от 100 Мбит/с до 2 Гбит/с, а данные могут быть надежно переданы на расстояние до 2 километров без повторителя. Оптоволоконный кабель может поддерживать передачу видео и голосовой информации так же, как и передачу данных. Поскольку световые импульсы полностью закрыты в пределах внешней оболочки, оптоволоконный носитель фактически невосприимчив к внешней интерференции и подслушиванию. Эти качества делают оптоволоконный кабель привлекательным выбором для защищенных сетей или сетей, которые требуют очень быстрой передачи на большие расстояния.

Поскольку световые импульсы могут двигаться только в одном направлении, системы на базе оптоволоконных кабелей

должны иметь входящий кабель и исходящий кабель для каждого сегмента, который будет посылать и получать данные. Волоконный кабель также жёсток и сложен в установке, что делает его самым дорогим типом сетевого носителя. Волоконный носитель требует специальных соединителей — коннекторов и высококвалифицированной установки. Эти факторы в дальнейшем приведут к высокой стоимости внедрения. Одним способом снижения расходов является ограничение использования волоконного кабеля сетевыми магистралями или теми областями, где имеет значение влияние электромагнитного наложения, возгораемость или другие вопросы окружения.

При проектировании или расширении сетей нужно принимать во внимание факторы, перечисленные в табл. 3.3.

Таблица 3.3. **Сравнительные характеристики кабелей**

Тип кабеля	Скорость передачи, Мбит/с	Длина передачи, м	Простота установки	Подверженность помехам	Стоимость
Неэкранированная витая пара	100	100	Прост в установке	Подвержен помехам	Самый дешевый
Тонкий коаксиальный	10	185	Прост в установке	Хорошая защита от помех	Дороже витой пары
Толстый коаксиальный	10	500	Прост в установке	Хорошая защита от помех	Дороже тонкого коаксиального кабеля
Оптоволоконный	100—2000	2000	Труден в установке	Не подвержен помехам	Самый дорогой

3.4. Беспроводные каналы связи

В дополнение к традиционным физическим носителям методы беспроводной передачи данных могут являться удобной, а иногда и неизбежной альтернативой кабельным соединениям. Беспроводные технологии различаются по типам сигнала, частоте (бóльшая частота означает бóльшую скорость передачи) и расстоянию передачи. Тремя главными типами беспроводной передачи данных являются радиосвязь, связь в микроволновом диапазоне и инфракрасная связь.

Радиосвязь

Технологии радиосвязи (Radio Waves) пересылают данные на радиочастотах и практически не имеют ограничений по дальности. Она используется для соединения локальных сетей на больших географических расстояниях. Радиопередача в целом имеет высокую стоимость, подлежит государственному регулированию и крайне чувствительна к электронному и атмосферному наложению. Она также подвержена перехвату, поэтому требует шифрования или другой модификации при передаче, чтобы обеспечить разумный уровень безопасности.

Связь в микроволновом диапазоне

Передача данных в микроволновом диапазоне (Microwaves) использует высокие частоты и применяется как на коротких расстояниях, так и в глобальных коммуникациях. Их главное ограничение заключается в том, что передатчик и приемник должны быть в зоне прямой видимости друг друга. Передача данных в микроволновом диапазоне обычно используется для соединения локальных сетей в отдельных зданиях, где использование физического носителя затруднено или непрактично. Связь в микроволновом диапазоне также широко используется в глобальной

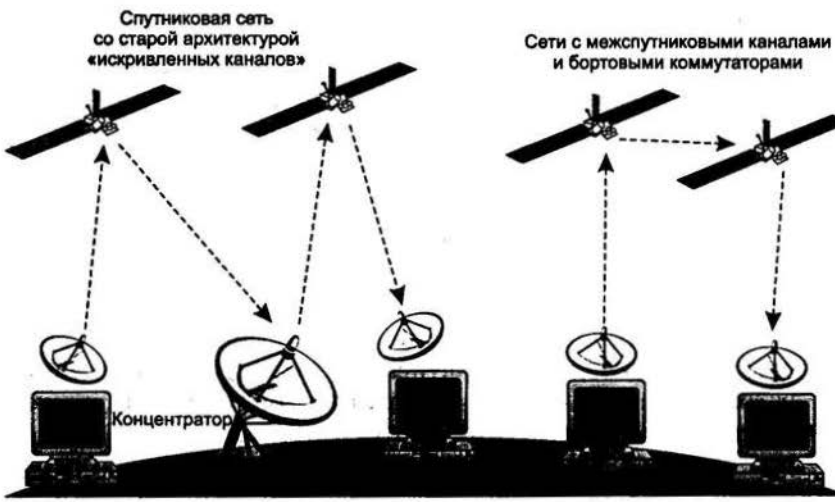

Рис. 3.8. Схема спутниковой связи

передаче с помощью спутников и наземных спутниковых антенн, обеспечивающих выполнение требования прямой видимости (рис. 3.8). Спутники в системах связи могут находиться на геостационарных (высота 36 тысяч км) или низких орбитах. При геостационарных орбитах заметны задержки на прохождение сигналов (туда и обратно около 520 мс). Возможно покрытие поверхности всего земного шара с помощью четырех спутников. В низкоорбитальных системах обслуживание конкретного пользователя происходит попеременно разными спутниками. Чем ниже орбита, тем меньше площадь покрытия и, следовательно, нужно или больше наземных станций, или требуется межспутниковая связь, что естественно утяжеляет спутник. Число спутников также значительно больше (обычно несколько десятков). Например, глобальная спутниковая сеть Iridium, имеющая и российский сегмент, включает 66 низкоорбитальных спутников, диапазон частот 1610—1626,5 МГц.

Инфракрасная связь

Инфракрасные технологии (infrared transmissions), функционирующие на очень высоких частотах, приближающихся к частотам видимого света, могут быть использованы для установления двусторонней или широковещательной передачи на близких расстояниях. Они обычно используют светодиоды (LED, light-emitting diode) для передачи инфракрасных волн приемнику. Поскольку они могут быть физически заблокированы и испытывать интерференцию с ярким светом, инфракрасная передача ограничена малыми расстояниями в зоне прямой видимости. Инфракрасная передача обычно используется в складских или офисных зданиях, иногда для связи двух зданий. Другим популярным использованием инфракрасной связи является беспроводная передача данных в портативных компьютерах.

Технология Bluetooth

Bluetooth (переводится как «синий зуб») — производственная спецификация беспроводных персональных сетей (от англ. Wireless personal area network — WPAN).

Bluetooth обеспечивает обмен информацией между такими устройствами как карманные и обычные персональные компьютеры, мобильные телефоны, ноутбуки, принтеры, цифровые фо-

тоаппараты, мышки, клавиатуры, джойстики, наушники, гарнитуры на надежной, недорогой, повсеместно доступной радиочастоте для ближней связи.

Bluetooth позволяет этим устройствам сообщаться, когда они находятся в радиусе до 10—100 метров друг от друга (дальность очень сильно зависит от преград и помех), даже в разных помещениях.

Радиосвязь Bluetooth осуществляется в ISM-диапазоне (от англ. Industry, Science and Medicine), который используется в различных бытовых приборах и беспроводных сетях (свободный от лицензирования диапазон 2,4—2,4835 ГГц). В Bluetooth применяется метод расширения спектра со скачкообразной перестройкой частоты (от англ. Frequency Hopping Spread Spectrum — FHSS). Метод FHSS прост в реализации, обеспечивает устойчивость к широкополосным помехам, а оборудование стоит недорого.

Согласно алгоритму FHSS, в Bluetooth несущая частота сигнала скачкообразно меняется 1600 раз в секунду (всего выделяется 79 рабочих частот шириной в 1 МГц, а в Японии, Франции и Испании полоса у́же — 23 частотных канала). Последовательность переключения между частотами для каждого соединения является псевдослучайной и известна только передатчику и приемнику, которые каждые 625 мкс (один временной слот) синхронно перестраиваются с одной несущей частоты на другую. Таким образом, если рядом работают несколько пар приемник—передатчик, то они не мешают друг другу. Этот алгоритм является также составной частью системы защиты конфиденциальности передаваемой информации: переход происходит по псевдослучайному алгоритму и определяется отдельно для каждого соединения. При передаче цифровых данных и аудиосигнала (64 кбит/с в обоих направлениях) используются различные схемы кодирования: аудиосигнал не повторяется (как правило), а цифровые данные в случае утери пакета информации будут переданы повторно. Без помехоустойчивого кодирования это обеспечивает передачу данных со скоростями 723,2 кбит/с, с обратным каналом 57,6 кбит/с или 433,9 кбит/с в обоих направлениях.

Беспроводные сети Wi-Fi

Wi-Fi (от англ. Wireless Fidelity — «беспроводная точность») — беспроводная сеть, а также стандарт на оборудование беспроводных сетей Wireless LAN. Разработан консорциумом

Wi-Fi Alliance на базе стандартов IEEE 802.11, «Wi-Fi» — торговая марка «Wi-Fi Alliance». Технологию назвали Wireless-Fidelity по аналогии с Hi-Fi.

Установка Wireless LAN рекомендовалась там, где развертывание кабельной системы было невозможно или экономически нецелесообразно. В нынешнее время во многих организациях используется Wi-Fi, так как при определенных условиях скорость работы сети уже превышает 100 Мбит/с. Пользователи могут перемещаться между точками доступа по территории покрытия сети Wi-Fi.

Мобильные устройства (КПК, смартфоны, PSP и ноутбуки), оснащенные клиентскими Wi-Fi приемо-передающими устройствами, могут подключаться к локальной сети и получать доступ в Internet через точки доступа или хот-споты.

Обычно схема Wi-Fi сети содержит не менее одной точки доступа и не менее одного клиента. Также возможно подключение двух клиентов в режиме точка—точка, когда точка доступа не используется, а клиенты соединяются посредством сетевых адаптеров «напрямую». Точка доступа передает свой идентификатор сети (Service Set identifier — SSID) с помощью специальных сигнальных пакетов на скорости 0,1 Мбит/с каждые 100 мс. Поэтому 0,1 Мбит/с — наименьшая скорость передачи данных для Wi-Fi. Зная SSID сети, клиент может выяснить, возможно ли подключение к данной точке доступа. При попадании в зону действия двух точек доступа с идентичными SSID приемник может выбирать между ними на основании данных об уровне сигнала.

Преимущества Wi-Fi:

- позволяет развернуть сеть без прокладки кабеля, что может уменьшить стоимость развертывания и/или расширения сети. Места, где нельзя проложить кабель, например, вне помещений и в зданиях, имеющих историческую ценность, могут обслуживаться беспроводными сетями;
- позволяет иметь доступ к сети мобильным устройствам;
- Wi-Fi-устройства широко распространены на рынке. Устройства разных производителей могут взаимодействовать на базовом уровне сервисов;
- Wi-Fi — это набор глобальных стандартов. В отличие от сотовых телефонов, Wi-Fi-оборудование может работать в разных странах по всему миру.

Недостатки Wi-Fi:

- частотный диапазон и эксплуатационные ограничения в различных странах неодинаковы. Во многих европейских

странах разрешены два дополнительных канала, которые запрещены в США; В Японии есть еще один канал в верхней части диапазона, а другие страны, например Испания, запрещают использование низкочастотных каналов. Более того, некоторые страны, например Россия, Белоруссия и Италия, требуют регистрации всех сетей Wi-Fi, работающих вне помещений, или требуют регистрации Wi-Fi-оператора;
- высокое по сравнению с другими стандартами потребление энергии, что уменьшает время жизни батарей и повышает температуру устройства;
- Wi-Fi имеют ограниченный радиус действия. Типичный домашний маршрутизатор Wi-Fi стандарта 802.11b или 802.11g имеет радиус действия 45 м в помещении и 450 м снаружи;
- наложение сигналов закрытой или использующей шифрование точки доступа и открытой точки доступа, работающих на одном или соседних каналах, может помешать доступу к открытой точке доступа. Эта проблема может возникнуть при большой плотности точек доступа, например, в больших многоквартирных домах, где многие жильцы ставят свои точки доступа Wi-Fi;
- неполная совместимость между устройствами разных производителей или неполное соответствие стандарту может привести к ограничению возможностей соединения или уменьшению скорости;
- уменьшение производительности сети во время дождя.

Технология WiMAX

WiMAX (от англ. Worldwide Interoperability for Microwave Access) — телекоммуникационная технология, разработанная с целью предоставления универсальной беспроводной связи на больших расстояниях для широкого спектра устройств (от рабочих станций и портативных компьютеров до мобильных телефонов). Основана на стандарте IEEE 802.16, который также называют Wireless MAN (Wireless Metropolitan Area Networks — беспроводные сети масштаба города).

В общем виде WiMAX-сети состоят из следующих основных частей: базовых и абонентских станций, а также оборудования, связывающего базовые станции между собой, с поставщиком сервисов и с Internet.

Для соединения базовой станции с абонентской используется высокочастотный диапазон радиоволн от 1,5 до 11 ГГц. В идеальных условиях скорость обмена данными может достигать 70 Мбит/с, при этом не требуется обеспечения прямой видимости между базовой станцией и приемником.

WiMAX применяется как для решения проблемы «последней мили», так и для предоставления доступа в сеть офисным и районным сетям.

Между базовыми станциями устанавливаются соединения (прямой видимости), использующие диапазон частот от 10 до 66 ГГц, скорость обмена данными может достигать 120 Мбит/с. При этом по крайней мере одна базовая станция подключается к сети провайдера с использованием классических проводных соединений. Однако, чем большее число базовых станций подключено к сетям провайдера, тем выше скорость передачи данных и надежность сети в целом.

Структура сетей семейства стандартов IEEE 802.16 схожа с традиционными сетями мобильной связи (базовые станции действуют на расстояниях до десятков километров, для их установки не обязательно строить вышки — допускается установка на крышах домов при соблюдении условия прямой видимости между станциями).

3.5. Системы мобильной связи

Системы мобильной связи осуществляют передачу информации между пунктами, один или оба из которых являются подвижными. Характерным признаком систем мобильной связи является применение радиоканала. К технологиям мобильной связи относятся пейджинг, твейджинг, сотовая телефония.

Пейджинг — система односторонней связи, при которой передаваемое сообщение поступает на пейджер пользователя, извещая его о необходимости предпринять то или иное действие или просто информируя его о тех или иных текущих событиях. Это наиболее дешевый вид мобильной связи.

Твейджинг — это двухстронний пейджинг. В отличие от пейджинга возможно подтверждение получения сообщения и даже проведение некоторого подобия диалога.

Сотовые технологии обеспечивают телефонную связь между подвижными абонентами (ячейками). Связь осуществляется через базовые (стационарные) станции, выполняющие коммутирующие функции.

Разработано несколько стандартов мобильной связи.

Одной из наиболее широко распространенных технологий мобильной связи (в том числе и в России) является технология, соответствующая стандарту для цифровых сетей сотовой связи GSM (Global System for Mobile Communications). GSM может поддерживать интенсивный трафик (270 кбит/с), обеспечивает роуминг (т. е. автоматическое отслеживание перехода мобильного пользователя из одной соты в другую), допускает интеграцию речи и данных и связь с сетями общего пользования. Используются разновидности: сотовая связь GSM-900 в частотном диапазоне 900 МГц (более точно 890—960 МГц) и микросотовая связь GSM-1800 в диапазоне 1800 МГц (1710—1880 МГц). Название микросотовая обусловлено большим затуханием и, следовательно, меньшей площадью соты. Однако увеличение числа каналов выгодно при высокой плотности абонентов. Мощность излучения мобильных телефонов — 1—2 Вт.

Архитектура GSM-системы представлена на рис. 3.9. В каждой соте действует базовая станция BTS (Base Transciever Station), обеспечивающая прием и передачу радиосигналов абонентам. Базовая станция имеет диапазон частот, отличный от диапазонов соседних сот. Мобильная ячейка прослушивает соседние базовые станции и сообщает контроллеру базовых станций (BSC — Base Station Controller) о качестве приема с тем, чтобы контроллер мог своевременно переключить ячейку на нужную станцию. Центр коммутации (MSC — Mobile services

Рис. 3.9. Схема сотовой телефонной связи

Switching Centre) осуществляет коммутацию и маршрутизацию, направляя вызовы нужному абоненту, в том числе во внешние сети общего пользования. В базе данных хранятся сведения о местоположении пользователей, технических характеристиках мобильных станций, данные для идентификации пользователей.

Контрольные вопросы

1. Дайте определение линии связи.
2. Дайте определение физической среды передачи данных.
3. Как классифицируются линии связи?
4. Перечислите основные характеристики линий связи.
5. Дайте определение амплитудно-частотной характеристики, полосы пропускания, затухания, пропускной способности линий связи.
6. Охарактеризуйте помехоустойчивость, перекрестные наводки, достоверность передачи данных линий связи.
7. Перечислите основные типы кабелей.
8. Дайте характеристику кабелей на основе неэкранированной витой пары.
9. Дайте характеристику кабелей на основе экранированной витой пары.
10. Дайте характеристику коаксиальным кабелям.
11. Охарактеризуйте волоконно-оптические кабели.
12. Дайте характеристику беспроводным каналам связи.
13. Каким будет теоретический предел скорости передачи данных в битах в секунду по каналу с шириной полосы пропускания в 10 кГц, если мощность передатчика составляет 0,01 мВт, а мощность шума в канале равна 0,0001 мВт?

Глава 4
ЛОКАЛЬНЫЕ ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ

4.1. Общая характеристика локальных сетей

Локальными сетями называют частные сети, размещающиеся в одном здании или на территории какой-либо организации размерами до нескольких километров. Их часто используют для объединения компьютеров и рабочих станций в офисах компании или предприятия для обмена информацией и предоставления совместного доступа к ресурсам сети (принтерам, сканерам и др.).

Локальные вычислительные сети (ЛВС) применяются и при разработке коллективных проектов, например сложных программных комплексов. На базе ЛВС можно создавать системы автоматизированного проектирования. Это позволяет реализовывать новые технологии проектирования изделий машиностроения, радиоэлектроники и вычислительной техники. В условиях развития рыночной экономики появляется возможность создавать конкурентоспособную продукцию, быстро модернизировать ее, обеспечивая реализацию экономической стратегии предприятия. Кроме того, ЛВС позволяют реализовывать новые информационные технологии в системах организационно-экономического управления, а в учебных лабораториях вузов они позволяют повысить качество обучения и внедрять современные интеллектуальные технологии обучения.

Локальные сети характеризуются размерами, технологией передачи данных и топологией их построения.

Под **размерами** локальных сетей понимают длину сетевого кабеля, соединяющего компьютеры. Они могут находиться в пределах от нескольких метров до нескольких километров.

По **технологии** организации локальные сети подразделяют на **широковещательные** и сети с передачей от **«точки к точке»** (point-to-point).

Широковещательные сети обладают единым каналом связи, совместно используемым всеми машинами сети. Пакеты, передаваемые одной машиной, получают все компьютеры сети. Пакет имеет поле «адрес», по которому благодаря дешифратору адреса только одна машина, которой предназначается сообщение, считывает его, а затем обрабатывает. Остальные машины игнорируют это сообщение. Такие технологии с успехом используются в небольших локальных сетях.

Сети с передачей от «точки к точке» состоят из большого числа соединенных машин и используются, в отличие от предыдущей технологии, в больших корпоративных сетях. Передаваемые пакеты проходят через ряд промежуточных машин по некоему ранее вычисленному алгоритму пути от источника к получателю.

Существует три основные **топологии** сети, рассмотренные ранее: **шинная, кольцевая** и топология типа **«звезда»**, которые обладают свойством **однородности**, т. е. все компьютеры в такой сети имеют равные права в отношении доступа к другим компьютерам. Такая однородность структуры делает простой процедуру наращивания числа компьютеров, облегчает обслуживание и эксплуатацию сети. Однако, при этом в таких сетях использование типовых структур порождает различные ограничения, важнейшими из которых являются:

- ограничения на длину связи между узлами;
- ограничения на количество узлов;
- ограничения на интенсивность трафика, порождаемого узлами сети.

Для снятия этих ограничений используются специальные **структуризации** сети и специальное **структурообразующее оборудование** — повторители, концентраторы, мосты, коммутаторы, маршрутизаторы.

При организации взаимодействия узлов в локальных сетях основная роль отводится протоколу канального уровня. Однако для того, чтобы канальный уровень мог справиться с этой задачей, структура локальных сетей должна быть вполне определенной, так, например, наиболее популярный протокол канального уровня — Ethernet — рассчитан на параллельное подключение всех узлов сети к общей для них шине — отрезку коаксиального

кабеля или иерархической древовидной структуре сегментов, образованных повторителями. Протокол Token Ring также рассчитан на вполне определенную конфигурацию — соединение компьютеров в виде логического кольца.

4.2. Методы доступа к среде передачи данных

Под **доступом к сети** понимают взаимодействие компьютера в сети **со средой передачи данных** для обмена информацией с другими ЭВМ.

В настоящее время наиболее распространенными методами доступа (правами на передачу информации) к локальной сети являются (рис. 4.1):

- **случайный доступ** CSMA/CS (carrier sense multiple access with collision detection) — множественный доступ с контролем несущей и обнаружением конфликтов.
- **маркерные методы** — на основе маркерной шины и маркерного кольца.

Существует две разновидности метода случайного доступа: **CSMA/CS** — множественный доступ с контролем несущей и обнаружением конфликтов — и **приоритетный доступ**.

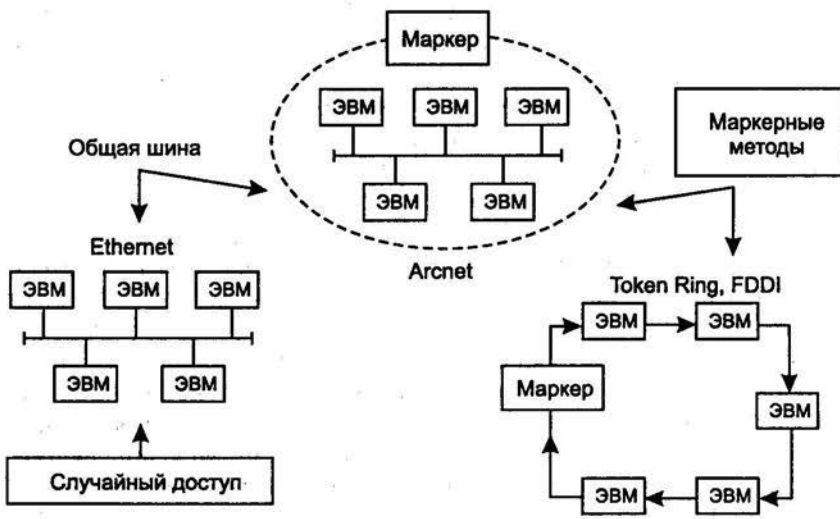

Рис. 4.1. Методы доступа к локальной сети

4.2.1. Множественный доступ с контролем несущей и обнаружением конфликтов

В сетях Ethernet используется метод доступа к среде передачи данных, называемый методом коллективного доступа с опознаванием несущей и обнаружением коллизий CSMA/CD (рис. 4.2).

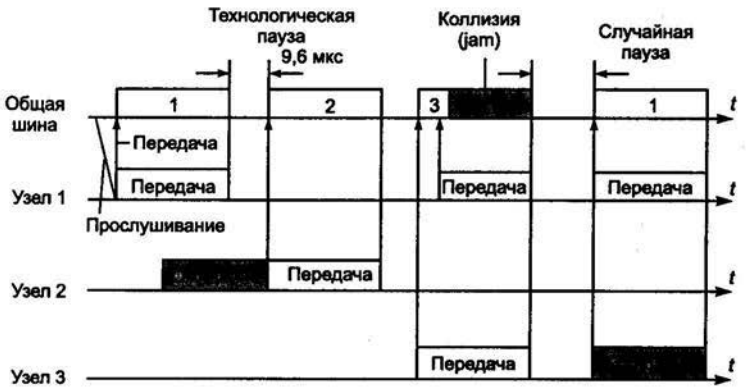

Рис. 4.2. Метод коллективного доступа с опознаванием несущей и обнаружением коллизий CSMA/CD

Этот метод применяется исключительно в сетях с логической общей шиной. Все компьютеры такой сети имеют непосредственный доступ к общей шине, поэтому она может быть использована для передачи данных между любыми двумя узлами сети. Одновременно все компьютеры сети имеют возможность немедленно (с учетом задержки распространения сигнала по физической среде) получить данные, которые любой из компьютеров начал передавать на общую шину.

Все данные, передаваемые по сети, помещаются в кадры определенной структуры и снабжаются уникальным адресом станции назначения.

Чтобы получить возможность передавать кадр, станция должна убедиться, что разделяемая среда свободна. Это достигается прослушиванием основной гармоники сигнала, которая также называется несущей частотой (carrier-sense — CS). Признаком незанятости среды является отсутствие на ней несущей частоты, которая при манчестерском способе кодирования равна 5—10 МГц, в зависимости от последовательности единиц и нулей, передаваемых в данный момент.

Если среда свободна, то узел имеет право начать передачу кадра. В сети Ethernet на коаксиальном кабеле сигналы передатчика узла распространяются в обе стороны, так что все узлы сети их получают. Кадр данных всегда сопровождается преамбулой (preamble), которая состоит из 7 байт, состоящих из значений 10101010, и 8-го байта, равного 10101011. Преамбула нужна для вхождения приемника в побитовый и побайтовый синхронизм с передатчиком.

Все станции, подключенные к кабелю, могут распознать факт передачи кадра, и та станция, которая узнает собственный адрес в заголовках кадра, записывает его содержимое в свой внутренний буфер, обрабатывает полученные данные, передает их вверх по своему стеку, а затем посылает по кабелю кадр-ответ. Адрес станции источника содержится в исходном кадре, поэтому станция-получатель знает, кому нужно послать ответ.

Если другой узел, желающий начать передачу, обнаружил, что среда занята (на ней присутствует несущая частота), он будет вынужден ждать, пока первый узел не прекратит передачу кадра.

После окончания передачи кадра все узлы сети обязаны выдержать технологическую паузу (Inter Packet Gap) в 9,6 мкс. Эта пауза, называемая также межкадровым интервалом, нужна для приведения сетевых адаптеров в исходное состояние, а также для предотвращения монопольного захвата среды одной станцией. После окончания технологической паузы узлы имеют право начать передачу своего кадра, так как среда свободна. Из-за задержек распространения сигнала по кабелю не все узлы строго одновременно фиксируют факт окончания передачи кадра.

При описанном подходе возможна ситуация, когда две станции одновременно пытаются передать кадр данных по общей среде. Механизм прослушивания среды и пауза между кадрами не гарантируют от возникновения такой ситуации, когда две станции или более одновременно решают, что среда свободна, и начинают передавать свои кадры. Говорят, что при этом происходит **коллизия** (collision), так как содержимое обоих кадров сталкивается на общем кабеле и происходит искажение информации. Методы кодирования, используемые в Ethernet, не позволяют выделять сигналы каждой станции из общего сигнала.

Коллизия является нормальной ситуацией в работе сетей Ethernet. Для возникновения коллизии не обязательно, чтобы несколько станций начали передачу абсолютно одновременно, такая ситуация маловероятна. Гораздо вероятней, что коллизия

возникает из-за того, что один узел начинает передачу раньше другого, но до второго узла сигналы первого просто не успевают дойти к тому времени, когда второй узел решает начать передачу своего кадра. То есть коллизии — это следствие распределенного характера сети. Чтобы корректно обработать коллизию, все станции одновременно наблюдают за возникающими на кабеле сигналами. Если передаваемые и наблюдаемые сигналы отличаются, то фиксируется обнаружение коллизии (collision detection — CD). Для увеличения вероятности скорейшего обнаружения коллизии всеми станциями сети станция, которая обнаружила коллизию, прерывает передачу своего кадра (в произвольном месте, возможно, и не на границе байта) и усиливает ситуацию коллизии посылкой в сеть специальной последовательности из 32 бит, называемой jam-последовательностью. После этого обнаружившая коллизию передающая станция обязана прекратить передачу и сделать паузу в течение короткого случайного интервала времени. Затем она может снова предпринять попытку захвата среды и передачи кадра.

Следует отметить, что метод доступа CSMA/CD вообще не гарантирует станции, что она когда-либо сможет получить доступ к среде. Конечно, при небольшой загрузке сети вероятность такого события невелика, но при коэффициенте использования сети, приближающемся к 1, такое событие становится очень вероятным. Этот недостаток метода случайного доступа — плата за его чрезвычайную простоту, которая сделала технологию Ethernet самой недорогой. Другие методы доступа — маркерный доступ сетей Token Ring, FDDI и другие — свободны от этого недостатка.

Четкое распознавание коллизий всеми станциями сети является необходимым условием корректной работы сети Ethernet. Если какая-либо передающая станция не распознает коллизию и решит, что кадр данных ею передан верно, то этот кадр данных будет утерян. Из-за наложения сигналов при коллизии информация кадра исказится, и он будет отбракован принимающей станцией (возможно, из-за несовпадения контрольной суммы). Скорее всего, искаженная информация будет повторно передана каким-либо протоколом верхнего уровня, например транспортным или прикладным, работающим с установлением соединения. Но повторная передача сообщения протоколами верхних уровней произойдет через значительно более длительный интервал времени (иногда даже через несколько секунд) по сравнению

с микросекундными интервалами, которыми оперирует протокол Ethernet. Поэтому если коллизии не будут надежно распознаваться узлами сети Ethernet, то это приведет к заметному снижению полезной пропускной способности данной сети.

Для надежного распознавания коллизий должно выполняться следующее соотношение:

$$T_{min} \geq PDV,$$

где T_{min} — время передачи кадра минимальной длины; PDV — время, за которое сигнал коллизии успевает распространиться до самого дальнего узла сети.

Так как в худшем случае сигнал должен пройти дважды между наиболее удаленными друг от друга станциями сети (в одну сторону проходит неискаженный сигнал, а на обратном пути распространяется уже искаженный коллизией сигнал), то это время называется **временем двойного оборота** (Path Delay Value — PDV).

При выполнении этого условия передающая станция должна успевать обнаружить коллизию, которую вызвал переданный ее кадр, еще до того, как она закончит передачу этого кадра. Очевидно, что выполнение этого условия зависит, с одной стороны, от длины минимального кадра и пропускной способности сети, а с другой стороны, от длины кабельной системы сети и скорости распространения сигнала в кабеле (для разных типов кабеля эта скорость несколько отличается).

Все параметры протокола Ethernet подобраны таким образом, чтобы при нормальной работе узлов сети коллизии всегда четко распознавались. При выборе параметров, конечно, учитывалось и приведенное выше соотношение, связывающее между собой минимальную длину кадра и максимальное расстояние между станциями в сегменте сети.

В стандарте Ethernet принято, что минимальная длина поля данных кадра составляет 46 байт (что вместе со служебными полями дает минимальную длину кадра 64 байт, а вместе с преамбулой — 72 байт или 576 бит). Отсюда может быть определено ограничение на расстояние между станциями. Так, в 10-мегабитном Ethernet время передачи кадра минимальной длины равно 575 битовых интервалов, следовательно, время двойного оборота должно быть меньше 57,5 мкс. Расстояние, которое сигнал может пройти за это время, зависит от типа кабеля и для толстого коаксиального кабеля равно примерно 13 280 м. Учитывая, что

за это время сигнал должен пройти по линии связи дважды, расстояние между двумя узлами не должно быть больше 6635 м. В стандарте величина этого расстояния выбрана существенно меньше с учетом других, более строгих ограничений.

Одно из таких ограничений связано с предельно допустимым затуханием сигнала. Для обеспечения необходимой мощности сигнала при его прохождении между наиболее удаленными друг от друга станциями сегмента кабеля максимальная длина непрерывного сегмента толстого коаксиального кабеля с учетом вносимого им затухания выбрана в 500 м. Очевидно, что на кабеле в 500 м условия распознавания коллизий будут выполняться с большим запасом для кадров любой стандартной длины, в том числе и 72 байт (время двойного оборота по кабелю 500 м составляет всего 43,3 битовых интервала). Поэтому минимальная длина кадра могла бы быть установлена еще меньше. Однако разработчики технологии не стали уменьшать минимальную длину кадра, имея в виду многосегментные сети, которые строятся из нескольких сегментов, соединенных повторителями.

Повторители увеличивают мощность передаваемых с сегмента на сегмент сигналов, в результате затухание сигналов уменьшается и можно использовать сеть гораздо большей длины, состоящую из нескольких сегментов. В коаксиальных реализациях Ethernet разработчики ограничили максимальное количество сегментов в сети пятью, что в свою очередь ограничивает общую длину сети 2500 метрами. Даже в такой многосегментной сети условие обнаружения коллизий по-прежнему выполняется с большим запасом (сравним полученное из условия допустимого затухания расстояние в 2500 м с вычисленным выше максимально возможным по времени распространения сигнала расстоянием 6635 м). Однако в действительности временной запас является существенно меньше, поскольку в многосегментных сетях сами повторители вносят в распространение сигнала дополнительную задержку в несколько десятков битовых интервалов. Естественно, небольшой запас был сделан также для компенсации отклонений параметров кабеля и повторителей.

В результате учета всех этих и некоторых других факторов было тщательно подобрано соотношение между минимальной длиной кадра и максимально возможным расстоянием между станциями сети, которое обеспечивает надежное распознавание коллизий. Это расстояние называют также максимальным **диаметром сети**.

С увеличением скорости передачи кадров, что имеет место в новых стандартах, базирующихся на том же методе доступа CSMA/CD, например Fast Ethernet, максимальное расстояние между станциями сети уменьшается пропорционально увеличению скорости передачи. В стандарте Fast Ethernet оно составляет около 210 м, а в стандарте Gigabit Ethernet оно было бы ограничено 25 метрами, если бы разработчики стандарта не предприняли некоторых мер по увеличению минимального размера пакета.

4.2.2. Приоритетный доступ

При этом способе концентратор, получив одновременно два запроса, отдает предпочтение тому, который имеет более высокий **приоритет**. Эта технология реализуется в виде системы с опросом. Интеллектуальный концентратор опрашивает подключенные к нему компьютеры и при наличии у нескольких из них запроса на передачу разрешает передать пакет данных тому, у которого приоритет, установленный для него, выше. Одним из примеров такого доступа является технология 100 VG (Voice Grade — голосовой канал) Any Lan, обладающая следующими возможностями:

- скорость передачи данных — более 100 Мбит/с;
- поддержка структурированной кабельной системы на основе витой пары и оптоволоконного кабеля.

4.2.3. Маркерные методы доступа

К маркерным методам доступа относятся два наиболее известных типа передачи данных по локальной сети: **маркерная шина** (стандарт IEEE 802.4) и **маркерное кольцо** (стандарт IEEE 802.5)

Маркер — управляющая последовательность бит, передаваемая компьютером по сети. Маркер предназначен для управления доступом к сети компьютеров в маркерных методах доступа.

Маркер включает в себя три поля длиной в один байт каждый (рис. 4.3): начальный ограничитель SD (Start Delimiter), представляющий собой уникальную последовательность JK00JK000, которую нельзя спутать ни с одной битовой последовательностью внутри кадра; управление доступом AC (Access Control), состоящее в свою очередь еще из четырех полей: PPP — битов приори-

тета, бита маркера T (при T = 1 передаваемый кадр — маркер доступа), бита монитора M (устанавливается в 1 активным монитором, и в 0 другими станциями сети), RRR — резервные биты; конечный ограничитель ED (End Delimiter), который, как и начальный ограничитель, содержит уникальную последовательность JK1LK1, а также два бита признаков: I (Intermediate), указывающий, является ли кадр последним в серии кадров или промежуточным (I=1), E (Error) — признак ошибки.

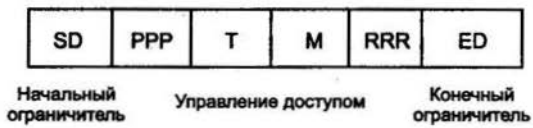

Рис. 4.3. Формат маркера

Станция, имеющая данные для передачи, получив маркер, изымает его из кольца, тем самым получая право на передачу информации, заменяет его кадром данных установленного формата, содержащего следующие поля: начальный ограничитель SD, управление кадром FC (Frame Control), адрес назначения DA (Destination Address), адрес источника SA (Source Address), данные (INFO), контрольная сумма (INFO), контрольная сумма FCS, конечный ограничитель ED, статус кадра FS (Frame Status).

4.3. Сети Ethernet

Обычный **Ethernet**, являющийся одним из самых простых и дешевых в построении из когда-либо разработанных стандартов локальных сетей, создан на базе экспериментальной сети Ethernet Network, предложенной фирмой Xerox, в 1975 году. В сетях Ethernet все компьютеры имеют непосредственный доступ к общей шине, поэтому она может быть использована для передачи данных между любыми двумя узлами сети. Одновременно все компьютеры имеют возможность немедленно получить данные, которые любой из компьютеров начал передавать на общую шину. Такая простота подключения и передачи информации компьютерами — одна из причин, которые привели стандарт Ethernet к такому успеху. Иногда такое построение сети называют методом коллективного доступа (Multiply Access).

В зависимости от типа физической реализации различают следующие типы Ethernet:

- 10base-5 (толстый коаксиальный кабель), называемый по типу используемого в ней носителя — толстого коаксиального кабеля. Недостатками этого типа построения Ethernet являются: неудобный в использовании кабель за счет своей толщины (внешний диаметр составляет около 10 мм), высокая стоимость, максимальное допустимое количество станций — не более 100. Достоинствами данного стандарта является его высокая защищенность от внешних воздействий и сравнительно большая длина сегмента — до 500 м. Данный стандарт разработан фирмой Xerox и считается классическим Ethernet;
- 10base-2 (тонкий коаксиальный кабель) — самая из простых в установке и дешевых типов сети. Тонкий коаксиальный кабель — до 5 мм, прокладывается вдоль расположения компьютеров сети. На конце каждого сегмента располагается 50-омный резистор (терминатор), предотвращающий возникновение эффекта отраженной волны. К недостаткам данного типа сети Ethernet относят: выход из строя сети при повреждении кабеля и сравнительно трудоемкое обнаружение отказавшего отрезка кабеля, которое возможно при использовании кабельного тостера, низкая защита от помех, максимальное число компьютеров в сети — не более 1024. Максимаальная длина сегмента данного стандарта без использования повтрителей составляет 185 м;
- 10base-T (витая пара) — это сети на основе витой пары, на сегодняшний день являются наиболее распространенными за счет того, что они строятся на основе витой пары и используют топологию типа «звезда». За счет этого конфигурировать локальную сеть становится значительно удобнее и рациональнее. Однако эти сети не лишены следующих недостатков: слабая помехозащищенность и восприимчивость к электрическим помехам не дают возможности использовать такие сети в непосредственной близости к источникам электромагнитных излучений;
- 10base-F (волоконно-оптический канал) — технология, использующая в качестве носителя волоконно-оптический кабель. По строению аналогичен Ethernet 10Base-T, т. е. использует топологию «звезда». Использование волоконно-оптического кабеля приводит к тому, что такое по-

строение ЛВС обеспечивает почти полную помехозащищенность от электромагнитных излучений. Однако этот метод построения Ethernet имеет следующие недостатки:

— волоконно-оптический кабель является самым дорогим из всех видов кабеля;
— волоконно-оптический кабель хрупкий, поэтому монтаж его очень затруднен.

Топология для всех четырех типов практически не различается. Данные в локальной сети передаются со скоростью до 10 Мбит/с, о чем говорит первая цифра в названии типа сети.

Существует еще одна разновидность технологии Ethernet — Fast Ethernet, способная передавать данные со скоростью до 100 Мбит/с, которая в свою очередь подразделяется на:

- 100base-T4 (4 витые пары);
- 100base-TX (2 витые пары);
- 100base-FX (волоконно-оптический канал).

Все отличия технологии Fast Ethernet от Ethernet сосредоточены на физическом уровне. Уровни MAC и LLC в Fast Ethernet остались абсолютно теми же и их описывают прежние главы стандартов 802.3 и 802.2.

Более сложная структура физического уровня технологии Fast Ethernet вызвана тем, что в ней используются три варианта кабельных систем:

- волоконно-оптический многомодовый кабель, используются два волокна;
- витая пара категории 5, используются две пары;
- витая пара категории 3, используются четыре пары.

Коаксиальный кабель, давший миру первую сеть Ethernet, в число разрешенных сред передачи данных новой технологии Fast Ethernet не попал. Это общая тенденция многих новых технологий, поскольку на небольших расстояниях витая пара категории 5 позволяет передавать данные с той же скоростью, что и коаксиальный кабель, но сеть получается более дешевой и удобной в эксплуатации. На больших расстояниях оптическое волокно обладает гораздо более широкой полосой пропускания, чем коаксиал, а стоимость сети получается ненамного выше, особенно если учесть высокие затраты на поиск и устранение неисправностей в крупной кабельной коаксиальной системе.

Отказ от коаксиального кабеля привел к тому, что сети Fast Ethernet всегда имеют иерархическую древовидную структуру, построенную на концентраторах, как и сети 10Base-T/10Base-F.

Основным отличием конфигураций сетей Fast Ethernet является сокращение диаметра сети примерно до 200 м, что объясняется уменьшением времени передачи кадра минимальной длины в 10 раз за счет увеличения скорости передачи в 10 раз по сравнению с 10-мегабитным Ethernet.

При использовании коммутаторов протокол Fast Ethernet может работать в полнодуплексном режиме, в котором нет ограничений на общую длину сети, а остаются только ограничения на длину физических сегментов, соединяющих соседние устройства (адаптер — коммутатор или коммутатор — коммутатор). Поэтому при создании магистралей локальных сетей большой протяженности технология Fast Ethernet также активно применяется, но только в полнодуплексном варианте совместно с коммутаторами.

4.4. Локальные сети на основе маркерной шины

Физически **маркерная шина** представляет собой линейный или древовидный кабель, к которому присоединены станции. Самой распространенной реализацией данного построения являются сети ArcNet. Логически соединение станций организовано в кольцо, в котором каждая станция знает адреса своих соседей «слева» и «справа». При инициализации логического кольца право посылать кадр получает станция с наибольшим номером. Переслав кадр, она передает право пересылки своему ближайше-

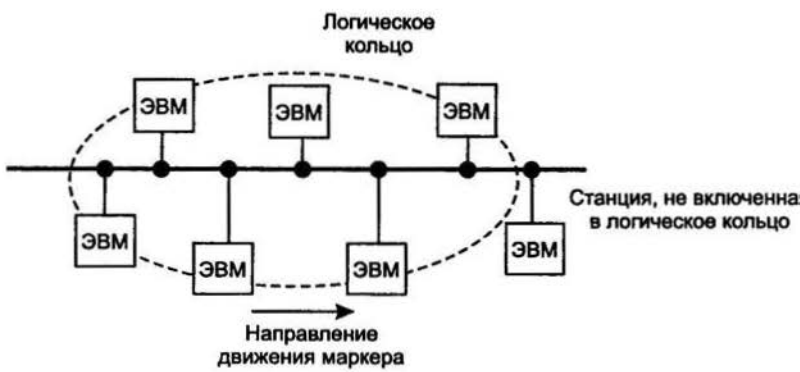

Рис. 4.4. Структура сети на основе маркерной шины

му соседу, посылая ему специальный управляющий кадр, называемый маркером (рис. 4.4).

Маркер перемещается по логическому кольцу, при этом право передачи кадров имеет только держатель маркера. Поскольку в каждый момент времени маркер может находиться только у одной станции, столкновений не происходит.

Физический порядок, в котором станции соединены кабелем, не имеет значения. Поскольку кабель является широковещательной средой, каждая станция получает каждый кадр, игнорируя кадры, адресованные не ей. Передавая маркер, станция посылает маркерный кадр своему логическому соседу по кольцу независимо от его физического расположения.

Инициализация кольца осуществляется следующим образом. Когда все станции выключены и одна из них переходит в подключенный режим, она замечает, что в течение определенного периода в сети нет трафика (по сети ничего не передается). Тогда она посылает широковещательный запрос с требованием маркера. Не услышав никаких конкурентов, претендующих на маркер, она сама создает маркер и кольцо, состоящее из одной станции. Периодически она посылает управляющий кадр, предлагающий другим станциям присоединиться к кольцу. Пример передаваемого кадра при маркерной организации сети представлен на рис. 4.5. Когда новые станции включаются, они отвечают на эти предложения и присоединяются к кольцу. При этом ее соседи «слева» и «справа» запоминают адрес вновь включенной в кольцо машины и провозглашают ее своим соседом.

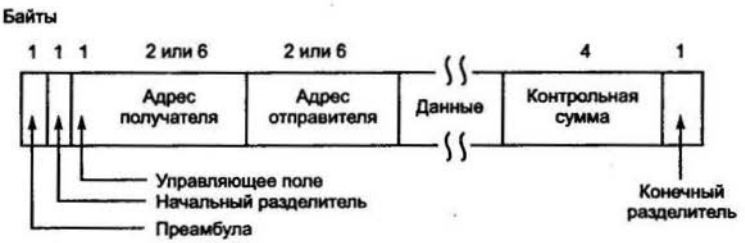

Рис. 4.5. Передаваемый кадр при организации сети маркерной шиной

При выходе из кольца некой станции она посылает своему предшественнику кадр, информирующий его о том, что с этого момента вместо нее будет ее преемник. После чего она прекращает передачу.

Если некая станция выходит из строя, то если ее преемник не начал передавать кадры и не передал маркер дальше, маркер посылается еще раз. Если и после этого станция-преемник не ответила, то посылается широковещательный запрос с информацией об адресе преемника и о станции, которая должна быть следующей. Когда некая станция видит этот запрос с адресом своего предшественника, она широковещательным ответом провозглашает преемником себя, и вышедшая из строя станция удаляется из кольца.

Если станция выбывает из кольца вместе с маркером, то происходит инициализация кольца заново.

4.5. Сети на основе маркерного кольца

Локальные сети на основе **маркерного кольца (Token Ring)** строятся на кольцевой архитектуре, что подразумевает индивидуальные соединения «точка—точка». Управляющая станция генерирует специальное сообщение — маркер (token) и последовательно передает его всем компьютерам. Правом передачи данных обладает единственный компьютер, располагающий маркером. Как только маркер достигает станции, которая собирается передавать данные, последняя «присваивает» маркер себе и изменяет его статус на «занято». Затем маркер дополняется всей информацией, которую предполагалось передать, и снова отправляется в сеть. Маркер будет циркулировать в сети до тех пор, пока не достигнет адресата информации. Получающая сторона обрабатывает полученную вместе с маркером информацию и опять передает маркер в сеть. Когда маркер возвращается к исходной станции, он удаляется, после чего генерируется новый маркер. Циркуляция начинается заново (рис. 4.6).

Серьезным недостатком такого типа построения сетей является то, что разрыв кабеля в одной точке приводит к полной остановке работоспособности сети.

На основе маркерного кольца строятся локальные сети Token Ring. В настоящее время существует две разновидности этого типа сетей с пропускной способностью 4 и 16 Мбит/с.

Одним из важнейших параметров сети является **время реакции** на запрос пользователя ($T_р$) — промежуток времени между моментом готовности подать запрос в сеть и моментом получе-

Рис. 4.6. Структура сети на основе маркерного кольца

ния ответа на запрос, т. е. возвращения отправленного кадра, что является подтверждением в получении этого кадра адресатом

$$T_{\text{р}} = T_{\text{ож}} + T_{\text{обсл}}, \qquad (3.1)$$

где $T_{\text{ож}}$ — максимальное время ожидания подачи кадра; $T_{\text{обсл}}$ — время обслуживания запроса.

С учетом того, что

$$T_{\text{ож}} = (N_{\text{рс}} - 1)T_{\text{об}},$$

где $N_{\text{рс}}$ — количество рабочих станций; $T_{\text{об}}$ — время, в течение которого маркер вместе с кадром совершает полный оборот в моноканале, и

$$T_{\text{об}} = T_{\text{с}} + T_{\text{к}} + T_{\text{сз}}, \qquad (3.2)$$

где $T_{\text{с}}$ — время распространения сигнала в передающей среде через весь моноканал; $T_{\text{к}}$ — время передачи кадра через моноканал; $T_{\text{сз}}$ — время задержки передаваемого кадра по кольцу в узлах сети и, исходя из того, что

$$T_{\text{с}} = S_{\text{к}}/V_{\text{с}}; \quad T_{\text{к}} = C_{\text{к}}/V_{\text{к}}; \quad T_{\text{сз}} = N_{\text{рс}}T_{\text{з}},$$

где $S_{\text{к}}$ — длина кольцевого моноканала; $V_{\text{с}}$ — скорость распространения сигнала; $C_{\text{к}}$ — длина маркера и кадра; $V_{\text{к}}$ — скорость

передачи данных; $T_з$ — время задержки маркера и кадра узлом, получаем

$$T_{об} = S_к/V_с + C_к/V_к + N_{рс}T_з \quad (3.3)$$

и

$$T_{ож} = (N_{рс} - 1)(S_к/V_с + C_к/V_к + N_{рс}T_з).$$

Тогда с учетом формул (3.1) и (3.3) имеем

$$T_р = (N_{рс} - 1)(S_к/V_с + C_к/V_к + N_{рс}T_з) + T_{обсл}. \quad (3.4)$$

Пример 3.1. Определить время реакции на запрос пользователя в локальной сети, построенной на топологии «маркерное кольцо», если известно, что $N_{рс} = 25$, $S_к = 12{,}5$ м, $V_с = 50\,000$ км/с, $C_к = 512$ байт, $V_к = 4$ Мбит/с, $T_з = 1500$ мкс — скорость передачи кадра по моноканалу.

Предполагая, что $T_{обсл} = T_{об}$, и пользуясь формулами (3.3) и (3.4), получаем

$$T_р = (N_{рс} - 1)(S_к/V_с + C_к/V_к + N_{рс}T_з) + (S_к/V_с + C_к/V_к + N_{рс}T_з) =$$

$$= N_{рс}(S_к/V_с + C_к/V_к + N_{рс}T_з) = 969\,350 \text{ мкс}.$$

4.6. Сети FDDI

FDDI (Fiber Distributed Data Interface — распределенный интерфейс передачи данных по волоконно-оптическим каналам) является высокоскоростной волоконно-оптической системой со скоростью передачи данных 100 Мбит/с. Сеть поддерживает метод доступа маркерное кольцо, но в отличие от Token Ring, система FDDI использует для передачи данных не одно кольцо, а два, передача информации по которым осуществляется в противоположных направлениях, причем второе кольцо является резервным (рис. 4.7, *а*).

В случае разрыва по каким-либо причинам первого кольца информация считываться со второго, что увеличивает надежность работоспособности сети. Если произошел разрыв сразу обоих колец в одном и том же месте, т. е. возможность с по-

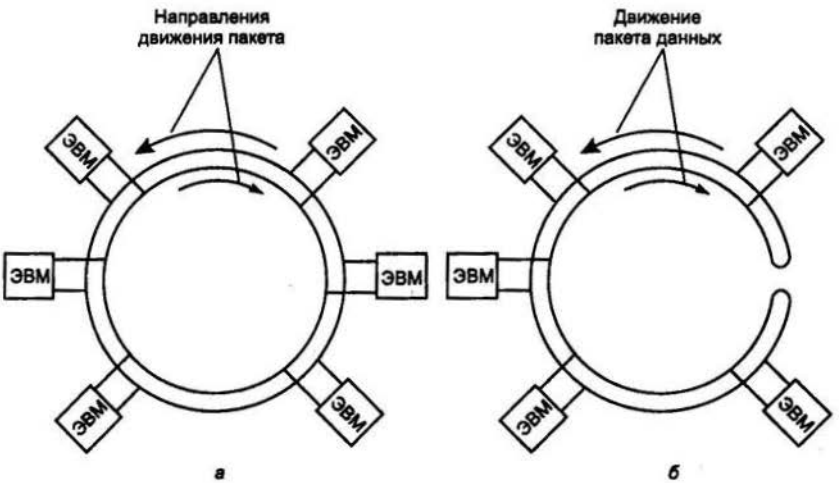

Рис 4.7. Структура сети FDDI:
а — обычная передача данных; *б* — передача данных при разрыве канала связи

мощью специальных переключателей объединить два кольца в одно (рис. 4.7, *б*).

В настоящее время разрабатывается модель сети, предполагающая возможность передавать различную информацию по двум кольцам одновременно, делая оба кольца основными. При этом пропускная способность такой системы увеличивается в 2 раза без уменьшения надежности ее работы.

4.7. Высокоскоростные локальные сети

В настоящее время в связи с увеличившимися объемами необходимой для передачи информации получили большое развитие сети с пропускной способностью свыше 100 Мбит/с. К таким сетям относится новое поколение сетей с топологией построения Ethernet — Gigabit Ethernet.

Технология Gigabit Ethernet представляет собой дальнейшее развитие стандартов 802.3 для сетей Ethernet с пропускной способностью 10 и 100 Мбит/с. Она призвана резко повысить скорость передачи данных, сохранив при этом совместимость с существующими сетями Ethernet, использующими метод случайного доступа к ЛВС.

4.8. Общие подходы к выбору топологии сети

В настоящее время наиболее распространенными являются локальные сети Ethernet с электрической средой обмена (10-, 100-base-T). В таких сетях на сегментах с максимальной стандартной длиной критичной по быстродействию и помехозащищенности является сама среда обмена. Поэтому увеличение быстродействия и улучшение помехозащищенности этих сетей становится возможным при переходе от электрической среды обмена к оптической.

В высокоскоростных сетях со средой обмена на волоконной оптике критичным по быстродействию является среда обработки сигналов (оборудование узлов). Увеличение быстродействия таких сетей становится возможным при переходе к следующему поколению элементной базы.

Однако, в случайных методах доступа при большом количестве пользователей наблюдается резкое снижение пропускной способности сети при их попытке одновременно передать сообщения по сети. Устойчивый же доступ к среде обмена при любом количестве пользователей обеспечивают маркерные методы. Поэтому при планировании сети необходимо придерживаться следующих принципов:

- если сеть состоит из небольших сегментов и небольшого количества пользователей, то максимальное быстродействие обеспечит сеть Ethernet с электрической средой передачи данных;
- если сеть состоит из большого количества пользователей и сравнительно небольших сегментов, то устойчивый доступ к сети обеспечат маркерные методы доступа;
- если сеть состоит из сегментов большой длины, то максимальное быстродействие обеспечат сети с оптической средой передачи.

4.9. Структурированные кабельные системы

В последние годы получил развитие новый вид организации промышленной связи — локальные кабельные системы, основанные на изготовлении, поставке, монтаже, сертификации полностью комплектных, стыкующихся со всем сетевым оборудова-

нием, систем проводки и соединений для зданий и сооружений. За этим видом продукции закрепилось название — **структурированные кабельные системы**, базирующиеся на специально разработанных в настоящее время для них стандартах и спецификациях.

Структура типичной кабельной системы, приведенная на рис. 4.8, представляет собой кабель локальной сети, прокладываемый между рабочими станциями и коммутируемый между ними с помощью концентраторов и кроссов. Обычно такое соединение заканчивается стандартным разъемом. Внутри многоэтажного здания прокладывают вертикальные и горизонтальные проводки, последние из которых еще делятся с помощью кроссов. Подобные кабельные системы и называются структурированными.

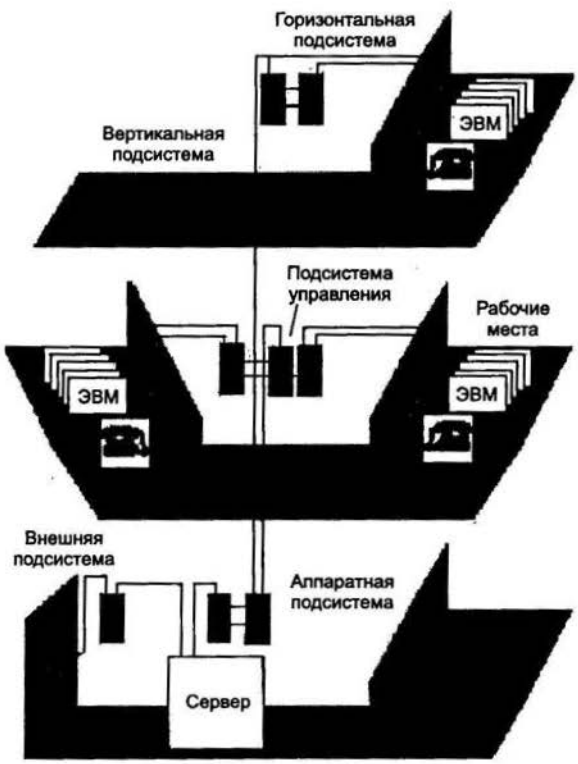

Рис. 4.8. Пример построения структурированной кабельной системы

Основным достоинством таких систем является то, что при перемещении служб и персонала внутри здания из одних помещений в другие изменять структуру проводки не надо. Достаточно аппаратуру из одних помещений перенести в другие и сделать необходимые переключения на кроссировочных панелях, поскольку розетки во всех помещениях однотипные для всех видов сетевого оборудования и телефонии — спецификации RJ-45. Такие системы не требуют каждый раз прокладывать новую проводку и ставить новые розетки, а позволяют использовать при любых переустройствах или перестановках ту сеть, которая капитально смонтирована в здании.

В основу одного соединения в структурированной системе входит стандартный кабель с четырьмя неэкранированными витыми парами, обеспечивающими соединения для компьютеров, телефонии, охранных сигнализаций и др. и позволяющими передавать голос, данные, видео, мультимедиа и графики.

Структурированная кабельная система состоит из следующих подсистем (см. рис. 4.8): рабочего места, предназначенного для подключения компьютеров, терминалов, принтеров, телефонов (факсов) и др.; горизонтальной, предназначенной для организации соединений сетевого оборудования в горизонтальной плоскости (на одном этаже) с помощью витых пар или оптических волокон; управления, состоящей преимущественно из концентраторов и кроссировочного оборудования и предназначенной для объединения и переключения соединительных цепей; вертикальной, обеспечивающей соединение подсистем управления, расположенных на разных этажах; аппаратной, предназначенной для организации связи центральной серверной с локальной или корпоративной сетью; внешней, служащей для соединения между собой сетей, расположенных в различных территориально удаленных зданиях, и базирующейся, как правило, на оптоволоконных соединениях.

В основе построения структурированных систем лежит стандарт TIA/EIA-568 (Commercial building telecommunication wiring standard), разработанный в 1991 г.

Данный стандарт устанавливает следующие требования к горизонтальной проводке:

- длина горизонтальных кабелей не должна превышать 90 м независимо от его типа;
- допускается применение четырех типов кабелей: четырехпарный из неэкранированных витых пар, двухпарный из

экранированных витых пар; каоксиальный, оптический с волокнами размером 62,5/125 мкм;
- типы соединений: модульный восьмиконтактный RJ-45, специальный IBM (IEEE 802.5), коаксиальный BNC, оптический соединитель;
- на каждом рабочем месте должно быть установлено не менее двух соединительных разъемов (один — модульный восьмиконтактный RJ-45, и другой — любой из перечисленных в предыдущем пункте);
- топология сети — «звезда».

Контрольные вопросы

1. Какие сети называют локальными и чем они характеризуются?
2. Что понимают под размерами локальных сетей?
3. В чем основное отличие широковещательной топологии локальной сети от сети с передачей «от точки к точке»?
4. В чем особенности шинной, кольцевой и звездообразной топологии сети?
5. Что понимают под свойством однородности?
6. Дайте определение понятию доступа к сети.
7. Перечислите наиболее распространенные методы доступа к сети.
8. Какие разновидности метода случайного доступа вы знаете?
9. Что понимают под конфликтом в локальной сети?
10. Перечислите маркерные методы доступа и объясните их основные принципы построения.
11. Для чего используется маркер?
12. Какие разновидности сетей Ethernet вы знаете?
13. В чем особенность организации высокоскоростных локальных сетей?

Глава 5
ОРГАНИЗАЦИЯ КОРПОРАТИВНЫХ СЕТЕЙ

5.1. Общие сведения

В настоящее время все большее число компаний испытывают необходимость в организации современных мощных **корпоративных сетей**. Растут требования как к скорости передачи информации (уменьшению времени доступа к сетевым ресурсам, находящимся в различных географических поясах), так и к надежности и защите передаваемых данных. Модульность построения аппаратно-программного обеспечения, новейшие технологии в развитии сетевых технологий и решают эти задачи.

Корпоративной сетью называется сеть, охватывающая большое количество компьютеров и располагающаяся в пределах одного предприятия. Корпоративная сеть соответствует английскому термину «enterprise-wide networks».

В связи с тем, что современные предприятия и их филиалы могут территориально охватывать разные города, страны и даже континенты, их корпоративные сети состоят из десятков и сотен локальных сетей, включающих в себя десятки тысяч компьютеров и сотни серверов, для объединения которых используются глобальные сети посредством организации связи с помощью телефонии, спутниковых и радиоканалов. Пример построения корпоративной сети представлен на рис. 5.1.

Для управления доступом к ресурсам таких сетей обычно используют единые базы учетных записей пользователей, которые позволяют получать доступ к ресурсам всей сети из разных частей предприятия и избавляют администраторов сети от дополнительной необходимости дублировать одно и то же пользовательское имя на нескольких серверах локальных сетей.

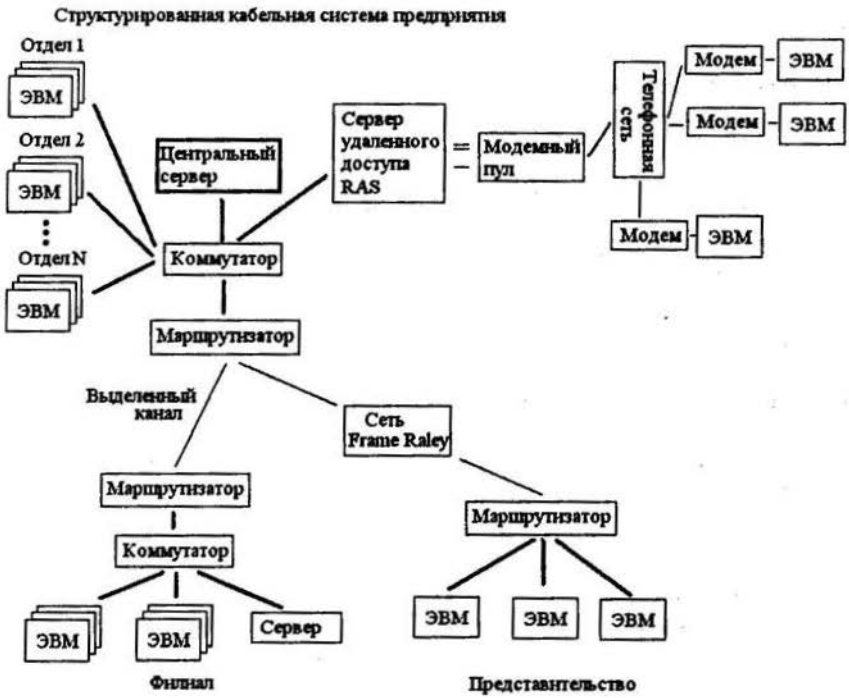

Рис. 5.1. Пример построения корпоративной сети

Одной из важнейших характеристик корпоративных сетей является их **гетерогенность**, т. е. способность обеспечивать обмен информацией компьютеров, имеющих различную коммуникационную и аппаратную конфигурацию, а также программное обеспечение.

Кроме того, оптимальность выбора маршрута от отправителя к получателю влияет на скорость передачи информации, что является «узким» местом в современных сетях, за счет своей низкой скорости передачи информации и качества сетей. Чтобы передаваемому кадру добраться до пункта назначения, ему может потребоваться преодолеть несколько транзитных участков между маршрутизаторами. Для решения этой задачи транспортный уровень располагает информацией о топологии сети.

Как уже указывалось ранее, существует два варианта организации работы сетевого уровня: с использованием **соединений**, а другой — **без соединений**. В контексте внутреннего устройства

подсети соединение обычно называют **виртуальным каналом**. Независимые пакеты в системе без установления соединений называются **дейтаграммами**.

Виртуальные каналы организованы таким образом, что для каждого посылаемого пакета не нужно выбирать маршрут заново. Этот маршрут используется для всех данных, передаваемых за время соединения. При разрыве соединения или выходе из строя маршрутизатора виртуальный канал перестает существовать. Таким образом, передаваемые пакеты всегда перемещаются по одному и тому же маршруту. При передаче пакетов указывается номер виртуального канала. Каждый маршрутизатор при такой организации сетевого уровня должен помнить, куда направлять пакеты для каждого из открытых в данный момент виртуальных каналов, для чего, кроме системной информации, маршрутизаторы хранят таблицу виртуальных каналов, проходящих через них.

При организации сетевого уровня без установления соединения, в отличие от виртуальной организации, маршрут для каждой передачи пакета выбирается заново. Перед передачей пакета необходимо рассчитать маршрут пересылки, что приводит к некоторой задержке, особенно в больших корпоративных сетях. Однако, в отличие от виртуального канала, данный способ организации более гибкий и позволяет легче приспосабливаться к неисправностям и заторам передачи данных. При передаче данных используются адреса получателя, которые при увеличении сетей становятся довольно длинными, до нескольких байтов. Маршрутизаторы при такой организации сети хранят номера входных и выходных линий для пунктов назначения пакетов.

5.2. Алгоритмы маршрутизации

Алгоритм маршрутизации — совокупность действий, которая выполняется активными компонентами сети для того, чтобы обеспечить возможность корректной доставки данных абонентам данной сети.

В сложных сетях всегда существует несколько альтернативных маршрутов для передачи пакетов между двумя станциями. Под **маршрутом** будем понимать последовательность маршрутизаторов, которую должен пройти пакет от станции отправителя до станции получателя.

При выполнении алгоритма маршрутизации узел должен получать информацию от соседних узлов, выполняющих такой же алгоритм маршрутизации, о сетях, которые могут быть достижимы при передаче данных через каждый соседний узел (рис. 5.2). Концентрируя такую информацию в так называемых таблицах маршрутизации, каждый узел может определить направление — маршрут передачи данных для каждой из доступных сетей. В том случае, если таких маршрутов оказалось несколько, алгоритм маршрутизации предусматривает возможность использования специального критерия для выбора оптимального маршрута — например, задержка прохождения маршрута отдельным пакетом, количество пройденных промежуточных маршрутизаторов и др. Чтобы по адресу назначения в сети можно было выбрать маршрут движения пакета, каждая станция анализирует таблицу маршрутизации.

Таблица маршрутизации представляет собой некую базу данных составных элементов сети (сетевых адресов маршрутизаторов, сетей, расстояние до сети назначения, флаг канала и др.).

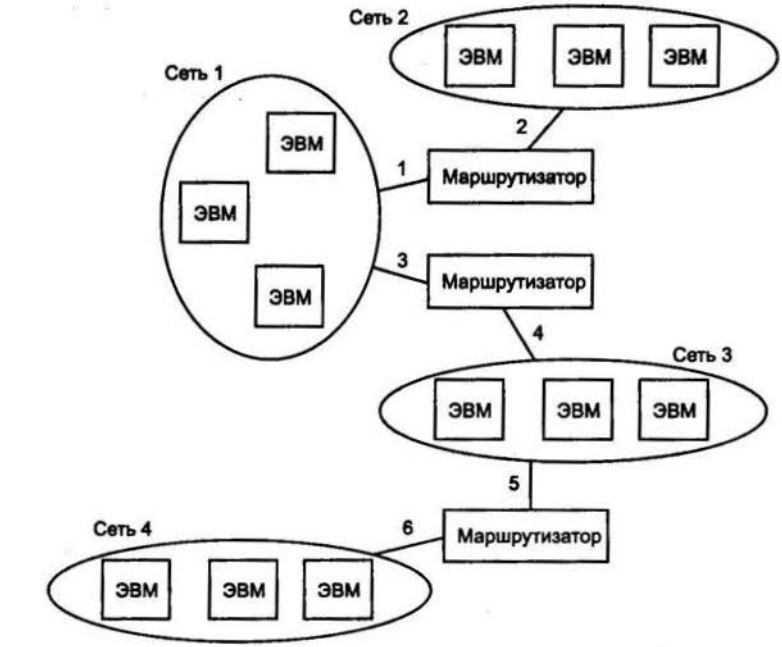

Рис. 5.2. Пример маршрутизации

Флаг U свидетельствует о том, что маршрут в настоящее время занят.

Таблица маршрутизации строится и для станций сети, передающих и принимающих пакеты, и для самих маршрутизаторов, отвечающих за пересылку пакетов между различными сетями.

Когда на маршрутизатор поступает новый пакет, из него извлекается адрес сети, который сравнивается с адресами сети в таблице маршрутизации. Строка с совпавшим адресом указывает, на какой ближайший маршрутизатор следует направить пакет.

С увеличением количества маршрутизаторов, а следовательно, и числа подсетей в больших корпоративных сетях, число записей в таблице маршрутизации также увеличивается. Это приводит к возрастанию времени поиска в ней нужной информации, что в свою очередь уменьшает скорость передачи данных и приводит к снижению пропускной способности сети в целом. Рациональным решением данной проблемы является следующий принцип построения таблицы: в нее вносятся только адреса маршрутизаторов, связывающих данную сеть с «соседними» сетями, а все остальные сети идентифицируются в таблице специальной записью — «маршрутизатор по умолчанию», через который пролегает путь ко всем остальным сетям. Пример построения таблицы маршрутизации для сети 1 (см. рис. 5.2) представлен в табл. 5.1

Таблица 5.1. **Пример построения таблицы маршрутизации**

Наименование сети — получателя пакета	Адрес маршрутизатора	Расстояние до сети получателя	Флаг состояния канала
Сеть 2	1	1	U
По умолчанию	3	—	

В зависимости от способа, который используется для обеспечения обмена информацией о маршрутах в сети между узлами при выполнении алгоритма маршрутизации, различают два типа протоколов маршрутизации:

- протоколы **distant vector**, предусматривающие передачу информации о маршрутах периодически, через установленные интервалы времени. Одним из примеров реализации такой технологии является протокол маршрутизации RIP (Routing Information Protocol), применяемый в сетях небольшого размера;

- протоколы **link state**, предусматривающие передачу информации о маршрутах в момент первоначального включения или возникновения изменений в структуре информационных каналов.

Прежде чем пакет будет передан через сеть, необходимо установить **виртуальное соединение** между абонентами сети. Существует два типа виртуальных соединений — коммутируемый виртуальный канал (Switched Virtual Circuit — SVC) и постоянный виртуальный канал (Permanent Virtual Circuit — PVC). При создании коммутируемого виртуального канала коммутаторы сети настраиваются на передачу пакетов динамически, по запросу абонента, а создание постоянного виртуального канала происходит заранее.

Необходимость создания виртуальных каналов заключается в том, что маршрутизация пакетов между коммутаторами сети на основании таблиц коммутации происходит только один раз — при создании виртуального канала. После создания виртуального канала передача пакетов коммутации происходит на основании идентификаторов виртуальных каналов.

5.3. Уровни и протоколы

Диспетчер ввода/вывода, через который осуществляется доступ к сетевой среде, включает в себя большинство сетевых компонентов. Они организованы в несколько уровней (рис. 5.3):

- **драйверы плат сетевого адаптера**, совместимые со спецификацией интерфейса сетевых устройств (Network Device Interface Specification — **NDIS**), используя соответствующие сетевые платы и протоколы, соединяют компьютеры под управлением СОС;
- **протоколы** организуют надежную передачу данных между компьютерами в сети.

Драйверы файловой системы предоставляют приложениям доступ к локальным и удаленным файловым ресурсам, например сетевым принтерам.

Драйвер — это программа, непосредственно взаимодействующая с сетевым адаптером. **Модуль** — это программа, взаимодействующая с драйвером, сетевыми прикладными программами или другими модулями. Драйвер сетевого адаптера и, возможно, другие модули, специфичные для физической сети передачи

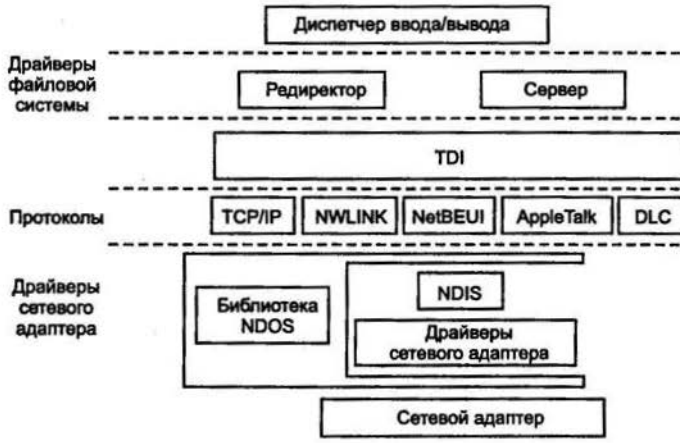

Рис. 5.3. Организация сетевых уровней

данных, предоставляют сетевой интерфейс для протокольных модулей семейства TCP/IP.

Все компоненты общаются через программные интерфейсы, называемые **границами** (boundaries). **Граница** — это унифицированный интерфейс между функциональными уровнями сетевой модели. Появление границ в качестве средств доступа к сетевым уровням открывает сетевые компоненты ОС для сторонних разработчиков и облегчает написание сетевых драйверов и служб. Пограничные слои делают сетевую архитектуру сетевой операционной системы модульной, предоставляя разработчикам базу для создания распределенных приложений. Например, разработчикам транспортных протоколов достаточно реализовать только один уровень, а не всю модель OSI целиком.

5.3.1. Спецификация интерфейса сетевых устройств

Драйверы NDIS-совместимых (Network Device Interface Specification — спецификация интерфейса сетевых устройств) сетевых устройств обеспечивают взаимодействие сетевого адаптера и программного, аппаратного и микропрограммного обеспечения компьютера. Сетевые устройства являются физическим интерфейсом между компьютером и сетевым кабелем.

Каждая сетевая плата может иметь один или несколько драйверов. Чтобы работать и надежно функционировать в ОС, они

должны быть совместимы с данной спецификацией. Эта спецификация обеспечивает независимую привязку одного или более протоколов к одному или более драйверу сетевой платы.

Так как сетевые устройства и их драйверы не зависят от протоколов, смена протокола не требует реконфигурации сетевых устройств.

NDIS определяет программный интерфейс, используемый протоколами для взаимодействия с драйверами сетевых плат. Любой протокол, совместимый с данной спецификацией, может взаимодействовать с любым **NDIS**-совместимым драйвером сетевой платы. Поэтому нет необходимости включать в сам протокол код для работы со специфическими драйверами сетевых адаптеров.

Канал связи между драйвером протокола и драйвером сетевого устройства устанавливается во время **привязки (binding)**.

Спецификация NDIS обеспечивает:

- каналы связи между сетевыми платами и соответствующими драйверами;
- независимость протоколов и драйверов сетевых плат;
- неограниченное число сетевых плат;
- неограниченное число протоколов, привязываемых к одной сетевой плате.

5.3.2. Протоколы

Протоколы организуют связь между двумя или более компьютерами. Некоторые протоколы часто называют транспортными, например TCP/IP, NWLink, NetBEUI и AppleTalk. Протоколы расположены над уровнем интерфейса NDIS.

Существуют следующие виды протоколов.

Transmission Control Protocol/Internet Protocol (TCP/IP). Это маршрутизируемый протокол, поддерживающий глобальные вычислительные сети (Wide Area Network — WAN). Протокол TCP/IP используется в Internet.

NWLink IPX/SPX-совместимый транспорт. Это версия протокола Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX), совместимая со спецификацией NDIS.

NetBEUI. Очень быстрый и эффективный немаршрутизируемый протокол, который в основном полагается на широковещательную передачу и используется в небольших сетях.

Apple Talk. Используется на компьютерах под управлением Windows NT Server совместно с Services for Macintosh для поддержки клиентов Apple Macintosh.

Протокол TCP/IP

Семейство протоколов TCP/IP работает на любых моделях компьютеров, произведенных различными производителями компьютерной техники и работающих под управлением различных операционных систем. С помощью протоколов TCP/IP можно объединить практически любые компьютеры.

Архитектура протоколов TCP/IP предназначена для объединенной сети, состоящей из соединенных друг с другом шлюзами отдельных разнородных пакетных подсетей, к которым подключаются разнородные машины. Каждая из подсетей работает в соответствии со своими специфическими требованиями и имеет свою природу средств связи. Однако предполагается, что каждая подсеть может принять пакет информации (данные с соответствующим сетевым заголовком) и доставить его по указанному адресу в этой конкретной подсети. Не требуется, чтобы подсеть гарантировала обязательную доставку пакетов и имела надежный сквозной протокол. Таким образом, две машины, подключенные к одной подсети, могут обмениваться пакетами.

Сетевой протокол TCP/IP обеспечивает взаимодействие компьютеров с различными архитектурами и ОС через взаимосвязанные сети. TCP/IP — это гибкий стек протоколов, созданных для глобальных вычислительных сетей (**ГВС**), легко адаптируемый к широкому спектру сетевого оборудования. TCP/IP можно применять для взаимодействия с системами на основе Windows NT, с устройствами, использующими другие сетевые продукты, с системами других фирм, например с UNIX-системами.

TCP/IP — это маршрутизируемый сетевой протокол, предоставляющий такие средства как:

- стандартный маршрутизируемый корпоративный сетевой протокол;
- архитектура, облегчающая взаимодействия в гетерогенных средах;
- доступ к Internet и его ресурсам.

Каждый компьютер в сети TCP/IP имеет адреса трех уровней.

1. Локальный адрес узла, определяемый технологией, с помощью которой построена отдельная сеть, в которую входит

данный узел. Для узлов, входящих в локальные сети, это MAC-адрес сетевого адаптера или порта маршрутизатора, например 23-B4-65-7C-DC-11. Эти адреса назначаются производителями оборудования и являются уникальными адресами, так как управляются централизованно. Для всех существующих технологий локальных сетей MAC-адрес имеет формат 6 байтов: старшие 3 байта — идентификатор фирмы производителя, а младшие 3 байта назначаются уникальным образом самим производителем. Для узлов, входящих в глобальные сети, такие как X.25 или frame relay, локальный адрес назначается администратором глобальной сети.

2. IP-адрес, состоящий из 4 байт, например 192.15.0.30. Этот адрес используется на сетевом уровне и назначается администратором во время конфигурирования компьютеров и маршрутизаторов.

3. Символьный идентификатор-имя, например:

COMP21.AUD221.COM, также назначаемый администратором. Его также называют DNS-именем.

TCP/IP — это стек протоколов, созданный для межсетевого обмена. На рис. 5.4 представлена структура протокола **TCP/IP**.

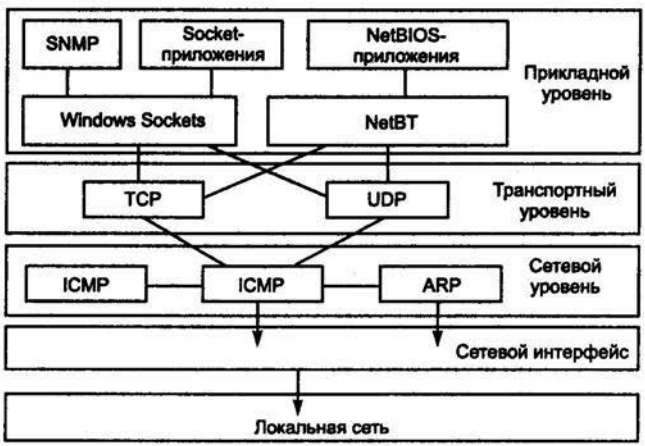

Рис. 5.4. Стек протоколов TCP/IP

В **SNMP** (Simple Network Management Protocol) содержатся данные мониторинга MIB (Management Information Base). **Windows Sockets (WinSock)** — стандартный интерфейс между socket-приложениями и протоколами TCP/IP.

NetBT (NetBIOS над TCP/IP) — службы NetBIOS, в том числе службы имен, дейтаграмм и сессий. Также предоставляет стандартный интерфейс между NetBIOS-приложениями и протоколами TCP/IP.

Протокол **TCP** (Transmission Control Protocol) представляет гарантированную доставку пакетов с установлением соединения.

Протокол **UDP** (User Datagram Protocol) представляет негарантированную доставку пакетов без установления соединения. Протоколы TCP и UDP предоставляют разные услуги прикладным процессам. Большинство прикладных программ пользуются только одним из них. Если вам нужна надежная и эффективная доставка по длинному и ненадежному каналу передачи данных, то лучшим может быть TCP. Если вам нужна доставка дейтаграмм и высокая эффективность на быстрых сетях с короткими соединениями, то лучше может быть UDP. Если ваши потребности не попадают ни в одну из этих категорий, то выбор транспортного протокола не ясен. Однако прикладные программы могут устранять недостатки выбранного протокола. Если вы выбрали TCP, а вам нужно передавать записи, то прикладная программа должна вставлять маркеры в поток байтов так, чтобы можно было различить записи.

Протокол **ICMP** (Internet Control Message Protocol) обеспечивает специальную связь между хостами (host — главный компьютер, ведущий узел), отчет о сообщениях и ошибках доставки пакетов.

Протокол **IP** (Internet Protocol) выполняет функции адресации и маршрутизации.

Протокол **ARP** (Address Resolution Protocol) осуществляет отображение адресов IP в адреса подуровня управления доступом к среде передачи. Адрес IP обязателен для каждого компьютера, использующего TCP/IP. Он представляет собой логический 32-разрядный адрес, применяемый для идентификации TCP/IP-хоста. Подуровень управления доступом к среде передачи напрямую взаимодействует с сетевой платой и отвечает за безошибочную передачу данных между двумя компьютерами в сети. Другими словами, протокол ARP служит для определения локального адреса устройства по IP-адресу передаваемого пакета. Существует также протокол, решающий обратную задачу, — нахождение IP-адреса по известному локальному адресу — RARP (Reverse Address Resolution Protocol — реверсивный ARP).

Основные параметры протокола TCP/IP

Логический 32-разрядный **IP-адрес** — адрес, используемый для идентификации TCP/IP-хоста, состоит из двух частей: идентификатора сети и идентификатора хоста и имеет длину 4 байта — первая часть определяет номер сети, вторая — номер узла в сети. Каждый компьютер, использующий протокол TCP/IP, должен иметь уникальный адрес IP, например 10.0.0.2.

Подсеть — это сеть в многосетевой среде, использующая адреса IP с общим идентификатором сети. Применяя подсети, организация может разделить одну большую сеть на несколько физических сетей и соединить их маршрутизаторами. Для разбиения IP-адреса на идентификаторы сети и хоста служит маска подсети. При попытке соединения TCP/IP с помощью маски подсети определяет, находится ли целевой хост в локальной или удаленной сети. Пример маски подсети — 255.255.0.0. Чтобы взаимодействовать напрямую, компьютеры в сети должны иметь одинаковую маску подсети.

Чтобы действовала связь с хостом из другой сети, должен быть указан IP-адрес основного шлюза. Если на локальном хосте не указан маршрут до целевой сети, то TCP/IP посылает пакеты для удаленных сетей на **основной шлюз**. Если он не указан, связь будет ограничена только локальной сетью (подсетью). Например, адрес основного шлюза может быть 157.0.2.2.

Компьютеры IP-сетей обмениваются между собой информацией, используя в качестве адресов 4-байтные коды, которые принято представлять соответствующей комбинацией десятичных чисел, напоминающей нумерацию абонентов в телефонии, например 157.104.15.15. Это означает, что каждое из четырех чисел в IP адресе больше или равно 0 и меньше или равно 255. Как можно увидеть на приведенном примере, числа условно отделяются друг от друга точками.

Протокол NWLink

Протокол NWLink IPX/SPX Compatible Transport — это разработанная Microsoft 32-разрядная NDIS 4.0-совместимая версия протокола IPX/SPX (Internetwork Packet Exchange/ Sequenced Packet Exchange) фирмы Novell.

NWLink чаще всего применяется в сетевых средах, где компьютеры должны иметь доступ к клиент-серверным приложени-

ям, выполняющимся на сервере Novell NetWare, или, наоборот, клиенты Novell должны обращаться к приложениям Windows NT. NWLink позволяет компьютерам под управлением Windows NT взаимодействовать с другими сетевыми устройствами, использующими IPX/SPX, такими как принтер-серверы. Протокол NWLink подходит и для малых сетевых сред, состоящих только из Windows NT и клиентов Microsoft.

NWLink поддерживает следующие сетевые протоколы API, обеспечивающие функции IPC:

- WinSock (Windows Sockets) поддерживает существующие Novell-приложения, написанные в соответствии с интерфейсом NetWare IPX/SPX Sockets. WinSock обычно используется для связи с NetWare Loadable Modules (NLM). Заказчики, реализующие клиент-серверные решения с помощью модулей NLM, могут перенести их в среду Windows NT Server и сохранить при этом совместимость со своими клиентами;
- NetBIOS над IPX, реализованный в виде NWLink NetBIOS, поддерживает взаимодействие между рабочими станциями Novell, применяющими NetBIOS, и компьютерами с Windows NT, использующими NWLink NetBIOS.

При установке и конфигурировании NWLink IPX/SPX необходимо указать тип пакетов и номер сети. Тип пакетов определяет способ, по которому сетевая плата будет форматировать данные для отправки по сети. Многие операционные системы позволяют автоматически определять тип передаваемых пакетов.

Протокол NetBEUI

Протокол NetBEUI (NetBIOS Extended User Interface) разработан для небольших локальных вычислительных сетей (ЛВС), состоящих из 20—200 компьютеров. Так как этот протокол немаршрутизируемый, он не подходит для глобальных сетей.

NetBEUI обеспечивает совместимость с существующими ЛВС, в которых применяется протокол NetBEUI, и обеспечивает взаимодействие со старыми сетевыми системами, такими как Microsoft LAN Manager и Microsoft Windows.

Протокол NetBEUI реализует следующие возможности: связь между компьютерами с установлением или без установления соединения; автоматическую настройку; защиту от ошибок; невысокие требования к памяти.

Так как NetBEUI полагается на широковещательную передачу при выполнении многих функций, например, при обнаружении и регистрации имен, его применение приводит к увеличению широковещательного трафика по сравнению с другими протоколами.

Transport Driver Interface

Transport Driver Interface (TDI) — пограничный слой, предоставляющий общий программный интерфейс взаимодействия транспортных протоколов с драйверами файловой системы, такими как служба Workstation (Рабочая станция) — редиректор — или служба Server (Сервер). TDI обеспечивает их независимость друг от друга.

Так как TDI обеспечивает независимость сетевых компонентов друг от друга, можно добавлять, удалять или менять протоколы, не перенастраивая всю сетевую подсистему узла.

Драйверы файловой системы

Драйверы файловой системы служат для доступа к файлам. Всякий раз, когда вы делаете запрос на чтение или запись файла, в работу включается драйвер файловой системы. Несколько основных сетевых компонентов реализованы в виде драйверов файловой системы, например службы Workstation (Рабочая станция) и Server (Сервер).

Редиректор

Диспетчер ввода/вывода определяет, кому адресован запрос на ввод/вывод: локальному диску или сетевому ресурсу. Если последнему, редиректор перехватывает запрос и посылает (перенаправляет) его соответствующему сетевому ресурсу. **Редиректор** (RDR) — это компонент, расположенный над TDI и взаимодействующий с транспортными протоколами средствами TDI. Редиректор обеспечивает подсоединение к Windows for Workgroups, LAN Manager LAN Server и другим сетевым серверам Microsoft.

Редиректор реализован в виде драйвера. Это дает следующие преимущества:

- приложения могут применять Windows NT API ввода/вывода для доступа к файлам как на локальном, так и на удаленном компьютере. С точки зрения диспетчера ввода/вывода, нет никакой разницы между обращением к файлам

на локальном жестком диске и использованием редиректора для доступа к файлам на удаленном компьютере в сети;
- редиректор может выполняться в режиме ядра и напрямую вызывать другие драйверы и компоненты, такие как диспетчер кэша, повышая таким образом производительность;
- редиректор, как любой драйвер файловой системы, можно динамически загружать и выгружать;
- редиректор COC может сосуществовать с редиректорами сторонних производителей.

Сервер

Вторым компонентом сети является служба **Server** (Сервер). Как и редиректор, она располагается над TDI, реализована в виде драйвера файловой системы и напрямую взаимодействует с другими драйверами файловой системы, выполняя запросы на чтение и запись.

Server предоставляет соединения, запрашиваемые клиентскими редиректорами, и обеспечивает доступ к требуемым ресурсам.

Когда эта служба получает от удаленного компьютера запрос на чтение файла, который расположен на локальном диске сервера, происходит следующее:
- сетевые драйверы нижнего уровня получают запрос и передают его Server;
- Server передает запрос на чтение файла соответствующему локальному драйверу файловой системы;
- для доступа к файлу этот драйвер вызывает низкоуровневые драйверы дисков;
- данные от них передаются локальному драйверу файловой системы;
- тот передает их обратно Server; служба передает их низкоуровневому сетевому драйверу, который обеспечивает доставку данных до машины-клиента.

5.4. Адресация компьютеров в Internet

Под **Internet** подразумевается совокупность сетей, базирующихся на IP-технологии обмена данными (IP — Internet Protocol) и обеспечивающих пользователям наивысшую степень

удобства на коммутируемых или выделенных линиях: максимально высокие скорости, работу с электронной почтой и предоставление самых современных услуг, в числе которых центральное место занимает **WWW-технология** (World Wide Web — Всемирная информационная паутина).

Каждый узел в объединенной сети, как указывалось выше, должен иметь свой уникальный IP-адрес, состоящий из двух частей — номера сети и номера узла. Какая часть адреса относится к номеру сети, а какая к номеру узла, определяется значениями первых битов адреса.

Если адрес начинается с 0, то сеть относят к классу A, и номер сети занимает один байт, а остальные 3 байта интерпретируются как номер узла в сети. Сети класса A имеют номера в диапазоне от 1 до 126 (см. рис. 5.5). В таких сетях количество узлов должно быть больше 216, но не превышать 224.

Если первые два бита адреса равны 1, то сеть относится к классу B и является сетью средних размеров с числом узлов 28—216.

Если адрес начинается с последовательности 110, то это сеть класса C с числом узлов не больше 28 (см. рис. 5.5).

Если адрес начинается с последовательности 1110, то он является адресом класса D и обозначает особый, групповой адрес — multicast. Если в пакете в качестве адреса назначения указан адрес класса D, то такой пакет должны получить все узлы, которые образуют группу с номером, указанным в поле адреса.

Если адрес начинается с последовательности 11110, то это адрес класса E, он зарезервирован для будущих применений (рис. 5.5).

В общем случае, такие числовые адреса могут иметь некоторое разнообразие трактовок, из которых приведем здесь следующую:

<класс сети><номер сети><номер компьютера>.

Такая комбинация подразумевает, что множество представимых числовых номеров делится на сети разного масштаба (рис. 5.5, 5.6).

С помощью специального механизма маскирования любая сеть, в свою очередь, может быть представлена набором более мелких сетей.

Рис. 5.5. Классы адресов Internet

Класс	Диапазон
A	**0**.0.0.0 — **127**.255.255.255
B	**128**.0.0.0 — **191**.255.255.255
C	**192**.0.0.0 — **223**.255.255.255
D	**224**.0.0.0 — **239**.255.255.255
E	**240**.0.0.0 — **247**.255.255.255

Рис. 5.6. Диапазоны IP-адресов в разных классах сетей

Определение номеров сети по первым байтам адреса — не вполне гибкий механизм для адресации. На сегодняшний день получили широкое распространение маски. Маска — это тоже 32-разрядное число, она имеет такой же вид, как и IP-адрес. Маска используется в паре с IP-адресом, но не совпадает с ним.

Принцип определения номера сети и номера узла IP-адреса с использованием маски состоит в следующем: двоичная запись маски содержит единицы в тех разрядах, которые в IP-адресе должны представляться как номер сети и нули в тех разрядах, которые представляются как номер хоста. Кроме того, поскольку номер сети является целой частью адреса, единицы в маске должны представлять непрерывную последовательность.

Каждый класс IP-адресов (A, B, C) имеет свою маску, используемую по умолчанию:

Класс A — 11111111.00000000.00000000.00000000 (255.0.0.0);

Класс B — 11111111.11111111.00000000.00000000 (255.255.0.0);

Класс C — 11111111.11111111.11111111.00000000 (255.255.255.0);

Например, если адресу 190.215.124.30 задать маску 255.255.255.0, то номер сети будет 190.215.124.0, а не 190.215.0.0, как это определяется правилами системы классов.

С ростом объемов информации в Internet увеличилось и количество его узлов. В результате путешествие по глобальной сети с помощью адресов, представленных в виде чисел, стало неудобным. На смену им пришли так называемые **доменные имена**.

Домен (domain) — территория, область, сфера — фрагмент, описывающий адрес в текстовой форме. Адрес конечного узла представляется в виде не цифрового кода, как было указано выше, а в виде набора текстовой информации формата:

domain4.domain3.domain2.domain1,

где domain1 — буквенное обозначение страны, например ru, eng и др., или одной из следующих спецификаций:

com — коммерческие организации;

edu — учебные и научные организации;

gov — правительственные организации;

mil — военные организации;

net — сетевые организации разных сетей;

org — другие организации;

domain4, domain3, domain2 описывают, как правило, более низшие уровни адреса, например наименование города, отдела, раздела и т. д.

DNS (Domain Name System) — это распределенная база данных, поддерживающая иерархическую систему имен для идентификации узлов в сети Internet. Служба DNS предназначена для автоматического поиска IP-адреса по известному символьному имени узла. Спецификация DNS определяется стандартами RFC 1034 и 1035. DNS требует статической конфигурации своих таблиц, отображающих имена компьютеров в IP-адрес.

Протокол DNS является служебным протоколом прикладного уровня. Этот протокол несимметричен — в нем определены DNS-серверы и DNS-клиенты. DNS-серверы хранят часть распределенной базы данных о соответствии символьных имен и IP-адресов. Эта база данных распределена по административным

доменам сети Internet. Клиенты сервера DNS знают IP-адрес сервера DNS своего административного домена и по протоколу IP передают запрос, в котором сообщают известное символьное имя и просят вернуть соответствующий ему IP-адрес.

Если данные о запрошенном соответствии хранятся в базе данного DNS-сервера, то он сразу посылает ответ клиенту, если же нет, то он посылает запрос DNS-серверу другого домена, который может сам обработать запрос либо передать его другому DNS-серверу. Все DNS-серверы соединены иерархически, в соответствии с иерархией доменов сети Internet. Клиент опрашивает эти серверы имен, пока не найдет нужные отображения. Этот процесс ускоряется из-за того, что серверы имен постоянно кэшируют информацию, предоставляемую по запросам. Клиентские компьютеры могут использовать в своей работе IP-адреса нескольких DNS-серверов для повышения надежности своей работы.

Каждый домен DNS администрируется отдельной организацией, которая обычно разбивает свой домен на поддомены и передает функции администрирования этих поддоменов другим организациям. Каждый домен имеет уникальное имя, а каждый из поддоменов имеет уникальное имя внутри своего домена. Имя домена может содержать до 63 символов. Каждый хост в сети Internet однозначно определяется своим *полным доменным именем (fully qualified domain name — FQDN)*, которое включает имена всех доменов по направлению от хоста к корню. Пример полного DNS-имени:

citint.dol.ru.

Номера сетей назначаются либо централизованно, если сеть является частью Internet, либо произвольно, если сеть работает автономно. Номера узлов и в том и в другом случае администратор волен назначать по своему усмотрению, не выходя, разумеется, из разрешенного для этого класса сети диапазона.

Координирующую роль в централизованном распределении IP-адресов до некоторого времени играла организация InterNIC, однако с ростом сети задача распределения адресов стала слишком сложной, и InterNIC делегировала часть своих функций другим организациям и крупным поставщикам услуг Internet.

Уже сравнительно давно наблюдается дефицит IP-адресов. Очень трудно получить адрес класса B и практически невозможно стать обладателем адреса класса A. При этом надо отметить,

что дефицит обусловлен не только ростом сетей, но и тем, что имеющееся множество IP-адресов используется нерационально. Очень часто владельцы сети класса С расходуют лишь небольшую часть из имеющихся у них 254 адресов.

Для смягчения проблемы дефицита адресов разработчики стека TCP/IP предлагают разные подходы. Принципиальным решением является переход на новую версию IPv6, в которой резко расширяется адресное пространство за счет использования 16-байтовых адресов. Однако и текущая версия IPv4 поддерживает некоторые технологии, направленные на более экономное расходование IP-адресов. Одной из таких технологий является технология *масок* и ее развитие — технология *бесклассовой междоменной маршрутизации (Classless Inker-Domain Routing — CIDR)*. Технология CIDR отказывается от традиционной концепции разделения адресов протокола IP на классы, что позволяет получать в пользование столько адресов, сколько реально необходимо. Благодаря CIDR поставщик услуг получает возможность «нарезать» блоки из выделенного ему адресного пространства в точном соответствии с требованиями каждого клиента, при этом у него остается пространство для маневра на случай его будущего роста.

5.5. Службы обмена данными

5.5.1. Сети X.25

Сети **X.25** являются на сегодняшний день самыми распространенными сетями с коммутацией пакетов, используемыми для построения корпоративных сетей.

Данные сети могут работать на ненадежных линиях передачи информации благодаря протоколам с установлением соединения и коррекцией ошибок на двух уровнях — канальном и сетевом.

Сети X.25 базируются на следующих основополагающих принципах организации, отличающих их от других:

- наличие в структуре сети специального устройства — PAD (Packet Assembler Disassembler), предназначенного для выполнения операции сборки нескольких низкоскоростных потоков байт от алфавитно-цифровых терминалов в пакеты, передаваемые по сети и направляемые компьютерам для обработки;

- наличие трехуровневого стека протоколов с использованием на канальном и сетевом уровнях протоколов с установлением соединения, управляющих потоками данных и исправляющих ошибки;
- ориентация на однородные стеки транспортных протоколов во всех узлах сети — сетевой уровень рассчитан на работу только с одним протоколом канального уровня и не может подобно протоколу IP объединять разнородные сети.

Дополнительными устройствами в сети X.25 являются также коммутаторы (центры коммутации пакетов), расположенные в различных географических областях и соединенные высокоскоростными каналами связи, обеспечивающими обмен данными между ними (рис. 5.7).

Рис. 5.7. Структура построения сети X.25

5.5.2. Уровень передачи данных ATM

Технология передачи данных **ATM** (Asynchronous Transfer Mode — асинхронный режим передачи) основана на передаче данных пакетами фиксированной длины размером 53 байта (рис. 5.8).

Сети ATM предполагают передачу данных при установленном соединении, т. е. сначала устанавливается соединение меж-

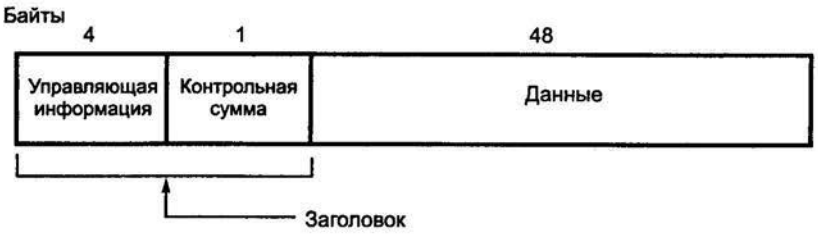

Рис. 5.8. Формат пакета данных ATM

ду источником информации и приемником и только затем начинается передача пакетов данных, после чего соединение разрывается.

5.5.3. Сети SDH

Появление стандартов синхронной цифровой иерархии передачи данных (SDH) в 1988 году ознаменовало собой новый этап развития транспортных сетей. Технология SDH широко используется для организации надежной передачи данных. SDH была разработана для того, чтобы получить стандартный протокол для взаимодействия **провайдеров** — поставщиков сетевых услуг; унифицировать американские, европейские и японские цифровые системы; обеспечить мультиплексирование цифровых сигналов на гигабитных скоростях; обеспечить поддержку функций эксплуатации и технического обслуживания OA&M (operation, administration and maintenance — функционирование, администрирование и техническое обслуживание).

Системы синхронной передачи не только преодолели ограничения систем-предшественниц (PDH), но и снизили накладные расходы на передачу информации. Ряд уникальных достоинств — доступ к низкоскоростным каналам без полного демультиплексирования всего потока, высокая отказоустойчивость, развитые средства мониторинга и управления, гибкое управление постоянными абонентскими соединениями — обусловил ее высокий темп развития, ставший основой первичных сетей нового поколения.

Стек протоколов SDH состоит из протоколов трех основных уровней (рис. 5.9):

- уровень соединения контролирует доставку данных между двумя конечными пользователями сети;

- уровень управления передачей данных поддерживает физическую целостность сети, поддерживает операции административного контроля, осуществляет различные операции реконфигурирования в случае отказа какого-либо элемента сети и др.;
- физический уровень, названный в стандарте фотонным (photonic), имеет дело с кодированием бит информации с помощью модуляции света.

Рис. 5.9. Организация сети SDH

На сегодняшний день технология SDH считается не только перспективной, но и достаточно апробированной технологией для создания транспортных сетей. Технология SDH обладает рядом важных достоинств с пользовательской, эксплуатационной и инвестиционной точек зрения:

- умеренная структурная сложность, снижающая затраты на монтаж, эксплуатацию и развитие сети, в том числе подключение новых узлов;
- широкий диапазон возможных скоростей — от 155,520 Мбит/с (STM-1) до 2,488 Гбит/с (STM-16) и выше;
- возможность интеграции с каналами PDH, поскольку цифровые каналы PDH являются входными каналами для сетей SDH;
- высокая надежность системы благодаря централизованному мониторингу и управлению, а также возможности использования резервных каналов;
- высокая степень управляемости системы благодаря полностью программному управлению;
- возможность динамического предоставления услуг — каналы для абонентов могут создаваться и настраиваться динамически, без внесения изменений в инфраструктуру системы;
- высокий уровень стандартизации технологии, что облегчает интеграцию и расширение системы, дает возможность применения оборудования различных производителей;

- высокая степень распространения стандарта в мировой практике.

Стандарт SDH обладает достаточной степенью зрелости, что делает его надежным для инвестиций.

В дополнение к перечисленным достоинствам необходимо отметить развитие магистральных телекоммуникаций российских операторов связи на основе SDH, что предоставляет дополнительные возможности для привлекательных интеграционных решений. Перечисленные достоинства делают решения, основанные на технологии SDH, рациональными с точки зрения инвестиций. В настоящее время она может считаться базовой для построения современных транспортных сетей как для корпоративных сетей различного масштаба, так и для сетей связи общего пользования.

Контрольные вопросы

1. Какие эталонные модели построения сети вы знаете и каковы их отличительные особенности?
2. В чем заключается назначение сетевого и транспортного уровней?
3. Дайте определение понятию «алгоритм маршрутизации».
4. Какие протоколы маршрутизации вы знаете?
5. Для чего устанавливаются виртуальные соединения?
6. Что подразумевают под понятием драйвер?
7. Какие вы знаете протоколы и каковы их отличительные черты?
8. Перечислите основные параметры протокола TCP/IP.
9. Какие способы адресации компьютеров в Internet вы знаете?
10. Дайте определения службам редиректор и сервер.
11. Перечислите все известные вам службы обмена данными и в чем их особенности организации?

Глава 6
СЕТЕВЫЕ ОПЕРАЦИОННЫЕ СИСТЕМЫ

6.1. Классификация операционных систем

Сетевые операционные системы (ОС) созданы для клиент-серверных применений. В общих чертах это означает подсоединение однопользовательской рабочей станции общего назначения (клиента) к многопользовательским серверам и распределение нагрузки между ними. Сетевая операционная система необходима для управления потоками сообщений между рабочими станциями и серверами. Она может позволить любой рабочей станции работать с разделяемым сетевым диском или принтером, которые физически не подключены к этой станции. По запросу клиента сервер предоставляет ему различные сервисные функции. Кроме этого, сетевые ОС обеспечивают совместное использование в сети файлов и принтеров — эти возможности встроены в саму ОС. В результате подобная интегрированная сетевая поддержка позволяет компьютеру, например с сетевой операционной системой Windows Server, одновременно взаимодействовать со следующими сетевыми средами:

- с сетями Microsoft, включая Windows Server, Windows XP и т. д.;
- с сетями на базе Transmission Control Protocol/Internet Protocol (TCP/IP), включая UNIX-хосты;
- с сетями на основе AppleTalk (при использовании Windows NT Server Services for the Macintosh);
- с сетями Novell Netware.

Операционные системы могут различаться особенностями реализации внутренних алгоритмов управления основными ресурсами компьютера (процессорами, памятью, устройствами),

особенностями использованных методов проектирования, типами аппаратных платформ, областями использования и многими другими свойствами. По этим признакам проведена классификация ОС, показанная на рис. 6.1.

Рис. 6.1. Классификация операционных систем

Алгоритмы управления ресурсами определяют эффективность сетевой операционной системы. Среди них важнейшими являются следующие алгоритмы.

Поддержка **многозадачности** определяется по числу одновременно выполняемых задач: однозадачные (MS-DOS) и многозадачные (OS/2, UNIX, Windows 98/2000/XP и др.). Однозадачные ОС включают средства управления периферийными устройствами, средства управления файлами, средства общения с пользователем. Многозадачные ОС, кроме перечисленных функций однозадачных ОС, управляют разделением совместно используемых ресурсов, таких как память, оперативная память, файлы и внешние устройства и др.

Поддержка **многопользовательского режима** определяется по числу одновременно работающих пользователей и подразделяется на однопользовательские (MS-DOS, Windows 3.x и др.) и многопользовательские (UNIX, Windows Server). Многопользовательские системы, в отличие от однопользовательских, обладают

более развитой системой защиты информации каждого пользователя от несанкционированного доступа других пользователей, а также совместного доступа к разделяемым между ними ресурсам.

Поддержка **вытесняющей и невытесняющей многозадачности** определяется по способу распределения процессорного времени между несколькими одновременно существующими в системе процессами. Основным различием между вытесняющей и невытесняющей многозадачностью является степень централизации механизма планирования процессов. У невытесняющей многозадачности механизм планирования процессов сосредоточен в операционной системе, а у вытесняющей распределен между ОС и прикладными программами. При невытесняющей многозадачности активный процесс выполняется до тех пор, пока он сам не отдаст управление операционной системе для того, чтобы она сама выбрала из очереди другой готовый к выполнению процесс. При вытесняющей многозадачности решение о переключении процесса с одного процесса на другой принимается операционной системой, а не самим активным процессом.

Поддержка **многопроцессорной обработки** определяется числом процессоров, задействованных на обработку активных процессов. При многопроцессорной обработке все алгоритмы управления усложняются на порядок, данный режим обработки также называют **мультипроцессированием**. Многопроцессорные ОС могут классифицироваться по способу организации вычислительного процесса на асимметричные и симметричные. Асимметричные ОС выполняются целиком только на одном из процессов системы, распределяя прикладные задачи по остальным процессорам. Симметричная ОС полностью децентрализована и использует весь пул процессоров, разделяя их между системными и прикладными задачами.

Особенности построения **аппаратных платформ** базируются на свойствах операционной системы, ориентированных на аппаратные средства, на которых она реализуется. По типу аппаратуры различают ОС персональных компьютеров, мейнфреймов, кластеров и сетей ЭВМ. Среди перечисленных типов компьютеров могут встречаться как однопроцессорные варианты, так и многопроцессорные. Для больших компьютеров, например многопроцессорных серверов, функции планирования потока выполнения задач реализуются путем использования сложных приоритетных заданий и требуют большей вычислительной мощности, чем в ОС персональных компьютеров, в связи с чем ОС

больших машин являются более сложными и функциональными. Сетевые ОС имеют в своем составе средства передачи сообщений между компьютерами по линиям связи. На основе этих сообщений сетевая ОС поддерживает разделение ресурсов компьютера между удаленными пользователями, подключенными к сети. Для реализации этих функций сетевые ОС поддерживают специальные программные компоненты, реализующие коммуникационные протоколы, рассмотренные в предыдущей главе.

Другие требования предъявляются к операционным системам кластеров. **Кластер** — слабо связанная совокупность нескольких вычислительных систем, работающих совместно для выполнения общих приложений и предоставляющихся пользователю единой системой. Наряду со специальной аппаратурой для функционирования кластерных систем необходима программная поддержка со стороны ОС, которая сводится к синхронизации доступа к разделяемым ресурсам, обнаружению отказов и динамической конфигурации системы. Кроме того, существуют ОС, специально разработанные таким образом, чтобы при необходимости их можно было перенести с одного компьютера на другой. Такие ОС называют **мобильными**.

Особенности областей использования для многозадачных ОС подразделяются на три типа в соответствии с использованными при их разработке критериями эффективности:

- системы пакетной обработки (например, ОС ЕС);
- системы разделения времени (UNIX, VMS);
- 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, т. е. решение максимального числа задач в единицу времени.

Для достижения этой цели в системах пакетной обработки используется следующая схема функционирования: в начале работы формируется пакет задания, каждое задание содержит требование к системным ресурсам; из этого пакета заданий формируется мультипрограммная смесь, т. е. множество одновременно выполняемых задач. Для одновременного выполнения выбираются задачи, предъявляющие отличающиеся требования к ресурсам, так, чтобы обеспечивалась сбалансированная загрузка всех устройств вычислительной машины; например, в мультипрограммной сме-

си желательно одновременное присутствие вычислительных задач с интенсивным вводом-выводом. Выбор нового задания из пакета заданий зависит от внутренней ситуации, складывающейся в системе, т. е. выбирается «выгодное» задание. Следовательно, в таких ОС невозможно гарантировать то или иное задание в течение определенного периода времени. 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 он приносит задания, отдает его диспетчеру-оператору, а в конце дня после выполнения всего пакета задания получает результат. Очевидно, что такой порядок снижает эффективность работы пользователя.

Системы **разделения времени** призваны исправить основной недостаток систем пакетной обработки — изоляцию пользователя-программиста от процесса выполнения его задач. Каждому пользователю системы разделения времени предоставляется терминал, с которого он может вести диалог со своей программой. Так как в системах разделения времени 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. Ясно, что 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, и, кроме того, имеются накладные расходы вычислительной мощности на более частое переключение процессора с задачи на задачу. Критерием рациональности построения систем разделения времени является не максимальная пропускная способность, а удобство и эффективность работы пользователя.

Системы **реального времени** применяются для управления различными техническими объектами, такими, например, как станок, спутник, научно-экспериментальная установка или тех-

нологическими процессами, такими, как гальваническая линия, доменный процесс 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. Это время называется **временем реакции системы**, а соответствующее свойство системы — **реактивностью**. 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, часть задач может выполняться в режиме пакетной обработки, а часть — в режиме реального времени или в режиме разделения времени. В таких случаях режим пакетной обработки часто называют **фоновым** режимом.

В качестве особенностей методов построения при описании операционной системы часто указываются характерные черты ее структурной организации и основные концепции, положенные в ее основу.

Рассмотрим три базовые концепции.

Во-первых, большинство ОС используют 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, зато система получается более гибкой — ее функции можно наращивать, модифицировать или сужать, добавляя, модифицируя или исключая серверы пользовательского режима. Кроме того, серверы хорошо защищены друг от друга, как и любые пользовательские процессы.

Во-вторых, 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 внедрения во внутренние структуры объекта, что делает данные недоступными для несанкционированного использования извне, структурированность системы, состоящей из набора хорошо определенных объектов.

В-третьих, 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 или хотя бы некоторого подмножества из этого популярного набора. Концепция множественных прикладных сред наиболее просто реализуется в ОС на базе микроядра, над которым работают различные серверы, часть которых реализуют прикладную среду той или иной операционной системы.

Распределенная организация операционной системы позволяет упростить работу пользователя 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 (Remote Procedure Call) для прозрачного распределения программных процедур по машинам, многонитевой обработки, позволяющей распараллеливать вычисления в рамках одной задачи и выполнять эту задачу сразу на нескольких компьютерах сети, а также наличие других распределенных служб.

6.2. Обобщенная структура операционных систем

Системы должны быть гибкими с точки зрения бизнес-компонентов, открытыми на уровне технологий объектного взаимодействия, и, что очень важно для будущего, обладать высокой степенью стандартизованности выбранных базовых технологий. Чем больше производителей вычислительных систем поддерживают стандарт, тем ниже вероятность больших расходов при интеграции как программных, так и аппаратных комплексов.

Сетевая операционная система составляет основу любой вычислительной сети. Под сетевой операционной системой в широком смысле понимается совокупность операционных систем отдельных компьютеров, взаимодействующих с целью обмена сообщениями и разделения ресурсов по единым правилам — протоколам. В узком смысле сетевая ОС — это операционная система отдельного компьютера, обеспечивающая ему возможность работать в сети.

В сетевой операционной системе отдельной машины можно выделить несколько частей (рис. 6.2).

Средства **управления локальными ресурсами** компьютера выполняют функции распределения оперативной памяти между процессами планирования и диспетчеризации процессов, управления процессорами в мультипроцессорных машинах, управления периферийными устройствами и другие функции управления ресурсами локальных ОС.

Рис. 6.2. Структура сетевой ОС

Средства **предоставления собственных ресурсов** и услуг в общее пользование — серверная часть ОС (сервер). Эти средства обеспечивают, например, блокировку файлов и записей, что необходимо для их совместного использования; ведение справочников имен сетевых ресурсов; обработку запросов удаленного доступа к собственной файловой системе и базе данных; управление очередями запросов удаленных пользователей к своим периферийным устройствам.

Средства **запроса доступа к удаленным ресурсам** и услугам и их использования — клиентская часть ОС (редиректор). Эта часть выполняет распознавание и перенаправление в сеть запросов к удаленным ресурсам от приложений и пользователей, при этом запрос поступает от приложения в локальной форме, а передается в сеть в другой форме, соответствующей требованиям сервера. Клиентская часть также осуществляет прием ответов от серверов и преобразование их в локальный формат, так что для приложения выполнение локальных и удаленных запросов неразличимо.

Коммуникационные средства ОС, с помощью которых происходит обмен сообщениями в сети. Эта часть обеспечивает адресацию и буферизацию сообщений, выбор маршрута передачи сообщения по сети, надежность передачи и т. п., т. е. является средством транспортировки сообщений.

В зависимости от функций, возлагаемых на конкретный компьютер, в его операционной системе может отсутствовать либо клиентская, либо серверная части.

На рис. 6.3 показано взаимодействие сетевых компонентов.

Здесь ЭВМ 1 выполняет роль клиента, а ЭВМ 2 — роль сервера, соответственно на первой машине отсутствует серверная часть, а на второй — клиентская. На рисунке отдельно показан компонент клиентской части — редиректор. Именно редиректор перехватывает все запросы, поступающие от приложений, и анализирует их. Если выдан запрос к ресурсу данного компьютера, например **HDD** (Hard Disk Drive), то он переадресовывается соответствующей подсистеме локальной ОС, если же это запрос к удаленному ресурсу, он переправляется в сеть. При этом клиентская часть преобразует запрос из локальной формы в сетевой формат и передает его транспортной подсистеме, которая отвечает за доставку сообщений указанному серверу. Серверная часть операционной системы ЭВМ 2 принимает запрос, преобразует его и передает для выполнения своей локальной ОС. После того как результат получен, сервер обращается к транспорт-

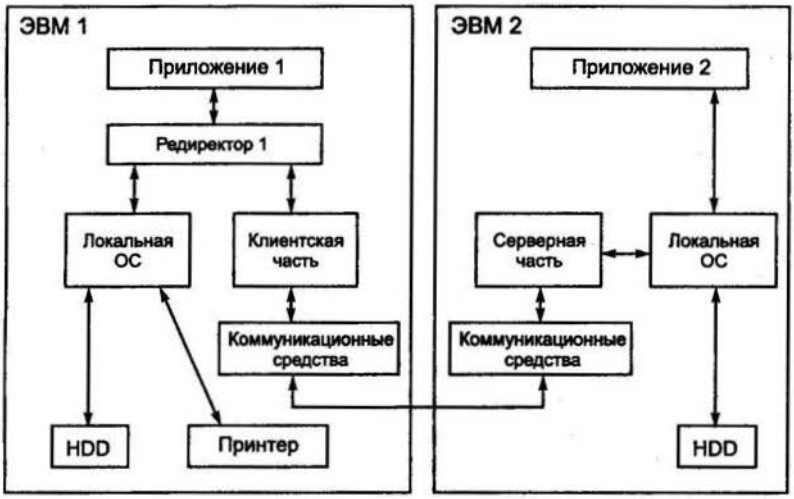

Рис. 6.3. Взаимодействие компонентов операционной системы при взаимодействии компьютеров

ной подсистеме и направляет ответ клиенту, выдавшему запрос. Клиентская часть преобразует результат в соответствующий формат и адресует его тому приложению, которое выдало запрос.

Существует два подхода к построению сетевых ОС (рис. 6.4).

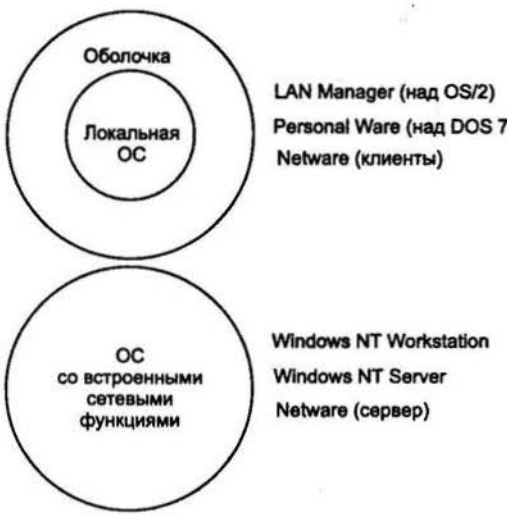

Рис. 6.4. Варианты построения сетевых ОС

Первые сетевые ОС представляли собой совокупность существующей локальной ОС и надстроенной над ней **сетевой оболочки**. При этом в локальную ОС встраивался минимум сетевых функций, необходимых для работы сетевой оболочки, которая выполняла основные сетевые функции. Примером такого подхода является использование на каждой машине сети операционной системы MS DOS (у которой, начиная с ее третьей версии, появились такие встроенные функции, как блокировка файлов и записей, необходимые для совместного доступа к файлам). Принцип построения сетевых ОС в виде сетевой оболочки над локальной ОС используется и в современных ОС, таких, например, как LANtastic или Personal Ware.

Однако более эффективным представляется путь разработки операционных систем, изначально предназначенных для работы в сети. Сетевые функции у ОС такого типа глубоко встроены в основные модули системы, что обеспечивает их логическую стройность, простоту эксплуатации и модификации, а также высокую производительность. Примером такой ОС является система Windows NT фирмы Microsoft, которая за счет встроенности сетевых средств обеспечивает более высокие показатели производительности и защищенности информации по сравнению с сетевой ОС LAN Manager той же фирмы (совместная разработка с IBM), являющейся надстройкой над локальной операционной системой OS/2. Компоненты сетевой операционной системы на каждой рабочей станции и файловом сервере взаимодействуют друг с другом посредством языка, называемого протоколом. Одним из общих протоколов является протокол фирмы IBM NetBIOS (Network Basic Input Output System — Сетевая операционная система ввода-вывода). Другим распространенным протоколом является IPX (Internet-work Packet Exchange — Межсетевой обмен пакетами) фирмы Novell.

6.3. Модель клиент—сервер и модель ОС на базе микроядра

Модель клиент—сервер — это еще один подход к структурированию ОС. В широком смысле модель клиент—сервер предполагает наличие программного компонента — потребителя какого-либо сервиса — клиента и программного компонента — по-

ставщика этого сервиса — сервера. Взаимодействие между клиентом и сервером стандартизуется, так что сервер может обслуживать клиентов, реализованных различными способами и, может быть, разными производителями. При этом главным требованием является то, чтобы они запрашивали услуги сервера понятным ему способом. Инициатором обмена обычно является клиент, который посылает запрос на обслуживание серверу, находящемуся в состоянии ожидания запроса (рис. 6.5). Один и тот же программный компонент может быть клиентом по отношению к одному виду услуг и сервером для другого вида услуг. Модель клиент—сервер является скорее удобным средством ясного представления функций того или иного программного элемента в той или иной ситуации, нежели технологией. Эта модель успешно применяется не только при построении ОС, но и на всех уровнях программного обеспечения, и имеет в некоторых случаях более узкий, специфический смысл, сохраняя, естественно, при этом все свои общие черты.

Рис. 6.5. Структура ОС клиент—сервер

В целях обеспечения эффективности и целостности работы ОС реализуется двумя режимами работы: **режим пользователя** (user mode) и **режим ядра** (kernel mode).

Применительно к структурированию ОС идея состоит в разбиении ее на несколько процессов — подсистем, каждая из которых выполняет отдельный набор сервисных функций — например, управление памятью, создание или планирование процессов. Каждая подсистема выполняется в пользовательском режиме. Клиент, которым может быть либо другой компонент ОС, либо прикладная программа, 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 (см. рис. 6.5).

Режим пользователя — менее привилегированный по сравнению с режимом ядра режим работы процессора. Он не имеет прямого доступа к аппаратуре. Выполняющийся в этом режиме код непосредственно имеет дело лишь с объектами своего адресного пространства (рис. 6.6).

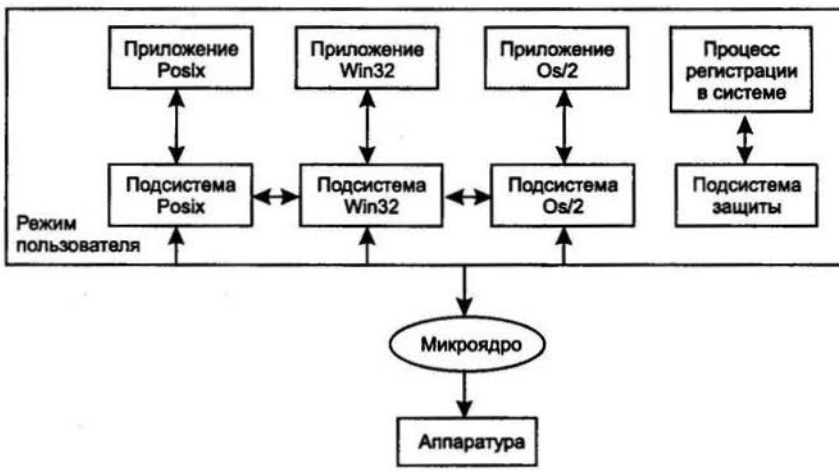

Рис. 6.6. Представление режима пользователя

Системные службы он вызывает через интерфейсы прикладных программ (Application Program Interface — API). Поддерживающие их приложения и подсистемы работают в режиме пользователя. При запуске приложения создается **процесс** *(process)*,

реализованный в виде **объекта** (*object*). Объект состоит из исполняемой программы, пространства адресов виртуальной памяти и одного или нескольких потоков.

Особенности процесса пользовательского режима таковы:

- не имеет прямого доступа к оборудованию. Это сделано в целях защиты от неверно работающих приложений или от несанкционированного доступа. Запросы на использование аппаратных ресурсов должны быть разрешены компонентом режима ядра;
- ограничен размерами выделенного адресного пространства. Ограничение размера памяти, используемой процессом, позволяет обеспечить дополнительную защиту ОС. Это ограничение устанавливается путем выделения процессу диапазона фиксированных адресов;
- может быть выгружен из физической памяти в виртуальную память на жестком диске. **Виртуальная память** (virtual memory, VRAM) использует пространство жесткого диска как дополнительную оперативную память. В результате процесс режима пользователя получает доступ к памяти, размер которой превышает объем ОЗУ;
- приоритет процесса данного типа ниже, чем у процессов режима ядра. Поэтому в сравнении с последними ему, как правило, предоставляется меньше процессорного времени. Это предохраняет ОС от снижения производительности или возникновения задержек, связанных с ожиданием завершения работы приложений.

Подход с использованием ядра заменил вертикальное распределение функций операционной системы на горизонтальное. Компоненты, лежащие выше микроядра, хотя и используют сообщения, пересылаемые через микроядро, взаимодействуют друг с другом непосредственно. Микроядро играет роль регулировщика. Оно проверяет сообщения, пересылает их между серверами и клиентами и предоставляет доступ к аппаратуре.

Режим ядра — это привилегированный режим работы, в котором код имеет прямой доступ ко всем аппаратным ресурсам и всей памяти, включая адресные пространства всех процессов режима пользователя (рис. 6.7).

Ниже перечислены функциональные возможности компонентов режима ядра, которые имеют:

- прямой доступ к оборудованию;
- прямой доступ ко всем видам памяти компьютера;

- более высокий приоритет исполнения, чем процессы режима пользователя.

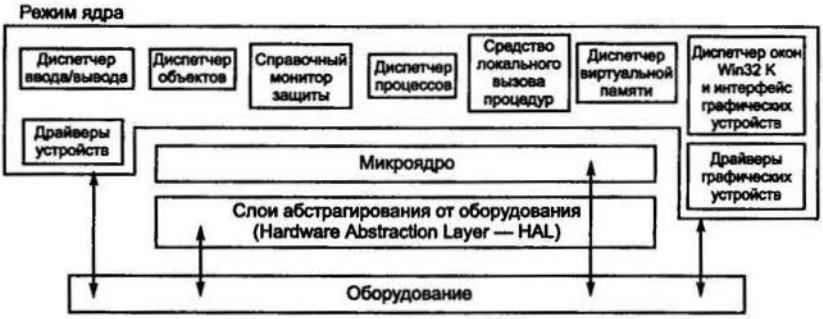

Рис. 6.7. Представление режима ядра

Кроме того, компоненты не выгружаются на жесткий диск в файл подкачки виртуальной памяти. Функционирование режима ядра обеспечивается **исполнительной системой**, включающей в себя системные службы, микроядро и слой абстрагирования от оборудования (HAL).

Исполнительная система представляет собой обобщенное наименование ряда подсистем и компонентов ОС, работающих в режиме ядра.

Поскольку системные (исполнительные) службы обеспечивают работу всех основных функций ОС, очень важно защитить их от влияния приложений и подсистем пользовательского режима. Такую защиту обеспечивают системные службы, работающие в режиме ядра:

- диспетчеры — различные модули, осуществляющие управление вводом-выводом, объектами, безопасностью, процессами, взаимодействием между процессами, виртуальной памятью, окнами и графикой;
- драйверы устройств — программные компоненты, управляющие доступом к оборудованию;

Микроядро предоставляет наиболее общие службы ОС, такие как диспетчеризация потоков, обработка прерываний первого уровня и отложенный вызов процедур. Микроядро расположено между слоем системных служб и HAL.

Слой абстрагирования от оборудования (HAL) представляет собой библиотеку режима ядра, включающую процедуры управ-

ления оборудованием. Этот программный слой позволяет скрыть особенности аппаратных платформ, предоставив ОС стандартные точки входа в процедуры, благодаря чему для нее исчезают различия между платформами и архитектурами. Поэтому ОС может функционировать на разных платформах с разными процессорами. Сетевая операционная система способна работать на одно- и многопроцессорных компьютерах и позволяет высокоуровневым драйверам графических адаптеров форматировать данные для мониторов разных типов.

Сетевые ОС обеспечивают работу с приложениями с помощью **подсистем среды**. Подсистема среды предоставляет API приложениям, разработанным под конкретную среду или ОС. Примером является широко распространенная подсистема Win32.

Микроядро реализует функции, лежащие в основе операционной системы. Это основа для менее существенных системных служб и приложений. В общем случае, подсистемы, бывшие традиционно неотъемлемыми частями операционной системы — файловые системы, управление окнами и обеспечение безопасности — становятся периферийными модулями, взаимодействующими с ядром и друг с другом.

Главный принцип разделения работы между микроядром и окружающими его модулями — включать в микроядро только те функции, которым абсолютно необходимо исполняться в режиме супервизора и в привилегированном пространстве. Под этим обычно подразумеваются машинозависимые 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.

Есть два пути построения подсистем. Один путь — разместить несколько таких чувствительных к режиму работы процессора серверов в пространстве ядра, что обеспечит им полный доступ к аппаратуре и в то же время связь с другими процессами с помощью обычного механизма сообщений. Такой подход был использован, например, при разработке Windows NT: кроме микроядра, в привилегированном режиме работает часть Windows NT, называемая executive — управляющей программой. Она включает ряд компонентов, которые управляют виртуальной памятью, объектами, вводом-выводом и файловой системой (включая сетевые драйверы), взаимодействием процессов и частично системой безопасности.

Другой путь заключается в том, чтобы оставить в ядре только небольшую часть сервера, представляющую собой механизм реализации решения, а часть, отвечающую за принятие решения, переместить в пользовательскую область.

6.4. Сетевые ОС NetWare фирмы Novell

ОС NetWare предназначены для обеспечения доступа к общим ресурсам сети со стороны нескольких пользователей. В качестве таких ресурсов выступают файлы данных, принтеры, модемы, модули и т. д.

NetWare поддерживает возможность описания различных типов объектов: пользователей, групп, файловых серверов, очередей печати, серверов печати и т. д. Каждый из этих типов объектов имеет свой набор свойств. Например, объект-пользователь характеризуется следующими атрибутами: пароль, балансовый счет, список групп. Значением атрибута является та совокупность данных, которая содержится в полях этого атрибута. Системная база данных представляет собой множество файлов, хранящихся на томе SYS файлового сервера.

Структурная схема ОС приведена на рис. 6.8. Ядро ОС NetWare загружается в ОП файлового сервера. В процессе функционирования ядро выполняет также роль диспетчера нитей (задач) операционной системы. Каждая нить или связана с каким-либо NLM-модулем (NetWare Loadable Module — загружаемый модуль NetWare), или представляет собой внутреннюю задачу ОС. NLM-модуль — это исполняемый файл ОС NetWare.

Рис. 6.8. Укрупненная структурная схема ОС NetWare

Системная база данных сетевых ресурсов является частью операционной системы и играет роль надежного хранилища системной информации:

- об объектах;
- об их свойствах (атрибутах);
- о значениях этих свойств.

ОС NetWare поддерживает следующие уровни протоколов по классификации OSI:

- канальный, обрабатывающий заголовок кадра (драйвер сетевого адаптера);
- сетевой (протоколы IPX, SPX, NetBIOS, TLI);
- транспортный (протоколы SPX, NetBIOS, TLI, NCP);
- сеансовый (протоколы NetBIOS, NCP);
- прикладной (протоколы RIP, NLSP, SAP).

Протокол IPX (Internetwork Packet eXchange) обрабатывает пакеты, являющиеся основным средством, которое используется при передаче данных в сетях NetWare.

Протокол IPX определяет самый быстрый уровень передачи данных в сетях NetWare. Он относится к классу дейтаграммных протоколов типа «точка—точка» без установления соединения. Это означает, что прикладной программе не требуется устанавливать специальное соединение с получателем. Впрочем, IPX имеет несколько недостатков:

- не гарантирует доставку данных;
- не гарантирует сохранения правильной последовательности при приеме пакетов;
- не подавляет прием дублированных пакетов, т. е. обработка ошибок, возникающих при передаче пакетов IPX, возлагается на прикладную программу, принимающую пакеты.

Указанных недостатков не имеет протокол транспортного уровня SPX (Sequenced Packet eXchange), ориентированный на установление соединения. Протокол SPX обрабатывает пакет SPX. Оценивая протоколы IPX и SPX, можно сказать, что протокол IPX быстр, но SPX надежен. В NetWare протокол NetBIOS является надстройкой над протоколом IPX и используется для организации обмена данными между рабочими станциями. Протокол NetBIOS реализован в виде резидентной программы NetBIOS.EXE, входящей в комплект поставки NetWare. Сравнивая методы адресации, используемые протоколами IPX/ SPX и NetBIOS, можно заметить, что метод адресации протокола NetBIOS более удобен. Можно адресовать данные не только од-

ной станции (как в IPX и SPX) или всем станциям сразу (как в IPX), но и группе станций, имеющих одинаковое групповое имя.

Файловая система

Одна из основных целей использования сетей — это обеспечение доступа всех пользователей к общим устройствам хранения информации, в основном, к жестким дискам. Организация файловой системы ОС NetWare во многом схожа с организацией файловой системы DOS, но также имеет отличия. Как и в DOS, информация хранится в файлах. Файлы размещаются в древовидной структуре каталогов и подкаталогов. Корнем такого дерева, в отличие от DOS, является том. Тома располагаются на серверах. При наличии соответствующих прав пользователь может получить доступ к томам всех серверов, доступных в сети.

Войдя в сеть, можно создавать другие каталоги. Пользователи могут обмениваться файлами через эти каталоги и хранить в них свои собственные файлы. Однако прежде чем использовать созданные каталоги, необходимо, во-первых, описать пользователей в системе и, во-вторых, наделить их правами, необходимыми для доступа к каталогам.

Пользователь осуществляет доступ к файлам и каталогам NetWare с рабочей станции, на которой установлена своя операционная система.

Средства защиты

Средства защиты информации встроены в NetWare на базовых уровнях операционной системы, а не являются надстройкой в виде какого-либо приложения.

Операционные системы NetWare содержат механизмы защиты следующих уровней:

- защита информации о пользователе;
- защита паролем;
- защита каталогов;
- защита файлов;
- межсетевая защита.

С точки зрения защиты ОС NetWare не делает различия между операционными системами рабочих станций. Станции, работающие под управлением DOS, Windows, OS/2, Macintosh и

UnixWare, обслуживаются совершенно одинаково, и все функции защиты применяются ко всем операционным системам, которые могут использоваться в сети NetWare.

6.5. Семейство ОС UNIX

Основные особенности

Операционная система UNIX с самого своего возникновения была по своей сути сетевой операционной системой. С появлением многоуровневых сетевых протоколов TCP/IP компания AT&T реализовала механизм потоков (Streams), обеспечивающий гибкие и модульные возможности для реализации драйверов устройств и коммуникационных протоколов. Streams представляют собой связанный набор средств общего назначения, включающий системные вызовы и подпрограммы, а также ресурсы ядра. В совокупности эти средства обеспечивают стандартный интерфейс символьного ввода-вывода внутри ядра, а также между ядром и соответствующими драйверами устройств, предоставляя гибкие и развитые возможности разработки и реализации коммуникационных сервисов.

Большая часть коммуникационных средств ОС UNIX основывается на использовании протоколов стека TCP/IP.

С самого начала ОС UNIX замышлялась как интерактивная система. Другими словами, операционная система UNIX предназначена для терминальной работы. Чтобы начать работать, человек должен «войти» в систему, введя со свободного терминала свое учетное имя (account name) и пароль (password). Человек, зарегистрированный в учетных файлах системы и, следовательно, имеющий учетное имя, называется зарегистрированным пользователем системы. Регистрацию новых пользователей обычно выполняет администратор системы. Пользователь не может изменить свое учетное имя, но может установить и/или изменить свой пароль.

ОС UNIX одновременно является операционной средой использования существующих прикладных программ и средой разработки новых приложений. Новые программы могут писаться на разных языках (Фортран, Паскаль, Модула, Ада и др.). Однако стандартным языком программирования в среде ОС UNIX является язык Си (который в последнее время все больше заме-

няется на Си++). Это объясняется тем, что, во-первых, сама система UNIX написана на языке Си, а, во-вторых, язык Си является одним из наиболее качественно стандартизованных языков.

Как и в любой другой многопользовательской операционной системе, обеспечивающей защиту пользователей друг от друга и защиту системных данных от любого непривилегированного пользователя, в ОС UNIX имеется защищенное ядро, которое управляет ресурсами компьютера и предоставляет пользователям базовый набор услуг.

К основным функциям ядра ОС UNIX принято относить следующие.

1. Инициализация системы — функция запуска и раскрутки. Ядро системы обеспечивает средство раскрутки (bootstrap), которое выполняет загрузку полного ядра в память компьютера и запускает ядро.

2. Управление процессами и нитями — функция создания, завершения и отслеживания существующих процессов и нитей (процессов, выполняемых на общей виртуальной памяти). Поскольку ОС UNIX является мультипроцессорной операционной системой, ядро обеспечивает разделение между запущенными процессами времени процессора (или процессоров в мультипроцессорных системах) и других ресурсов компьютера для создания внешнего ощущения того, что процессы реально выполняются в параллель.

3. Управление памятью — функция отображения практически неограниченной виртуальной памяти процессов в физическую оперативную память компьютера, которая имеет ограниченные размеры. Соответствующий компонент ядра обеспечивает разделяемое использование одних и тех же областей оперативной памяти несколькими процессами с использованием внешней памяти.

4. Управление файлами — функция, реализующая абстракцию файловой системы, иерархии каталогов и файлов. Файловые системы ОС UNIX поддерживают несколько типов файлов. Некоторые файлы могут содержать данные в формате ASCII, другие будут соответствовать внешним устройствам. В файловой системе хранятся объектные файлы, выполняемые файлы и т. д. Файлы обычно хранятся на устройствах внешней памяти; доступ к ним обеспечивается средствами ядра. В мире UNIX существует несколько типов организации файловых систем. Современные варианты ОС UNIX одновременно поддерживают большинство типов файловых систем.

5. Коммуникационные средства — функция, обеспечивающая возможности обмена данными между процессами, выполняющимися внутри одного компьютера (IPC — Inter-Process Communications), между процессами, выполняющимися в разных узлах локальной или глобальной сети передачи данных, а также между процессами и драйверами внешних устройств.

6. Программный интерфейс — функция, обеспечивающая доступ к возможностям ядра со стороны пользовательских процессов на основе механизма системных вызовов, оформленных в виде библиотеки функций.

Файловая система

Все файлы, с которыми могут манипулировать пользователи, располагаются в файловой системе, представляющей собой дерево, промежуточные вершины которого соответствуют каталогам, а листья — файлам и пустым каталогам. Реально на каждом логическом диске (разделе физического дискового пакета) располагается отдельная иерархия каталогов и файлов.

Каждый каталог и файл файловой системы имеет уникальное полное имя, задающее полный путь. Каталог, являющийся корнем файловой системы (корневой каталог), в любой файловой системе имеет предопределенное имя «/» (слэш).

Средства защиты

Поскольку ОС UNIX с самого своего зарождения задумывалась как многопользовательская операционная система, в ней всегда была актуальна проблема авторизации доступа различных пользователей к файлам файловой системы. Под авторизацией доступа понимаются действия системы, которые разрешают или не разрешают доступ данного пользователя к данному файлу в зависимости от прав доступа пользователя и ограничений доступа, установленных для файла. Схема авторизации доступа, примененная в ОС UNIX, настолько проста и удобна и одновременно настолько мощна, что стала фактическим стандартом современных операционных систем (не претендующих на качества систем с многоуровневой защитой).

При входе пользователя в систему программа login проверяет, что пользователь зарегистрирован в системе и знает правильный пароль (если он установлен), образует новый процесс и за-

пускает в нем требуемый для данного пользователя shell (оболочка). Но перед этим login устанавливает для вновь созданного процесса идентификаторы пользователя и группы, используя для этого информацию, хранящуюся в файлах /etc/passwd и /etc/group. После того как с процессом связаны идентификаторы пользователя и группы, для этого процесса начинают действовать ограничения для доступа к файлам. Процесс может получить доступ к файлу или выполнить его (если файл содержит выполняемую программу) только в том случае, если хранящиеся при файле ограничения доступа позволяют это сделать. Связанные с процессом идентификаторы передаются создаваемым им процессам, распространяя на них те же ограничения. Однако в некоторых случаях процесс может изменить свои права с помощью системных вызовов setuid и setgid, а иногда система может изменить права доступа процесса автоматически.

Как и принято в многопользовательской операционной системе, в UNIX поддерживается единообразный механизм контроля доступа к файлам и справочникам файловой системы. Любой процесс может получить доступ к некоторому файлу в том и только в том случае, если права доступа, описанные при файле, соответствуют возможностям данного процесса.

Защита файлов от несанкционированного доступа в ОС UNIX основывается на трех фактах. Во-первых, с любым процессом, создающим файл (или справочник), ассоциирован некоторый уникальный в системе идентификатор пользователя (UID — User Identifier), который в дальнейшем можно трактовать как идентификатор владельца вновь созданного файла. Во-вторых, с каждым процессом, пытающимся получить некоторый доступ к файлу, связана пара идентификаторов — текущие идентификаторы пользователя и его группы. В-третьих, каждому файлу однозначно соответствует его описатель — *i*-узел.

6.6. ОС Linux

Linux — это операционная система для IBM-совместимых персональных компьютеров и рабочих станций. Это многопользовательская ОС с сетевой оконной графической системой X Window System. ОС Linux поддерживает стандарты открытых систем и протоколы сети Internet и совместима с системами Unix, DOS,

MS Windows. Все компоненты системы, включая исходные тексты, распространяются с лицензией на свободное копирование и установку для неограниченного числа пользователей.

Система Linux разрабатывалась как ПК-версия операционной системы Unix, которая десятилетиями используется на мэйнфреймах и мини-ЭВМ и является основной ОС для рабочих станций. Linux предоставляет в распоряжение пользователя ПК скорость, эффективность и гибкость Unix, используя при этом все преимущества персональных машин.

С экономической точки зрения Linux обладает еще одним весьма существенным достоинством — это бесплатная система. Linux распространяется по генеральной открытой лицензии в рамках фонда свободного программного обеспечения (Free Software Foundation), что делает эту ОС доступной для всех желающих.

От Unix операционной системе Linux достались еще две замечательные особенности: она является многопользовательской и многозадачной системой. Многозадачность означает, что система может выполнять несколько задач одновременно. Многопользовательский режим означает, что в системе могут одновременно работать несколько пользователей, каждый из которых взаимодействует с ней через свой терминал. Еще одним из достоинств этой ОС является возможность ее установки совместно с Windows на один компьютер.

Linux способен любую персональную машину превратить в рабочую станцию. В наше время Linux является операционной системой для бизнеса, образования и индивидуального программирования. Университеты по всему миру применяют Linux в учебных курсах по программированию и проектированию операционных систем. Он стал незаменим в широких корпоративных сетях, а также для организации Internet-узлов и Web-серверов.

6.7. Семейство сетевых ОС Windows Server

Основные особенности

Структурно Windows Server может быть представлена в виде двух частей: часть операционной системы, работающая в режиме пользователя, и часть операционной системы, работающая в режиме ядра (см. рис. 6.5).

Windows Server может выступать как:

- файл-сервер;
- сервер печати;
- сервер приложений;
- контроллер домена;
- сервер удаленного доступа;
- сервер Internet;
- сервер обеспечения безопасности данных;
- сервер резервирования данных;
- сервер связи сетей;
- сервер вспомогательных служб.

Средства сетевого взаимодействия Windows Server направлены на реализацию взаимодействия с существующими типами сетей, обеспечение возможности загрузки и выгрузки сетевого программного обеспечения, а также на поддержку распределенных приложений.

Windows Server с точки зрения реализации сетевых средств имеет следующие особенности:

- встроенность на уровне драйверов, обеспечивает быстродействие;

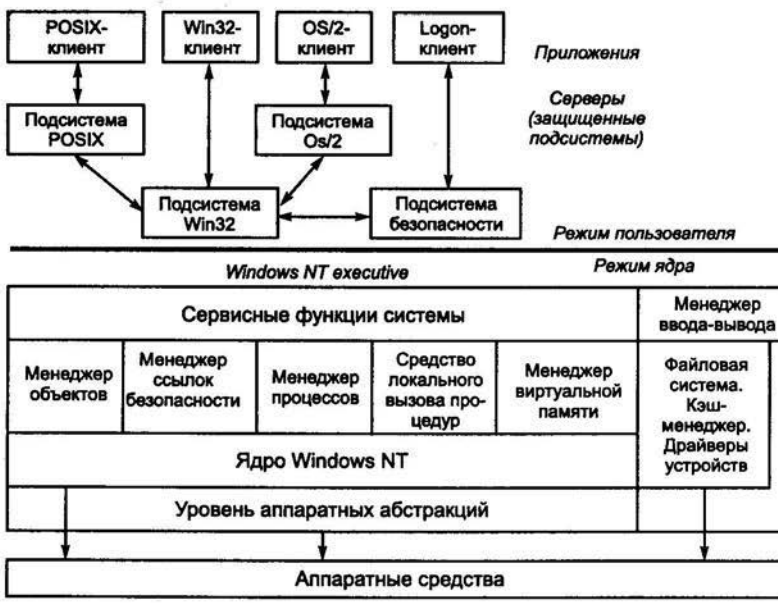

Рис. 6.9. Структура Windows NT

- открытость, предполагает легкость динамической загрузки/выгрузки и мультиплексируемость протоколов;
- наличие сервиса вызова удаленных процедур (RPC — Remote Procedure Call), именованных конвейеров и почтовых ящиков для поддержки распределенных приложений;
- наличие дополнительных сетевых средств, позволяющих строить сети в масштабах корпорации: дополнительные средства безопасности, централизованное администрирование, отказоустойчивость (источник бесперебойного питания, зеркальные диски).

Windows Server представляет из себя модульную операционную систему (рис. 6.9). Основными модулями являются:

- уровень аппаратных абстракций (Hardware Abstraction Layer — HAL);
- ядро (Kernel);
- исполняющая система (Windows NT executive);
- защитные подсистемы (Protected subsystems);
- подсистемы среды (Environment subsystems).

Основные свойства Windows NT

Улучшенное автораспознавание аппаратуры, возможность ручного выбора и конфигурирования сетевых адаптеров, если автоматическое распознавание не дает положительного результата.

Встроенная совместимость с NetWare. Возможность выполнения роли шлюза к сетям NetWare, так что Windows NT-компьютеры могут получать доступ к файлам, принтерам и серверам приложений NetWare.

Встроенная поддержка TCP/IP. Новая высокопроизводительная реализация протоколов TCP/IP, которая обеспечивает простое, мощное решение для межсетевого взаимодействия. Помимо этого, имеются базовые утилиты, такие как ftp, tftp, telnet, команды rarp, arp, route и finger.

Значительные улучшения средств удаленного доступа RAS, включающие поддержку IPX/SPX и TCP/IP, использование стандартов Point to Point Protocol (PPP) и Serial Line IP (SLIP).

Полная поддержка хранения встроенных объектов OLE и поиска составных документов. К этим возможностям относятся связывание, встраивание, связывание со встроенными объектами, технологии «drag-and-drop» и OLE-Automation.

Надежность.

Поддержка различных ОС. Клиентами в сети с Windows NT Server могут являться компьютеры с различными операционными системами. Стандартно поддерживаются ОС семейства Windows.

Взаимодействие с UNIX в Windows NT обеспечивается посредством поддержки общих стандартных сетевых протоколов (включая TCP/IP), стандартных способов распределенной обработки, стандартных файловых систем и совместного использования данных, а также благодаря простоте переноса приложений. Несмотря на то, что система Windows NT была разработана для поддержки работы по схеме клиент—сервер, для совместимости с UNIX-хостами встроена эмуляция терминалов.

SNMP. В Windows NT имеется ряд средств для интеграции в системы, использующие протокол SNMP (Simple Network Management Protocol), что позволяет выполнять удаленное администрирование Windows NT с помощью, например, SUN Net Manager и HP Open View. Обеспечивается поддержка графических и текстовых терминалов.

6.8. Администрирование сети Windows Server

Как уже указывалось в предыдущих параграфах главы, операционная система, управляющая обработкой, управлением и передачей информации, подразделяется на два основных типа: пользовательская и сервера. Соответственно назначение, функции и управление таких операционных систем различно.

Рабочая станция под управлением пользовательской операционной системы, как правило, может поддерживать: выполнение нескольких процессов, создавать, хранить и обновлять список конфигурации компьютера, средства доступа в Internet, службу сообщений, службу локальной безопасности и защиты файлов, папок и других локальных ресурсов компьютера, надежность функционирования приложений в операционной системе (каждое приложение выполняется в отдельном адресном пространстве).

Серверная операционная система, например Windows Server, оптимизирована для работы в качестве сервера файлов, печати, а также для приложений с широким спектром применений: от администрирования нескольких рабочих групп до корпоративных сетей. Основными функциями операционной системы сервера являются: поддержка многопроцессорной обработки задач,

управление и администрирование сервера и сети, отслеживание входящего и исходящего трафика сервера, поддержка Web-сервера, интеграция с клиентами других фирм производителей, например Macintosh и др.

6.8.1. Модели администрирования и регистрации в сети

Сети, работающие под управлением Microsoft Windows Server, могут быть организованы на основе доменной модели или модели рабочей группы.

Доменная модель характеризуется наличием в сети минимум одного компьютера, работающего под управлением Windows Server и выполняющего роль контроллера домена (domain controller). Домен — группа компьютеров, объединенных общей базой учетных записей пользователей и единой политикой защиты.

Модель рабочей группы позволяет организовать сеть на основе Windows Server без контроллера домена. Компьютеры при такой организации обладают равными правами на совместно используемые ресурсы. Главным недостатком построения таких сетей является отсутствие централизованного управления и администрирования учетных записей пользователей и защиты ресурсов, которые создаются на каждом компьютере, где пользователь будет регистрироваться.

Чтобы получить доступ к ресурсам, пользователям необходимо прежде всего зарегистрироваться — идентифицировать себя в домене или компьютере, при этом ему необходимо ввести имя пользователя, пароль, а также название домена, в котором зарегистрирована учетная запись или название компьютера. Окно, в котором происходит регистрация пользователя, раскрывается при загрузке операционной системы или при нажатии кнопок Ctrl-Alt-Delete и выборе пункта «Завершение работы» — далее «Завершение сеанса...», представлено на рис. 6.10.

Учетная запись пользователя — информация о пользователе системы, включающая в себя имя пользователя и пароль, необходимые для регистрации информации о принадлежности к той или иной рабочей группе или домену, права и привилегии.

Учетные записи бывают двух типов: глобальные и локальные. Глобальная учетная запись содержит информацию о пользователе домена. Она позволяет пользователю зарегистрировать-

Рис. 6.10. Окно регистрации входа пользователя в систему

ся в домене с любого компьютера сети и работать с доступными для него ресурсами. В Windows Server глобальную запись можно создать средствами User Manager for Domain (Диспетчер пользователей доменов). Она размещается в основной базе данных каталогов на главном контроллере домена PDC (Primary domain controller). Копии базы данных хранятся на всех резервных контроллерах домена BDC (Backup domain controller), которые с интервалом в 5 минут обновляются с основного контроллера домена. Пример построения такой сети представлен на рис. 6.11.

Локальная учетная запись содержит информацию о пользователе данного компьютера. С ее помощью пользователь может зарегистрироваться в системе и получить доступ к ресурсам ком-

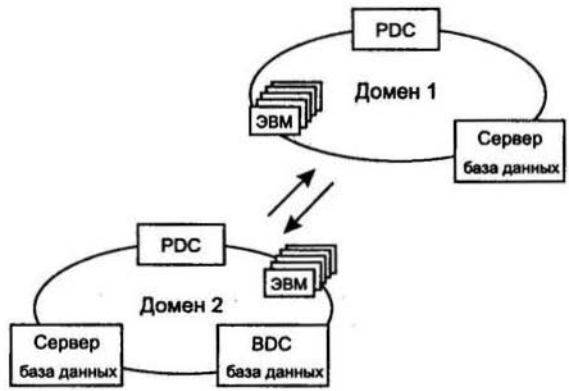

Рис. 6.11. Пример построения доменной модели сети

пьютера. Чтобы иметь право обратиться к ресурсам другого компьютера, надо и на нем завести локальную учетную запись пользователя.

6.8.2. Основные правила конфигурирования компьютеров, подключенных к сети

После того как было установлено физическое соединение сети (установлено и подключено сетевое оборудование), необходимо соответствующим образом сконфигурировать, т. е. программно настроить компьютеры, находящиеся в сети. Для этого необходимо произвести настройку сети. Это можно сделать только в том случае, если пользователь обладает соответствующими правами на конфигурирование системы. Такими правами, как правило, обладает пользователь из группы «Администратор». Настроить сетевые установки можно путем нажатия правой кнопки мыши на значке «Мое сетевое окружение», которое, как правило, располагается на Рабочем столе операционной системы, и выбрать пункт меню «Свойства». При этом откроется окно «Сеть и удаленный доступ к сети».

Для того чтобы раскрыть окно «Подключения по локальной сети — свойства» (рис. 6.12), в котором и настраиваются параметры подключения, необходимо правой кнопкой мыши нажать на значке «Подключение по локальной сети».

В этом окне необходимо установить протокол передачи данных, службу доступа к информации по сети, а также указать, клиентом каких сетей вы являетесь. Для выбора протокола передачи данных по сети необходимо в открывшемся окне нажать на кнопку «Установить», а затем в новом окно выбрать «Протокол», нажать «Добавить» (рис. 6.13). Раскроется список доступных для установки протоколов. Выберем, например, протокол передачи данных TCP/IP, для функционирования которого необходимо установить в свойствах данного протокола уникальный для каждого компьютера сети IP-адрес (например, 192.168.0.33) и маску подсети (например, 255.255.0.0).

Кроме того, чтобы получить возможность передавать данные по сети, а также иметь доступ к ресурсам другого компьютера, необходимо также установить, что пользователь является клиентом сети Microsoft, а также службу доступа к файлам и принтерам сетей Microsoft. Для этого необходимо в окне «Подключения

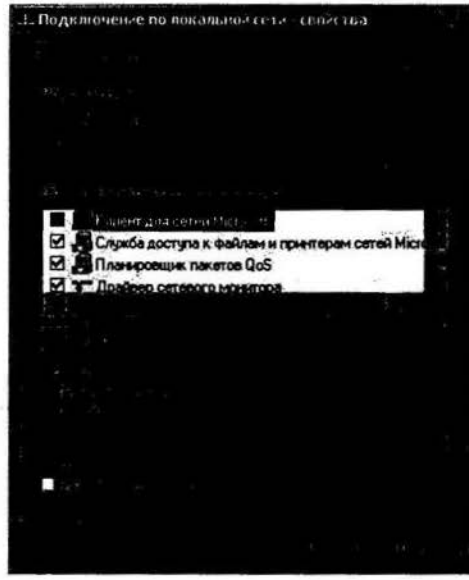

Рис. 6.12. Окно «Подключения по локальной сети — свойства»

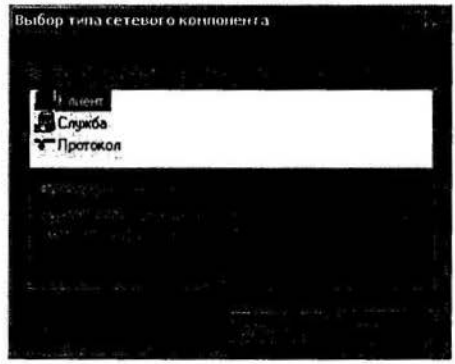

Рис. 6.13. Окно «Выбор типа сетевого компонента»

по локальной сети — свойства» выбрать «Установить», затем в открывшемся окне выбрать «Клиент», а затем из списка выбрать «Клиент для сетей Microsoft». Служба доступа к файлам и принтерам сетей Microsoft устанавливается аналогичным образом, только в окне «Выбор типа сетевого компонента» выбрать «Служба» и далее в открывшемся окне выбрать «Служба доступа к файлам и принтерам сетей Microsoft».

После выполнения вышеописанных действий дважды щелкнув левой кнопкой мыши на значке «Мое сетевое окружение». Вы должны увидеть список подключенных в данный момент и настроенных компьютеров в сети, у которых хотя бы один локальный ресурс имеет общий доступ.

По умолчанию все ресурсы компьютера — папки, принтеры и др. — не имеют общего доступа. Для того чтобы разрешить общий доступ к ресурсам своего компьютера, необходимо сначала выделить данный объект, затем, нажав правой кнопкой мыши на этом объекте, из раскрывшегося контекстного меню выбрать «Доступ». В открывшемся окне установить «Открыть общий доступ к этой папке» и при необходимости в строке «Сетевое имя» ввести имя, под которым другие компьютеры будут видеть данный ресурс.

6.8.3. Общие сведения об администрировании пользователей и рабочих групп

В сетевой операционной системе Windows Server присутствует специальный инструмент, предназначенный для администрирования глобальных учетных записей пользователей и групп на основном контроллере домена, а также локальные учетные записи на любом компьютере домена — Active Directory Users and Computers.

Окно Active Directory Users and Computers представлено на рис. 6.14.

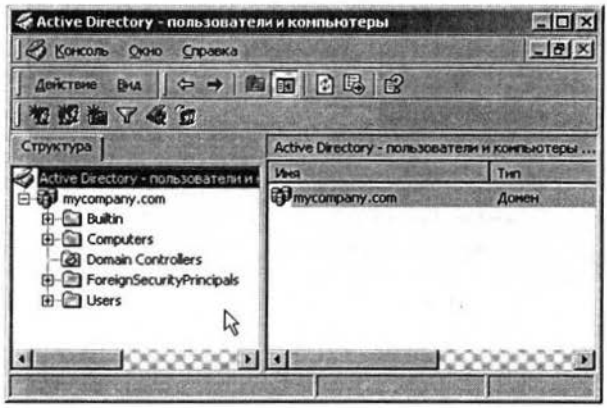

Рис. 6.14. Окно User Manager for Domain

Для того чтобы создать учетную запись нового пользователя в домене, необходимо в меню User выбрать «New User...». При этом появляются два последовательных окна (рис 6.15).

Здесь необходимо ввести имя пользователя (Username), под которым он будет регистрироваться в домене, полное имя пользователя (Full Name), описание, которое может отождествлять пользователя (Description), пароль для регистрации в домене

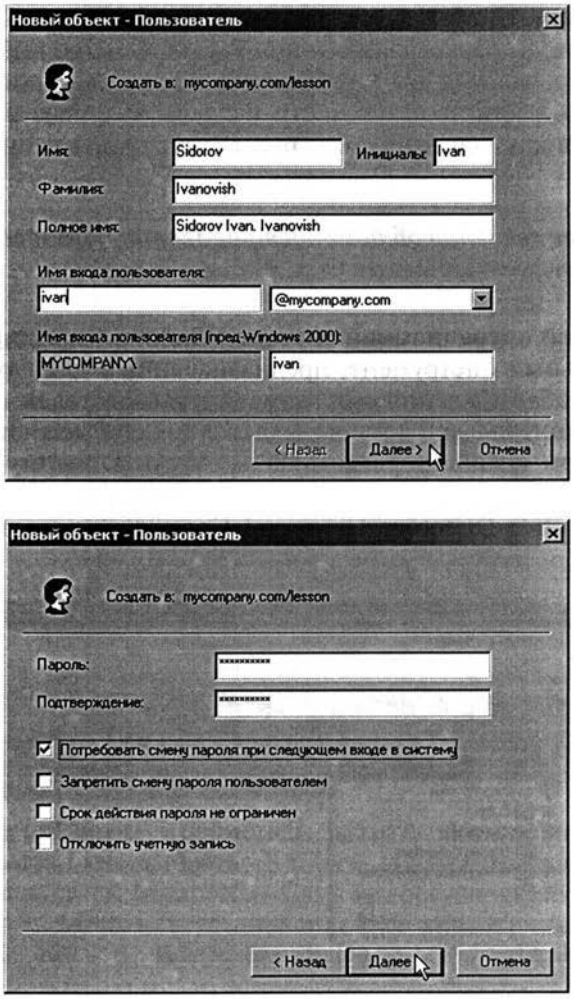

Рис. 6.15. Окно New User

(Password) и подтверждение пароля (Confirm Password). Кроме того, в этом окне можно задать смену пароля при первой регистрации пользователя (User Must Change Password at Next Logon), запретить смену пользователем пароля (User Cannot Change Password), ограничение действия пароля (Password Never Expires), отключить учетную запись (Account Disabled).

Контрольные вопросы

1. Для чего нужны сетевые операционные системы?
2. По каким основным признакам можно классифицировать ОС?
3. Что такое кластер и какие ОС называют мобильными?
4. Дайте определения понятиям: время реакции системы и реактивность.
5. Опишите два основных подхода к построению ОС.
6. Для чего необходима виртуальная память в компьютере?
7. Каким образом обеспечивается взаимодействие подсистем с исполнительной системой?
8. Опишите основные принципы построения подсистем.
9. В чем основное различие одноранговых и двухранговых классов сетей?
10. Перечислите известные вам ОС.
11. В чем заключается основной принцип организации распределенных вычислений?
12. Для чего необходима служба удаленного вызова процедур и сетевой динамический обмен данными?

Глава 7
СТРУКТУРА И ИНФОРМАЦИОННЫЕ УСЛУГИ ТЕРРИТОРИАЛЬНЫХ СЕТЕЙ

7.1. Структура территориальных сетей

Глобальная сеть Internet — самая крупная и единственная в своем роде сеть в мире. Среди глобальных сетей она занимает уникальное положение. Правильнее ее рассматривать как некоторую надсеть — объединение многих сетей, сохраняющих самостоятельное значение. Действительно, Internet не имеет ни четко выраженного владельца, ни национальной принадлежности. Любая сеть может иметь связь с Internet и, следовательно, рассматриваться как ее часть, если в ней используются принятые для Internet протоколы TCP/IP или имеются конверторы в протоколы TCP/IP. Практически все сети национального и регионального масштабов имеют выход в Internet.

Типичная территориальная (национальная) сеть имеет иерархическую структуру.

Верхний уровень — федеральные узлы, связанные между собой магистральными каналами связи. Магистральные каналы физически организуются на ВОЛС или на спутниковых каналах связи. Средний уровень — региональные узлы, образующие региональные сети. Они связаны с федеральными узлами и, возможно, между собой выделенными высоко- или среднескоростными каналами, такими как каналы T1, E1, B-ISDN или радиорелейные линии. Нижний уровень — местные узлы (серверы доступа), связанные с региональными узлами преимущественно коммутируемыми или выделенными телефонными каналами связи, хотя заметна тенденция к переходу к высоко- и среднескоростным каналам. Именно к местным узлам подключаются

локальные сети малых и средних предприятий, а также компьютеры отдельных пользователей. Корпоративные сети крупных предприятий соединяются с региональными узлами выделенными высоко- или среднескоростными каналами.

Иерархическая архитектура Internet может быть представлена так, как на рис. 7.1. **Автономная система** (AS — Autonomous System) — локальная сеть или система сетей (группа маршрутизаторов), находящаяся под единым техническим управлением, использующая единый протокол маршрутизации IGP (Interior Gateway Protocol) и имеющая собственную политику маршрутизации (маршруты к другим AS). Каждая AS имеет свой цифровой номер, присвоение которого осуществляет RIPE (Reseaux IP Europeens) — организация, отвечающая за распределение IP- адресов и номеров автономных систем в европейском регионе.

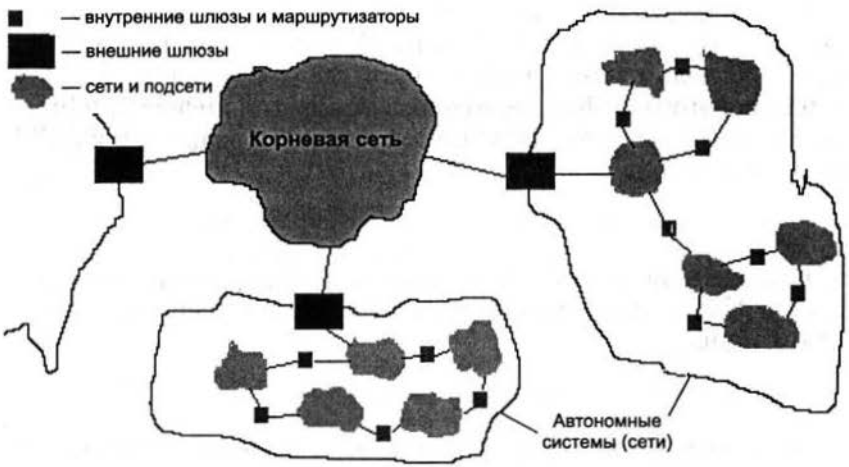

Рис. 7.1. Иерархическая структура территориальной сети

Автономные системы, как правило, управляются Локальными Интернет-Регистратурами (LIR — Local Internet Registry).

7.2. Сервисы Internet

Основные услуги телекоммуникационных технологий:

- передача файлов;
- электронная почта;

- телеконференции;
- справочные службы (доски объявлений);
- видеоконференции;
- доступ к информационным ресурсам (информационным базам) сетевых серверов;
- мобильная сотовая связь;
- компьютерная телефония.

Файловый обмен — это доступ к файлам, распределенным по различным компьютерам. В сети Internet на прикладном уровне используется протокол FTP. Доступ возможен в режимах off-line и on-line. В режиме off-line посылается запрос к FTP-серверу, сервер формирует и посылает ответ на запрос. В режиме on-line осуществляется интерактивный просмотр каталогов FTP-сервера, выбор и передача нужных файлов. Для осуществления указанных операций на ЭВМ пользователя должно быть установлено программное обеспечение FTP-клиент. При запросе файла по протоколу FTP пользователь должен знать, где находится нужный ему файл. Для этого удобно воспользоваться другой информационной системой сети Internet, называемой Archie. Обращаясь к клиенту Archie по команде

```
archie <имя файла>,
```

пользователь получает в ответ адрес сервера, имя директории и размер файла. Далее можно обращаться к FTP-серверу с помощью команды

```
ftp[<параметры>][<имя сервера>].
```

Квадратные скобки в записи команд означают необязательные части. Параметры используются только при отладке FTP. В качестве имени сервера указывается IP-имя или IP-адрес удаленного компьютера.

В большинстве серверов Internet для входа по FTP-команде нужны предварительная регистрация пользователя и указание пароля. Однако это не требуется при обращениях к общедоступным (анонимным) серверам. Такие серверы создают и обслуживают организации, заинтересованные в распространении информации определенного вида.

После выполнения команды обращения к серверу FTP-клиент переходит в командный режим. Ниже приведены примеры

команд, которые могут выполняться в командном режиме (где S — удаленный компьютер, T — локальный компьютер):

open [<имя S>] — устанавливает связь с удаленным компьютером;

close [<имя S>] — разрывает связь с удаленным компьютером, оставаясь в командном режиме;

quit — то же, что и close, но с выходом из командного режима (из ftp);

cd [<имя каталога в S>] — выбор каталога на сервере;

get [<имя файла в S>[<имя файла в T >]] — перепись файла с S на T;

mget [<имена файлов в S>] — то же, что и get, но нескольких файлов;

put [<имя файла в T>[<имя файла в S>]] — обратная перепись (допускается не во всех случаях);

mput <имена файлов в S> — то же, что и put, но более одного файла;

user <имя/пароль> — идентификация пользователя на сервере.

Пример последовательности команд при работе по протоколу FTP:

ftp> cd techno — переход в каталог techno;

ftp> ascii — установка передачи текста в коде ASCII (если указать «binary», то будут передаваться двоичные данные);

ftp> get test test.txt — перепись файла test в компьютер пользователя под именем test.txt;

ftp> quit — конец.

Во время сеанса связи инициируется управляющий (командный) процесс, который осуществляется через протокол Telnet и существует во время всего сеанса связи. Процесс передачи файла существует только на время передачи.

Протокол эмуляции терминала Telnet. С помощью этого протокола пользователь сети Internet может работать на удаленном компьютере. Связь устанавливается при обращении к Telnet-программе командой

telnet: <имя базы данных или системы каталогов> или <имя удаленного компьютера S>.

После установления связи все, что пользователь набирает на клавиатуре своего компьютера, передается на удаленный компь-

ютер S, а содержимое экрана удаленного компьютера S отображается на экране пользователя. Для возвращения в свой компьютер (т. е. в командный режим клиентской программы Telnet) нужно нажать соответствующую клавишу (Ctrl-). Примерами команд в клиентской программе могут служить: установление связи (open), возвращение в командный режим (close), завершение работы (quit). Передача сообщений при работе с Telnet осуществляется с помощью средств FTP.

Протокол Telnet должен иметь возможность работать в условиях разных аппаратных платформ клиента и сервера, что достигается через промежуточный виртуальный терминал.

Электронная почта (E-mail) — это средство обмена сообщениями по электронным коммуникациям (в режиме off-line). По электронной почте можно пересылать текстовые сообщения и архивированные файлы. В архивированных файлах могут содержаться данные в различных форматах.

Разработан ряд протоколов электронной почты для прикладного уровня. Наиболее популярны среди них протоколы SMTP (Simple Mail Transfer Protocol) в стеке протоколов TCP/IP и X.400 в модели ISO. Расширение числа возможных кодировок и форматов данных по сравнению с SMTP сделано в протоколе MIME (Multipurpose Internet Mail Extensions). На их базе разработано программное обеспечение E-mail, способное работать в обоих протоколах. Оно включает программы почтовых серверов и клиентов. Применение MIME упрощает пересылку графических и звуковых файлов, реализацию шифрования и электронной подписи.

На ЭВМ пользователя должна быть установлена программа-клиент, поддерживающая функции создания, передачи и приема сообщений. На почтовом сервере, выделяемом в корпоративной или локальной сети, организуется промежуточное хранение поступающих сообщений. Связь индивидуальных пользователей с почтовым сервером осуществляется по протоколам IMAP (Internet Message Access Protocol) или POP3 (Post Office Protocol). Для индивидуального пользователя, общающегося с другими абонентами по телефонной сети общего пользования, такое промежуточное хранение возможно на собственном компьютере, но тогда требуется либо круглосуточное включение компьютера, либо предварительная договоренность о времени связи.

В территориальных сетях почтовые сообщения проходят через ряд промежуточных федеральных или региональных узлов.

В таких узлах устанавливается программное обеспечение (так называемый агент передачи сообщений), выполняющее функции сортировки и маршрутизации сообщений.

Примерами программных систем электронной почты, выполняющих все отмеченные функции E-mail, могут служить Microsoft Mail, Outlook Express или Microsoft Outlook. Они позволяют адресовать и переадресовывать сообщения индивидуальному пользователю и/или группе пользователей, использовать доску объявлений, осуществлять поиск сообщений, пришедших в почтовый сервер, по контексту, адресу, времени отправки.

В настоящее время при разработке многих программных систем предусматривается интерфейс со средствами электронной почты. Клиентские программы E-mail стараются включать в Web-браузеры сети Internet, а также в такие прикладные программные системы, как АСУ, САПР, системы документооборота.

Письма в E-mail состоят из заголовка и тела (текста). В заголовке указывается, кому предназначено письмо, от кого оно поступило, кому посланы копии, дата отправки, указатель ключа, по которому пользователь может определить ключ для декодирования текста. В протоколе IMAP сначала клиенту передается заголовок, а текст остается на сервере, затем пользователь при желании может получить и весь текст. В протоколе POP3 при обращении к почтовому серверу на клиентский узел переписывается все сообщение.

Вспомогательные системы Archie и Whois в Internet. Вспомогательные средства облегчают поиск в разветвленных сетях. В Internet к ним относится Archie — информационная система для просмотра содержимого FTP-серверов. Вместо утомительной навигации вручную по каталогам система позволяет искать данные по ключевым словам или по образцу. Другая вспомогательная система в Internet — система Whois — справочник по абонентам электронной почты.

7.3. Виды конференц-связи

Телеконференции — доступ к информации, выделенной для группового использования в отдельных конференциях (newsgroups).

Возможны глобальные и локальные телеконференции. Основные функции программного обеспечения телеконференций:

включение материалов в телеконференцию, рассылка извещений о новых поступивших материалах, выполнение заказов. Возможны режимы E-mail и on-line.

Самая крупная система телеконференций — USENET. В USENET информация организована иерархически. Сообщения рассылаются или лавинообразно, или через списки рассылки. В режиме on-line можно прочитать список сообщений, а затем и выбранное сообщение. В режиме off-line из списка выбирается сообщение и на него посылается заказ.

Существуют также средства аудиоконференций (голосовых телеконференций). Вызов, соединение, разговор происходят для пользователя как в обычном телефоне, но связь идет через Internet.

Электронная «доска объявлений» BBS (Bulletin Board System) — технология, близкая по функциональному назначению к телеконференции, позволяет централизованно и оперативно направлять сообщения для многих пользователей. Программное обеспечение BBS сочетает в себе средства электронной почты, телеконференций и обмена файлами. Примеры программ, в которых имеются средства BBS, — Lotus Notes, World-group.

В настоящее время интенсивно развиваются технологии настольной конференц-связи в реальном масштабе времени. В зависимости от вида разделяемой пользователями информации возможны несколько уровней настольной конференц-связи:

- простая E-mail сессия;
- совместная работа над документом без голосовой связи (shared whiteboard — разделяемая «доска»);
- совместная работа над документом с голосовой связью (разновидность аудиоконференций);
- видеоконференция.

По мере повышения уровня возрастают требования к пропускной способности используемых каналов передачи данных. Для простых видов конференц-связи, а также и для аудиоконференций при применении современных эффективных способов сжатия информации можно использовать даже обычные телефонные линии, способные передавать информацию со скоростью от 8—10 кбит/с.

В зависимости от числа участников и способа интерактивной связи между ними различают двухточечную (unicast), широковещательную (broadcast) и многоточечную (multicast) конференции. Если в широковещательной конференции информация от

центрального узла доставляется всем участникам, то в многоточечной конференции она рассылается избирательно, т. е. одновременно может идти обмен разной информацией внутри нескольких подгрупп одной группы пользователей.

Наиболее очевидными областями применения настольной конференц-связи являются дистанционное обучение, медицинские консультации, различные бизнес-приложения.

Программное обеспечение телеконференций включает серверную и клиентскую части. В клиентской программе должны быть как минимум средства E-mail, многооконный текстовый редактор (так как принимаемый и отправляемый партнеру тексты помещаются в разные окна, отдельное окно может быть выделено для видео в случае видеоконференций), средства файлового обмена.

Серверная часть (MCU — Multipoint Control Unit) служит для распределения потока данных между пользователями с согласованием форматов окон с видеоинформацией, способов сжатия данных, скоростей потоков, идущих от разных сетей (пользователей).

Видеоконференция — способ связи, включающий передачу видеоизображений по телекоммуникационным каналам связи с возможностями интерактивного общения (в режиме on-line). Очевидно, что требования к пропускной способности каналов передачи данных в видеоконференциях существенно выше, чем в обычных телеконференциях. Видеоконференции стали доступными после развития высокоскоростных каналов связи и эффективных алгоритмов сжатия данных при их передаче.

Система видеоконференции включает дистанционно управляемую видеокамеру, монитор, микрофоны, динамики, устройство для считывания графических документов, кодеки (кодек — специальное устройство для сжатия информации, само слово образовано первыми слогами слов кодирование и декодирование).

При использовании в системе видеоконференции аналогового телевидения достигается самое высокое качество передачи динамических изображений, однако для этого требуется полоса около 5 МГц, что при кодово-импульсной модуляции и кодировании отсчетов восьмибитовыми комбинациями эквивалентно пропускной способности каналов 80 Мбит/с.

Цифровые видеосистемы также используют видеокамеру, монитор, микрофон, динамик, кодек. Связь чаще всего организуется по цифровым каналам (ISDN). Качество передачи изо-

бражения не так высоко, поэтому этот способ обходится значительно дешевле аналогового телевидения.

Для организации конференц-связи имеется группа стандартов серии T.120, разработанных ITU. Стандарты T.122/125 относятся к службе многоточечных соединений, T.126 — к whiteboard технологии, T.127 — к передаче файлов при многоточечной связи. Стандарт T.123 содержит описание транспортных протоколов, которые могут использоваться в системах конференц-связи. В стандарте T.124 разработан соответствующий язык диаграмм для пользователей с недостатками слуха или речи.

Другая группа стандартов конференц-связи H.32x посвящена реализации мультимедийных приложений в различных типах сетей. Стандарты H.320, H.321, H.322, H.323 и H.324 ориентированы соответственно на каналы N-ISDN (узкополосные), B-ISDN (широкополосные), локальные сети с гарантированной пропускной способностью, локальные сети без гарантированной полосы пропускания и телефонные линии с коммутацией каналов. Стандарт H.310 относится к мультимедийным приложениям с высоким разрешением. В этих стандартах устанавливаются требования к сжатию информации, к протоколу передачи, к синхронизации видео и звука.

7.4. Web-технологии

В сети Internet имеется уникальная информационная система WWW (World Wide Web — всемирная паутина). Другое ее краткое название — Web. Она представляет собой распределенное хранилище информации, а также серверное и клиентское программное обеспечение для обслуживания этой информации и доступа к ней.

Система WWW использует **гипертекст** — структурированный текст с введением в него перекрестных ссылок, отражающих смысловые связи частей текста. Слова-ссылки выделяются цветом и/или подчеркиванием. Выбор ссылки вызывает на экран связанный со словом-ссылкой текст или рисунок. Можно искать нужный материал по ключевым словам.

Информация, доступная по Web-технологии, хранится на Web-серверах. Сервер имеет специальную программу, постоянно отслеживающую приход на определенный порт (обычно это порт

80) запросов от клиентов. Сервер удовлетворяет запросы, посылая клиенту содержимое запрошенных Web-страниц или результаты выполнения запрошенных процедур.

Клиентские программы WWW называют **браузерами** (brousers). Имеются текстовые (например, Lynx) и графические (наиболее известны Netscape Navigator и MS Explorer) браузеры. В браузерах имеются команды листания, перехода к предыдущему или последующему документу, печати, перехода по гипертекстовой ссылке и т. п. Из браузеров доступны различные сервисы — FTP, Gopher, USENET, E-mail. Для подготовки материалов для их включения в базу WWW разработаны специальный язык HTML (Hyper Text Markup Language) и реализующие его программные редакторы, например Internet Assistant в составе редактора Word. Подготовка документов предусмотрена и в составе большинства браузеров.

Для связи Web-серверов и клиентов разработан протокол HTTP (Hyper Text Transfer Protocol), работающий на базе TCP/IP. Web-сервер получает запрос от браузера, находит соответствующий запросу файл и передает его для просмотра в браузер. Популярными серверами являются Apache, Netscape Enterprise Server и Microsoft Internet Information Server (IIS), которые могут работать как в Unix, так и в Windows NT. Все три сервера поддерживают механизм программных расширений, основанный на применении так называемого шлюзового интерфейса CGI (Common Gateway Interface), имеют встроенный HTML-редактор. Кроме того, в первых двух из них поддерживается стандарт шифрования SSL (Secure Sockets Layer) для защиты передаваемых по сети данных от несанкционированного доступа. Опыт показывает, что для крупных серверов предпочтительнее платформа Unix, тогда как для серверов с малым числом транзакций лучше подходит ОС Windows NT.

В настоящее время для облегчения поиска информации в Internet применяют **информационно-поисковые системы** (ИПС), располагаемые на доступных пользователям Internet-серверах. В этих системах собирается, индексируется и регистрируется информация о документах, имеющихся в обслуживаемой группе Web-серверов. Индексируются или все значащие слова, имеющиеся в документах, или только слова из заголовков. Пользователю предоставляется возможность обращаться к серверу с запросами на естественном языке, со сложными запросами, включающими логические связки. Примером таких ИПС может

служить AltaVista, Rambler. Например, для функционирования AltaVista фирма DEC выделила 6 компьютеров, самый мощный из них — 10-процессорная ЭВМ Alpha-8400 с базой данных объемом более 45 Гбайт.

7.5. Языки и средства создания Web-приложений

Бурное развитие глобальной сети Internet оказывает огромное влияние на все сферы деятельности человека. Internet вызвал революционные изменения в индустрии программного обеспечения. Появилась новая категория приложений, специально разработанных для Internet и учитывающих особенность серверов Web. Поэтому программы для Internet часто называют приложениями Web. Например, организация образования через Internet требует специальной организации учебных пособий, которые могут быть подготовлены в формате HTML, рассчитанном на просмотр учебника в одном из браузеров (Internet Explorer, Netscape Navigator). Для создания документов в формате HTML существуют различные программные средства. Например, текстовый редактор Word позволяет сохранять документ и отдельные его части в формате HTML и даже организовывать гиперсвязи между HTML-файлами. Для получения более сложного HTML-документа требуются навыки программирования на языке HTML.

Язык HTML — гипертекстовый язык, описывающий структуру документа, вид которого на экране определяется браузером.

Описание на HTML — это текст в формате ASCII и последовательность включенных в него команд (управляющих кодов, называемых также *дескрипторами,* или *тегами*). Эти команды расставляются в нужных местах текста, определяя шрифты, переносы, появление графических изображений, ссылки и т. п.

Команды имеют форму < >, где между скобками записывается имя команды.

Не вдаваясь в детали языка HTML, которые легко могут быть найдены в соответствующих книгах, приведем только необходимые сведения о нем.

Если открыть программу Блокнот, написать в нем следующие строчки:

```
<HTML>
<HEAD>
```

```
<TITLE>Информационный раздел 1</TITLE>
</HEAD>
<BODY>
    <FONT FACE="Times New Roman">
        <P>Информационный раздел 1.</P>
        <P>Текст</P>
    </FONT>
</BODY>
</HTML>
```

и сохранить их в виде файла с расширением .html, то открытие этого файла с помощью браузера Internet Explorer приведет к появлению в окне браузера простейшего HTML-документа (рис. 7.2).

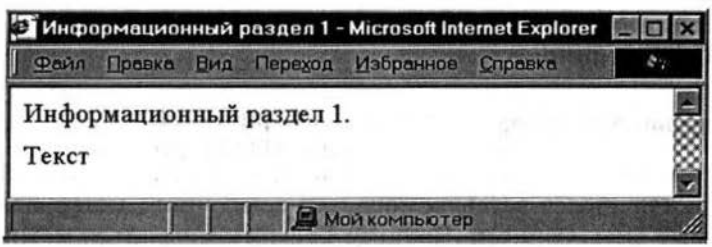

Рис. 7.2. Простейший HTML-документ

Теги <HTML>, </HTML> определяют начало и окончание HTML-документа.

Теги <HEAD>, </HEAD> определяют информацию, относящуюся к разделу заголовка HTML-документа, в частности, шрифт и текст самого заголовка:

```
<TITLE>Информационный раздел 1</TITLE>
```

Теги <BODY>, </BODY> определяют содержание HTML-документа и свойства этого содержания:

- тип шрифта

```
<FONT FACE ="Times New Roman">
</FONT>
```

- текстовое содержание

```
<P>Информационный раздел 1.</P>
<P>Текст</P>
```

Команды форматирования текста (дескрипторы компоновки):

Теги <P>, </P> определяют начало и окончание текстового фрагмента, начинающегося с новой строки;

 — перевод строки;

<HR> — перевод строки с печатью горизонтальной линии, разделяющей части текста.

Команды форматирования заголовков (дескрипторы стиля):

<H1> Текст </H1> — текст печатается наиболее крупным шрифтом, используется для заголовков верхнего уровня;

<H2> Текст </H2> — для следующего уровня и т. д. вплоть до команды <H6>.

Команды форматирования символов представлены парными символами B, I, U. Текст между открывающей и закрывающей командами будет выделен полужирно, курсивом, подчеркиванием соответственно.

Дескрипторы связи

В командах вставки графики и гипертекстовых ссылок используются адреса вставляемого или ссылочного материала, называемые URL (Uniform Resourse Locator). Ссылаться можно как на нужные места в том же документе, в котором поставлена ссылка, так и на другие файлы, находящиеся в любом месте сети. URL может представлять собой имя файла в данном узле сети или IP-имя другого узла с указанием местоположения файла в этом узле и, возможно, также метки внутри этого файла.

Команда гипертекстовой ссылки:

```
<A HREF="URL" >Текст </A>.
```

Текст в окне будет выделен цветом или подчеркиванием. Можно ссылаться на определенное место в документе. Тогда

```
<A HREF="URL#метка"> Текст </A>.
```

Сама метка в документе имеет вид:

```
<A NAME="метка"> Текст </A>.
```

Ссылки на фрагменты данного документа можно упростить:

```
<A HREF="#метка" >Текст </A>.
```

Для того чтобы встроить растровое изображение в документ HTML, необходимо использовать тег <IMG>. Общий вид этого тега показан ниже:

```
<IMG SRC="Адрес_файла_изображения"
NAME="Имя_изображения"
. . .
WIDTH="Ширина" HEIGHT="Высота">
```

Здесь указаны только три параметра. Полный список параметров тега <IMG> с кратким их описанием приведен в табл. 7.1.

Таблица 7.1. **Параметры тега <IMG>**

Параметр	Описание
SRC	Адрес URL-файла с растровым графическим изображением
NAME	Имя объекта, соответствующего растровому графическому изображению. Это имя может быть использовано для ссылки на объект в клиентском сценарии
ALT	Текстовая строка, которая отображается в тех случаях, когда браузер не может показывать графические изображения или когда такая возможность отключена
ALIGN	Выравнивание текста относительно графического изображения: LEFT — по левой границе; RIGHT — по правой границе; TOP — по верхней границе; MIDDLE — по центру изображения; BOTTOM — по нижней границе; TEXTTOP — выравнивание по верхней границе относительно самых высоких символов в текстовой строке; ABSMIDDLE — выравнивание середины текстовой строки относительно середины изображения; BASELINE — выравнивание нижней рамки изображения относительно базовой линии текстовой строки; ABSBOTTOM — выравнивание нижней границы изображения относительно нижней границы текущей строки
HEIGHT	Высота изображения в пикселах
WIDTH	Ширина изображения в пикселах
BORDER	Ширина рамки (в пикселах) вокруг изображения (используется только браузером Netscape Navigator)
HSPACE	Ширина (в пикселах) свободного пространства, отделяющего изображение от текста по горизонтали
VSPACE	Ширина (в пикселах) свободного пространства, отделяющего изображение от текста по вертикали
USEMAP	Адрес URL-файла, содержащего так называемую карту изображения, которая используется для сегментированной графики
ISMAP	Этот параметр указывает, что данное изображение является сегментированным

Параметры тега <IMG> определяют адрес файла с изображением, выравнивание текста, расположенного возле изображения, и т. д. С помощью параметров HEIGHT и WIDTH выполняется масштабирование графических изображений. Значение этих параметров указано в процентах от ширины окна просмотра.

Масштабирование позволяет подготовить графический файл весьма небольшого размера: он занимает значительную площадь в окне браузера, но быстро передается через Internet. Однако масштабирование сегментированных графических и фоновых изображений невозможно.

Если в документе HTML размещено несколько растровых изображений, то можно адресовать соответствующие объекты как элементы массива document.images. Например, первое изображение адресуется следующим образом: document.images[0]. Однако в некоторых случаях удобнее пользоваться именами изображений, определенными параметром NAME оператора <IMG>. Объект-изображение имеет свойство src, соответствующее параметру SRC оператора <IMG>. Адресуясь к этому свойству, можно не только определять текущий адрес URL-изображения, но и задавать новый.

Рассмотрим фреймовую структуру организации HTML-документа, когда окно просмотрщика (браузера) разделено на несколько частей, в каждую из которых выводится свой HTML-документ. Такая организация наиболее удобна для организации сайта или компьютерного учебника, так как позволяет совмещать удобную навигацию в пространстве сайта или учебника с удобным представлением его информации. Например, удобно разделять окно браузера на три части (три фрейма): в левой части расположить оглавление сайта (учебника) с гиперссылками на соответствующие информационные разделы, в правой части выводить содержание информационного раздела, к которому произведено обращение из фрейма оглавления, а в верхней части выводить название соответствующего информационного раздела (рис. 7.3).

Для того чтобы объединить несколько страниц HTML с помощью фреймов, нужно подготовить специальный документ HTML, в котором описаны такие параметры фреймов, как их размер и расположение.

Особенность такого документа — отсутствие на своем обычном месте области тела документа, выделенного тегами <BODY> и </BODY>. Вместо этого в файле описания фреймов присутст-

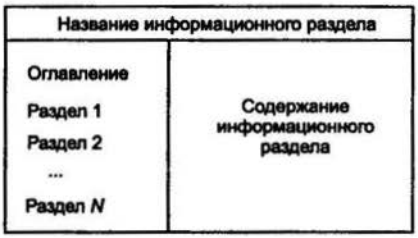

Рис. 7.3. Организация окна сайта или компьютерного учебника в виде фреймов

вуют теги <FRAMESET>, </FRAMESET>, <NOFRAME> и </NOFRAME>:

```
<html>
<head>
. . .
</head>
<frameset rows="Высота_строки" cols="Ширина_колонки"
   <frame src="Адрес_URL" name="Имя_фрейма">
   . . .
   <frame src="Адрес_URL" name="Имя_фрейма">
   <noframe>
      <body>
      . . .
      </body>
   </noframe>
</frameset>
</html>
```

Параметры rows и cols тега <FRAMESET> определяют размеры фреймов и задаются в виде списка значений, разделенных запятой.

Для тех браузеров, которые не могут работать с фреймами, необходимо подготовить документ HTML, расположив его тело между операторами <NOFRAHE> и </NOFRAME>. В этот документ стоит поместить сообщение о том, что для просмотра данной страницы Web необходимо применять более современный браузер.

Параметры тега <FRAMESET>

Рассмотрим подробнее параметры оператора <FRAMESET>, предназначенного для определения набора фреймов. Эти параметры описаны в табл. 7.2.

Таблица 7.2. **Параметры тега <FRAMESET>**

Параметр	Описание
COLS	Ширина колонки в процентах, пикселах или ее относительный размер
ROWS	Высота строки в процентах, пикселах или ее относительный размер
FRAMEBORDER	Если значение этого параметра равно 1, фреймы будут ограничены трехмерной рамкой, ширина которой задается в пикселах. В том случае, когда указано значение 0, рамка не создается
BORDER	Используется только браузером Netscape Navigator. Задает толщину рамки фрейма в пикселах
FRAMESPACING	С помощью этого параметра задается дополнительное расстояние между фреймами в пикселах

Параметры COLS и ROWS нужны в том случае, когда фреймы, определенные в наборе, располагаются в виде таблицы. Первый из этих параметров указывает ширину колонки, а второй — высоту строки. Если фреймы располагаются в одном столбце, параметр COLS указывать не надо. Аналогично, если фреймы занимают только одну строку, не нужно указывать параметр ROWS.

Можно задать значения для параметров COLS и ROWS либо в процентном отношении соответственно к ширине и высоте окна браузера, либо в пикселах. Если вместо значения указан символ "*", колонка или строка занимают всю оставшуюся часть окна.

Например, в следующей строке задана высота первого фрейма, равная 80 пикселам, а второй фрейм занимает всю нижнюю часть окна браузера:

```
<FRAMESET ROWS="90,*">
```

В следующем примере два фрейма, расположенные рядом, занимают соответственно 20 и 80 % ширины окна браузера

```
<FRAMESET COLS="20%, 80%">
```

Параметры оператора <FRAME>

Между тегами <FRAMESET> и </FRAMESET> располагаются теги <FRAME>, определяющие параметры отдельных фреймов. Это параметры SRC и NAME. Первый задает адрес URL документа HTML, который будет загружен в данный

фрейм, а второй — имя фрейма, которое можно использовать в клиентском сценарии для адресации объектов, расположенных во фрейме. Параметры тега <FRAME> приведены в табл. 3.2.

Таблица 3.2. **Параметры тега <FRAME>**

Параметр	Описание
MARGINHEIGHT	Используется только для «плавающих» фреймов в браузере Microsoft Internet Explorer. Задает выравнивание фрейма или текста, расположенного рядом с фреймом. Этот параметр может принимать следующие значения: LEFT, CENTER, RIGHT, TOP, BOTTOM
MARGINWIDTH	Размер отступа (в пикселах) по вертикали от границ фрейма
FRAMEBORDER	Размер отступа (в пикселах) по горизонтали от границ фрейма. Если значение этого параметра равно 1, фреймы ограничены трехмерной рамкой, ширина которой задается в пикселах. В том случае, когда указано значение 0, рамка не создается
NAME	Этот параметр задает имя фрейма, которое используется в теге ссылки <A> для указания, в какой фрейм нужно загрузить новый документ
NORESIZE	Если указан этот параметр, пользователь не сможет изменять размеры фрейма, передвигая его границы мышью
SCROLLING	Параметр SCROLLING определяет, нужно ли создавать полосы просмотра для пролистывания содержимого фрейма. Для этого параметра можно указывать следующие значения: YES — полосы просмотра создаются всегда; NO — полосы просмотра не создаются; AUTO — полосы просмотра создаются только при необходимости, когда документ HTML не помещается полностью в окне фрейма
SRC	Адрес URL-файла с документом HTML, который загружается в окно фрейма

Взаимодействие между фреймами

Средства клиентских сценариев, составленных на языках программирования, позволяют наделить фреймы возможностями, недостижимыми при использовании одного лишь языка разметки гипертекста HTML. Например, один из фреймов может содержать ссылки на документы, которые при активизации этих ссылок загружаются в окно другого фрейма. Клиентский сценарий позволит таким образом загружать не один документ, а одновременно несколько документов в разные фреймы.

Большую известность приобрели технология и язык программирования сетевых приложений Java, разработаные фирмой Sun Microsystems для систем распределенных вычислений.

Язык Java объектно-ориентированный, по сравнению с C++ Java более прост в использовании (так, например, убраны указатели), в нем введены многопотоковость и дополнительная защита от вирусов.

Для пользователей важны также следующие черты языка:

- аппаратная независимость (мобильность) за счет создания приложений в виде байт-кодов для некоторой виртуальной машины — каждая аппаратная платформа интерпретирует эти байт-коды; благодаря введению компиляции потеря эффективности, присущая интерпретации, здесь менее значительна;
- интеграция с браузерами;
- используемые программные объекты могут находиться в разных узлах, интерпретатор находит их и загружает в компьютер пользователя.

Другими словами, в узле-клиенте достаточно иметь лишь браузер, все остальное можно получить по сети. Однако при этом обостряется проблема информационной безопасности. В связи с этим загружаемым по сети программам (они называются *аплетами*) обычно запрещается обновлять и читать файлы, кроме тех, которые находятся на компьютере самого аплета.

Java-аплеты доступны из HTML-документов (обращение к ним производится через тег <applet>), хотя могут использоваться и независимо от них. При обращении к аплету он компилируется на сервере, а для исполнения передается клиенту вместе с Web-страницей.

Большое распространение получил интерфейс CGI (Common Gateway Interface — общий шлюзовой интерфейс) — программное обеспечение связи HTML-браузеров с другими прикладными программами и/или текстами, находящимися на серверной стороне.

Программа CGI — посредник между браузером и приложениями. Обычно программа CGI находится на сервере в специальном каталоге CGI_BIN, она является обработчиком запросов, идущих от браузера. Обращение к файлу из этого каталога означает запуск соответствующего обработчика. Если браузер обращается к документу не в HTML-формате, то CGI преобразует форму документа в HTML и возвращает ее браузеру.

В гипертекстовых документах также широко используется JavaScript — язык и интерпретатор этого языка для генерации и управления просмотром составных гипертекстовых документов. JavaScript более прост, чем Java, и тексты JavaScript исполняются быстрее, чем тексты Java или запросы к CGI, поскольку обработчики событий JavaScript реализованы в браузере, а не на сервере. Тексты на JavaScript записываются непосредственно в HTML-документе с помощью специальных тегов и имеют вид:

```
<SCRIPT LANGUAGE = "javascript"> <!- — . . . //- ->
</SCRIPT>
```

где <!- — . . . //- -> — текст в виде комментария.

В отличие от Java программы на JavaScript полностью интерпретируются в браузере.

Для разработки приложений в Internet уже созданы специальные языки и средства. Это, кроме упомянутых языков, также язык Visial Basic Script (VBScript).

Microsoft разработала технологию создания и использования интерактивных сетевых приложений, названную ActiveX. Некоторые компоненты ActiveX передаются в составе HTML-документов, другие служат для взаимодействия сервера с приложениями. Microsoft предлагает среду разработки Web-документов и приложений, включающую ряд продуктов, например:

- Internet Assistant — служит для создания HTML-документов, использует возможности редактора Word, взаимно преобразует форматы документов HTML и Word;
- FrontPage — применяется Web-мастерами и администраторами для сопровождения гипертекстовой информационной базы;
- Internet Studio — помогает художественному оформлению Web-страниц;
- Visual J++ в составе компилятора Java, набора JDK, средств взаимодействия Java-аплетов и ActiveX-компонентов, и др.

Internet-функции становятся неотъемлемой частью сетевых операционных систем. Так, в ОС Windows NT, начиная с версии 4.0, входит Internet-сервер IIS (Internet Information Server), реализующий технологии WWW, Gopher, FTP, ISAPI.

В качестве примера рассмотрим методику создания простейшего компьютерного учебника в формате HTML, использующего фреймовую структуру.

Методика создания компьютерного учебника в формате HTML

1. **Подготовить все разделы учебника** (оглавление, названия информационных разделов, главы, параграфы, примеры, контрольные вопросы и т. д.) **в текстовом редакторе Word и сохранить их в виде отдельных файлов**, например, oglavlenie.doc, title1.doc, title2.doc, ..., titleN.doc, ch1. doc, 1.1. doc, 1.2. doc, ..., 1.N. doc, ch2. doc, 2.1. doc, 2.2. doc, ..., 2.N. doc, ..., chN. doc, N.1. doc, N.2. doc, ..., N.N. doc.

2. **Преобразовать все файлы разделов Учебника в формат HTML**, для этого использовать опцию меню «Файл\Сохранить в формате HTML». Например, oglavlenie.html, title1. html, title2. html, ..., titleN. html, ch1.html, 1.1.html, 1.2.html, ..., 1.N.html, ch2.html, 2.1.html, 2.2.html, ..., 2.N.html, ..., chN.html, N.1.html, N.2.html, ..., N.N.html.

3. **Организовать основной загрузочный файл Учебника index.html, из которого будет осуществляться управление Учебником.**

В нашем случае создается HTML-файл с именем index.html, который является основным (первоначально загружающимся) файлом компьютерного учебника, из которого осуществляется все дальнейшее управление Учебником

```
<html>
<head>
<title>Название учебника</title>
</head>
<frameset FRAMEBORDER="1" rows="100,*">
<frame SCROLLING="no" NAME="title" SRC="title.html"
MARGINHEIGHT="1">
<frameset FRAMEBORDER="1" cols="300,*">
<frame SCROLLING="auto" NAME="oglavlenie"
SRC="oglavlenie.html">
<frame SCROLLING="auto" NAME="main" SRC="main.html">
</frameset>
<noframes>
<body BGCOLOR="#FFFFFF">
</body>
</noframes>
</frameset>
</html>
```

В нашем примере мы создаем три фрейма с именами oglavlenie, title и main. Результатом открытия этого файла в браузере является появление окна, представленного на рис. 7.4.

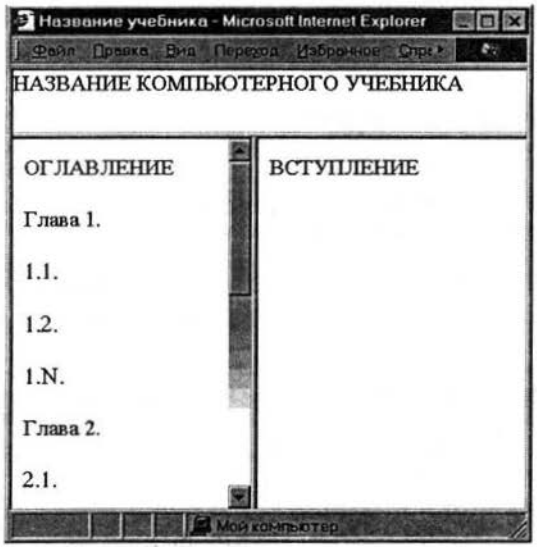

Рис. 7.4. Многофреймовое окно Учебника

4. **Организовать гипертекстовую среду Учебника.** Последним шагом в разработке компьютерного учебника является реализация гиперссылок из фрейма oglavlenie, загружающих соответствующие HTML-документы во фреймы title и main. Для этого следует открыть в программе Блокнот файл oglavlenie.html и вставить в него после тега <body> следующую запись:

```
<P><SCRIPT LANGUAGE="JavaScript"><!--
 function loadPage(szNewURL,szTitle)
 {
  parent.main.window.location.href=szNewURL;
  parent.title.window.location.href=szTitle;
 }
 // --></SCRIPT>
```

В каждую строку оглавления, из которой осуществляется гиперссылка к какому-либо информационному разделу, следует вставить запись, указывающую, какие файлы будут загружаться во фреймы main и title:

```
<A HREF="javascript:loadPage('Имя html-файла, помещаемого
в фрейм main',' Имя html-файла, помещаемого в фрейм
title');">
```

Получаем следующий код для файла oglavlenie.html:

```
<HTML>
<HEAD>
<TITLE>ОГЛАВЛЕНИЕ</TITLE>
</HEAD>
<BODY>
<P><SCRIPT LANGUAGE="JavaScript"><!--
   function loadPage(szNewURL,szTitle)
   {
   parent.main.window.location.href=szNewURL;
   parent.title.window.location.href=szTitle;
   }
   // --></SCRIPT>
<FONT FACE="Times New Roman"><P>ОГЛАВЛЕНИЕ</P>
<P><A
HREF="javascript:loadPage('ch1.html','title.html');">
Глава1.</P> </FONT>
<P><A HREF=
"javascript:loadPage('1.1.html','title.html');">1.1.
</P>
<P><A HREF=
"javascript:loadPage('1.2.html','title.html');">1.2.</P>
<P><A HREF=
"javascript:loadPage('1.N.html','title.html');">1.N.</P>
<FONT FACE="Times New Roman">
<P><A HREF=
"javascript:loadPage('ch2.html','title.html');">Глава
2.</P></FONT>
<P><A HREF=
"javascript:loadPage('2.1.html','title.html');">2.1.</P>
<P><A HREF=
"javascript:loadPage('2.2.html','title.html');">2.2.</P>
<P><A HREF=
"javascript:loadPage('2.N.html','title.html');">2.N.</P>
<FONT FACE="Times New Roman">
<P><A HREF=
"javascript:loadPage('chN.html','title.html');">Глава
N.</P> </FONT>
<P><A HREF=
"javascript:loadPage('N.1.html','title.html');">N.1.</P>
<P><A HREF=
"javascript:loadPage('N.2.html','title.html');">N.2.</P>
<P><A HREF=
"javascript:loadPage('N.N.html','title.html');">N.N.</P>
</BODY>
</HTML>
```

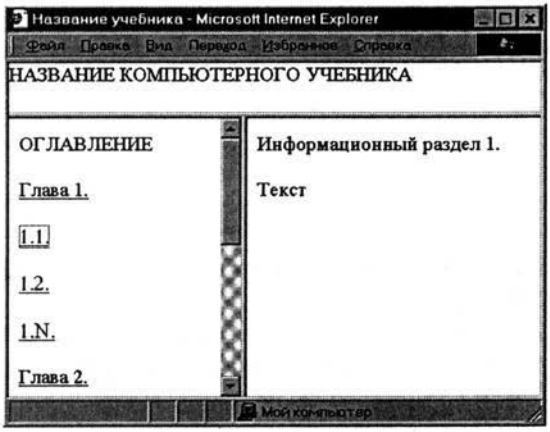

Рис. 7.5. Окно Учебника в формате HTML

После указанной процедуры открытый в браузере основной управляющий файл Учебника index.html, приобретает вид, представленный на рис. 7.5.

Контрольные вопросы

1. Опишите структуру территориальных сетей.
2. Какие типовые информационные услуги предоставляют территориальные сети?
3. Охарактеризуйте протоколы файлового обмена.
4. Охарактеризуйте протоколы электронной почты.
5. Какие протоколы дистанционного управления существуют?
6. Какие виды конференц-связи применяются в современных телекоммуникациях?
7. Охарактеризуйте современные WEB-технологии и области их применения.
8. Расскажите о языках и средствах создания WEB-приложений.
9. Составьте программу на языке HTML для создания простейшего гипертекстового документа.
10. Составьте программу на языке HTML для создания простейшего HTML-документа фреймовой структуры.

Список литературы

1. *Бройдо В. Л.* Вычислительные системы, сети и телекоммуникации. СПб.: Питер, 2002.

2. *Закер К.* Компьютерные сети. Модернизация и поиск неисправностей / пер. с англ. СПб.: БХВ — Петербург, 2002.

3. *Олифер В. Г., Олифер Н. А.* Компьютерные сети. Принципы, технологии, протоколы. СПб.: Питер, 2007.

4. *Остерлох Х.* Маршрутизация в IP-сетях. Принципы, протоколы, настройки : пер. с англ. СПб.: ДиаСофтЮП, 2002.

5. *Пакет К., Тир Д.* Создание масштабируемых сетей CISCO : пер. с англ. М.: Вильямс, 2002.

6. *Пескова С. А., Кузин А. В., Волков А. Н.* Сети и телекоммуникации. М.: Академия, 2009.

7. *Таненбаум Э.* Компьютерные сети. СПб.: Питер, 2002.

Оглавление

Александр Владимирович Кузин

Компьютерные сети

Учебное пособие

Редактор *А. В. Волковицкая*
Корректор *А. В. Алёшина*
Компьютерная верстка *И. В. Кондратьевой*
Оформление серии *П. Родькина*

Подписано в печать 14.06.2010. Формат $60 \times 90^1/_{16}$.
Печать офсетная. Гарнитура «Таймс». Усл. печ. л. 12,0. Уч.-изд. л. 12,4.
Бумага офсетная. Тираж 1500 экз. Заказ № 3765.

Издательство «ФОРУМ»
101990, Москва — Центр, Колпачный пер., д. 9а
Тел./факс: (495) 625-32-07, 625-52-43
E-mail: forum-knigi@mail.ru

По вопросам приобретения книг обращайтесь:

Отдел продаж издательства «ФОРУМ»
101990, Москва — Центр, Колпачный пер., д. 9а
Тел./факс: (495) 625-52-43
E-mail: alla-forum@mail.ru
www.forum-books.ru

Отдел продаж «ИНФРА-М»
127282, Москва, ул. Полярная, д. 31в
Тел.: (495) 380-05-40 (доб. 252)
Факс: (495) 363-92-12
E-mail: ati@infra-m.ru

Отдел «Книга-почтой»
E-mail: podpiska@infra-m.ru;
books@infra-m.ru

Отпечатано с готовых диапозитивов в ОАО ордена «Знак Почета»
«Смоленская областная типография им. В. И. Смирнова».
214000, г. Смоленск, проспект им. Ю. Гагарина, 2.