Профессиональное образование

ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

Е. О. Новожилов
О. П. Новожилов

КОМПЬЮТЕРНЫЕ СЕТИ

Учебное пособие

ACADEMA

ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАНИЕ

Е.О.НОВОЖИЛОВ, О.П.НОВОЖИЛОВ

КОМПЬЮТЕРНЫЕ СЕТИ

Рекомендовано
Федеральным государственным автономным учреждением
«Федеральный институт развития образования» (ФГАУ «ФИРО»)
в качестве учебного пособия для использования
в учебном процессе образовательных учреждений,
реализующих программы среднего профессионального
образования по специальности «Информационные системы (по отраслям)»

Регистрационный номер рецензии 423
от 24 июля 2012 г. ФГАУ «ФИРО»

4-е издание, стереотипное

ACADEMIA

Москва
Издательский центр «Академия»
2014

УДК 004.7(075.32)
ББК 32.973.202.2я723
Н741

Рецензент —
старший научный сотрудник ГНУ ГОСНИТИ Россельхозакадемии *А. А. Соломашкин*

Новожилов Е. О.

Н741 Компьютерные сети : учеб. пособие для студ. учреждений сред. проф. образования / Е. О. Новожилов, О. П. Новожилов. — 4-е изд., стер. — М. : Издательский центр «Академия», 2014. — 224 с.

ISBN 978-5-4468-1405-3

Рассмотрены компьютерные сети и тенденции их развития. Описаны модель взаимодействия открытых систем и стандартные стеки коммуникационных протоколов. Приведены основные понятия. Изложен широкий круг вопросов, касающихся структурно-функциональной организации сетей, формирования и обработки сигналов, межсетевого взаимодействия, оборудования сетей и сетевых технологий. Даны сведения по наиболее распространенным архитектурам локальных и глобальных сетей. Значительное внимание уделено административному управлению, безопасности и мониторингу сетей, а также возможным неисправностям в сетях и их устранению.

Учебное пособие может быть использовано при изучении общепрофессиональной дисциплины «Компьютерные сети» в соответствии с требованиями ФГОС СПО для специальности «Информационные системы (по отраслям)».

Для студентов учреждений среднего профессионального образования.

УДК 004.7(075.32)
ББК 32.973.202.2я723

ISBN 978-5-4468-1405-3

Уважаемый читатель!

Данное издание является частью учебно-методического комплекта по специальности 230401 «Информационные системы (по отраслям)».

Учебное пособие предназначено для изучения дисциплины «Компьютерные сети».

Учебно-методические комплекты нового поколения включают в себя традиционные и инновационные учебные материалы, позволяющие обеспечить изучение общеобразовательных и общепрофессиональных дисциплин и профессиональных модулей. Каждый комплект содержит учебники и учебные пособия, средства обучения и контроля, необходимые для освоения общих и профессиональных компетенций, в том числе и с учетом требований работодателя.

Учебные издания дополняются электронными образовательными ресурсами. Электронные ресурсы содержат теоретические и практические модули с интерактивными упражнениями и тренажерами, мультимедийные объекты, ссылки на дополнительные материалы и ресурсы в Интернете. В них включен терминологический словарь и электронный журнал, в котором фиксируются основные параметры учебного процесса: время работы, результат выполнения контрольных и практических заданий. Электронные ресурсы легко встраиваются в учебный процесс и могут быть адаптированы к различным учебным программам.

Учебно-методический комплект разработан на основании Федерального государственного образовательного стандарта среднего профессионального образования с учетом его профиля.

Предисловие

Компьютерные сети и сетевые технологии оказывают постоянно возрастающее влияние на все стороны нашей жизни. Их стремительное развитие требует широких и глубоких знаний, чему способствует введение дисциплины по компьютерным сетям в стандарты и учебные планы многих специальностей.

Цель учебника — дать целостное представление о компьютерных сетях: об основных понятиях, назначении, разновидностях, концепциях, технологиях, протоколах и администрировании сетей, а также тенденциях их развития.

Учебник содержит восемь глав.

В *главе 1* изложены вопросы структурно-функциональной организации сетей. Определены основные понятия, рассмотрена обобщенная структура телекоммуникационной сети, дана классификация и приведены принципы организации сетей по таким признакам, как архитектура, топология, операционная система, способ администрирования сети и др. Рассмотрены характеристики сетей и качество услуг, основные типы сетевых устройств и виды сред передачи данных.

В *главе 2* показана роль стандартизации и сетевых моделей для построения сетей и разработки сетевых технологий. Приведено описание семиуровневой сетевой модели. Рассмотрены стеки протоколов TCP/IP и IPX/SPX.

Глава 3 посвящена вопросам, связанным с переходом от исходного сообщения (информации) к сигналам, передаваемым по линиям связи: сигналы и их представление, кодирование, модуляция, мультиплексирование и демультиплексирование, компрессия-декомпрессия данных, обнаружение и исправление ошибок.

В *главе 4* рассмотрены базовые сетевые технологии: методы доступа к сети, коммутации и передачи данных, адресации узлов сети и маршрутизации.

Глава 5 посвящена сетевому оборудованию. Рассмотрены линии связи и их основные характеристики, проводные и беспроводная среды передачи данных. Показаны особенности использования мостов для логической структуризации сети. Приведена

схемная реализация коммутатора, дано описание принципа его работы и выполняемые функции.

В *главе 6* основное внимание уделено наиболее распространенным в нашей стране локальным сетям Ethernet. Рассмотрены особенности других архитектур сетей.

В *главе 7* представлены структура и состав, стандартные интерфейсы и общие сведения о различных типах глобальных сетей. Рассмотрены сети с коммутацией каналов и пакетов: сети плезиохронной (PDH) и синхронной (SDH/SONET) цифровых иерархий, цифровая абонентская линия DSL, сети с уплотненным волновым мультиплексированием (DWDM), сети X.25, Frame Relay, ISDN и ATM. Приведены краткие сведения об Internet.

В *главе 8* изложены основополагающие вопросы администрирования сетей. Рассмотрены основные задачи, принципы и некоторые виды управления сетями; основные понятия, политика, планирование, средства и технологии безопасности; основные понятия, термины, задачи и средства мониторинга сетей, а также возможные неисправности в сетях и их устранение.

При написании учебника авторы стремились учесть современные тенденции развития сетей и сетевых технологий. При этом большое внимание уделено выбору содержания тем и последовательности их изложения. Для лучшего восприятия и понимания сути излагаемых вопросов материал подробно структурирован, использованы текстовые выделения, дано большое количество иллюстраций.

Авторы надеются, что приведенный в учебнике материал поможет учащимся сформировать целостное представление об основных концепциях и общих тенденциях развития компьютерных сетей.

Глава 1

СТРУКТУРНО-ФУНКЦИОНАЛЬНАЯ ОРГАНИЗАЦИЯ СЕТЕЙ

1.1. ОБЩИЕ СВЕДЕНИЯ

Появление компьютерных сетей обусловлено развитием вычислительной техники и телекоммуникационных технологий. Компьютерную сеть можно представить:

- как распределенную вычислительную систему, в которой группа компьютеров решает одну общую задачу, обмениваясь между собой данными в автоматическом режиме;
- систему передачи информации на большие расстояния, в которой используются способы обработки данных (кодирования, мультиплексирования и др.), присущие различным телекоммуникационным технологиям.

К первой компьютерной сети относят *глобальную сеть* с коммутацией пакетов ARPAnet (**A**dvanced **R**esearch **P**rojects **A**gency **net**work — сеть управления перспективного планирования научно-исследовательских работ), которая была создана в 1969 г. в США для объединения суперкомпьютеров оборонных и научно-исследовательских центров, находящихся в разных городах. Появлению и развитию глобальных сетей способствовало наличие телефонных линий передачи, которые с помощью модемов обеспечивали многочисленным пользователям удаленный доступ к разделяемым ресурсам мощных компьютеров класса суперЭВМ.

Внедрению и интенсивному развитию *локальных сетей* (ЛС) способствовала разработка больших интегральных схем и создание на их основе персональных компьютеров. Появление таких сетей относится к началу 1980-х гг., когда широко распространенный компьютер Apple II и накопители на жестких магнитных дисках (винчестеры) к нему были тогда еще настолько дорогими, что колледжи не могли приобретать их для организации обучения. Компания *Corvus* обратила внимание на эту проблему и создала первую локальную вычислительную сеть, предназначенную для

использования в системе школьного образования. Школы приобретали один винчестер достаточно большой емкости, нужное число компьютеров Apple II без дисководов и соединяли их посредством локальной вычислительной сети. Каждый школьник как пользователь Apple II получал через сеть доступ к винчестеру и иллюзорно становился его единоличным обладателем.

В последние годы проявились и стали нарастать тенденции глубокого и всестороннего сближения, или *конвергенции* (Convergence), различных видов телекоммуникационных сетей, что обусловлено широким распространением компьютеров и цифровых методов обработки информации.

Телекоммуникационная сеть и ее составные части. Термин «телекоммуникация» (от греч. *tele* — далеко, вдаль и от лат. *communico* — делаю общим, связываю) можно трактовать как связь на расстоянии, поэтому под *телекоммуникационной сетью* будем понимать совокупность средств, обеспечивающих передачу информации между двумя оконечными устройствами (абонентами). В состав сети входят:

- *сетевое оборудование*. Включает в себя *оконечные* устройства (персональные компьютеры, серверы, аудио- и видеоустройства, сетевые принтеры, факс-аппараты, считыватели штрихкодов и др.) и *коммуникационное* оборудование (проводная, кабельная и (или) беспроводная среда передачи данных, а также такие промежуточные устройства, как сетевые адаптеры, модемы, повторители, мосты, коммутаторы и др.);
- *средства поддержки сетевого оборудования*. В такой сложной системе, какой является телекоммуникационная сеть, необходимо иметь более широкий арсенал программного обеспечения, а также стандартные наборы (стеки) коммуникационных протоколов, которые определяют правила взаимодействия сетевых устройств.

Структура телекоммуникационной сети. Телекоммуникационная сеть имеет иерархическую структуру (рис. 1.1), отражающую интенсивность трафика между отдельными ее узлами, расположенными в различных зданиях, населенных пунктах и регионах. Узлами сети являются *коммутаторы*, представляющие собой многопортовые устройства, к которым подключены линии связи. Рассмотрим отдельные компоненты телекоммуникационной сети.

Терминальные устройства пользователей расположены на периферии телекоммуникационной сети и составляют самый нижний уровень ее иерархии. Обычно тип используемых

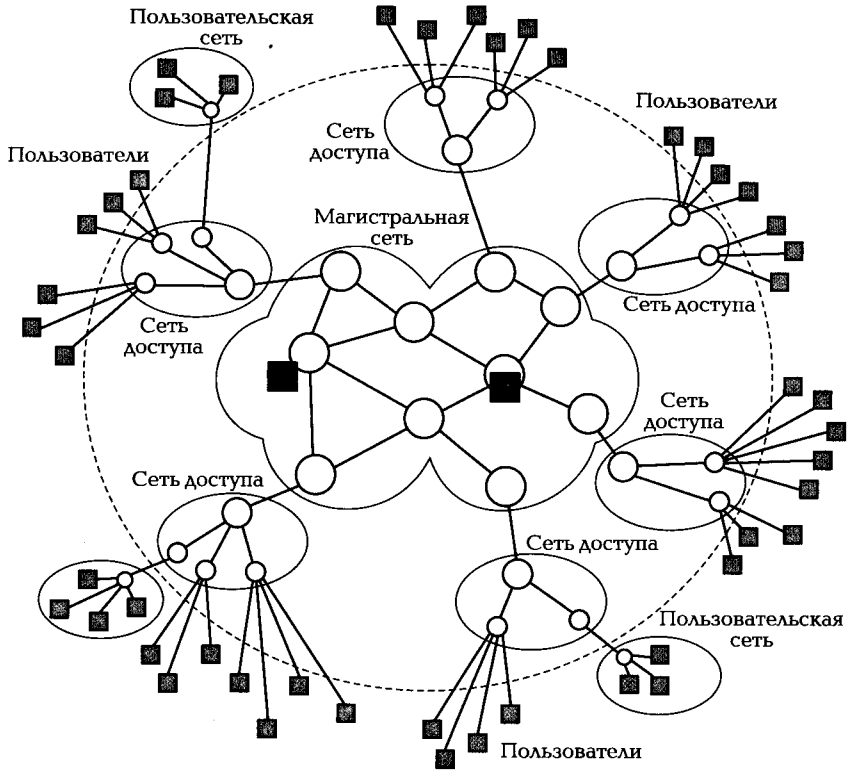
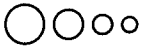


Рис. 1.1. Обобщенная структура телекоммуникационной сети:

 — коммутаторы; ■ — информационный центр; ■ — терминальное устройство

терминальных устройств определяет название сети. Основными терминальными устройствами в компьютерной сети являются компьютеры, в телефонной — телефонные аппараты, в телевизионной — телевизионные приемники, в радиовещательной — радиоприемники.

Информация от пользователей по абонентским каналам, часто называемым *абонентскими окончаниями*, поступает на коммутаторы сети доступа.

Сеть доступа представляет следующий уровень иерархии телекоммуникационной сети. Крупная сеть доступа может состоять из нескольких уровней. Основные функции сети доступа состоят:

- *в объединении*, или *мультиплексировании*, информационных потоков, поступающих от многочисленных пользовательских устройств, в один общий поток, и передаче агрегированного потока в коммутатор магистральной сети;
- *приеме и разделении*, или *демультиплексировании*, агрегированного потока на отдельные потоки таким образом, чтобы на входной порт оборудования пользователя поступала только адресованная ему информация.

Магистральная сеть предназначена для транзита агрегированных информационных потоков из сети доступа отправителей в сеть доступа получателей. Она содержит коммутаторы и высокоскоростные линии связи (магистрали).

Информационный центр, или центр управления сервисами, предназначен для оказания информационных услуг пользователям (абонентам) сети. Всем известны информационные услуги Internet, а также телефонных сетей (справочные услуги, вызов скорой помощи и милиции) и сетей сотовой связи (проведение телеголосования).

Отметим, что каждая телекоммуникационная сеть имеет свои особенности, например: в малых телефонных и компьютерных сетях отсутствуют информационные центры; сеть доступа и магистраль локальной компьютерной сети могут быть представлены отрезками кабеля; сеть доступа радиовещательной и телевизионной сетей выполняет только распределительные функции, поскольку информация в них передается в одном направлении (в сторону абонентов).

Основные понятия. Под *сетевой архитектурой* (Architecture) понимают совокупность средств, обеспечивающих полноценное функционирование сети. Архитектура сети дает полное представление о ее структурно-функциональной организации и возможностях по оказанию услуг абонентам. Это емкое понятие включает в себя:

- совокупность используемых базовых аппаратных средств и сетевых технологий;
- набор спецификаций (или стандартов), определяющих сетевую модель, физическую и логическую топологии, типы кабелей, ограничения на расстояние, методы сетевого доступа, размер пакетов, структуру заголовков и другие параметры и характеристики сети. *Спецификация* — это формализованное описание аппаратных и (или) программных компонентов, способов их взаимодействия с другими компонентами, условий эксплуатации, ограничений и особых характеристик;

- совокупность услуг, которыми могут пользоваться абоненты сети.

Под *сетевой технологией* понимают совокупность способов (методов, алгоритмов) обработки информации (цифровых данных), поддерживаемых соответствующими аппаратными средствами и программным обеспечением в процессе передачи информации от одного абонента сети к другому. Сетевая технология является составной частью архитектуры сети.

При классификации сетей по архитектуре часто выделяют основные общие признаки, присущие той или иной сети. Существуют следующие архитектуры *локальных сетей*: Ethernet, Token Ring, AppleTalk и ARCnet. В *глобальных сетях* выделяют архитектуры X.25, Frame Relay, ATM, ISDN и др.

1.2. КЛАССИФИКАЦИЯ СЕТЕЙ

В настоящее время в мире насчитывается огромное число различных телекоммуникационных сетей. Их основные классификационные признаки приведены в табл. 1.1.

Таблица 1.1

Признак	Перечень и название признаков или сетей
Тип оконечного устройства	Компьютерная, телефонная, телевизионная, радиовещательная, радиотелефонная и другие сети
Цель создания	Широковещание (телевизионная и радиовещательная сети). Двусторонний обмен (телефонная сеть, сеть сотовой связи). Передача цифровых данных (компьютерные сети, Internet)
Охват пользователей или территории	Локальная, городская, глобальная и другие сети
Топология и соединения	Шинная, кольцевая, звездообразная, древовидная, ячеистая, смешанная и другие топологии. Соединение точка — точка и один — ко многим
Среда передачи данных	Проводная среда (коаксиальный кабель, витая пара, оптоволокно). Беспроводная среда (канал радиосвязи, спутниковый канал, канал сотовой связи)

Окончвние табл. 1.1

Признак	Перечень и название признаков или сетей
Управление доступом к сети	Случайный и детерминированный доступ
Принцип организации обмена	Сети с коммутацией каналов, сообщений, пакетов
Принадлежность сети	Сеть оператора сети (поставщика услуг), частная, корпоративная, публичная сети
Выполняемые функции	Первичные и вторичные (наложенные) сети. Пользовательская сеть, сеть доступа, магистральная сеть
Однородность	Однородная сеть с однородным оборудованием. Неоднородная сеть с разнотипным оборудованием
Организация управления	Централизованное управление. Децентрализованное (распределенное) управление
Способ соединения	Физические сети с постоянным соединением абонентов. Виртуальные сети, соединения в которых могут изменяться

Среди компьютерных сетей важное место занимают локальные и глобальные сети.

Локальные сети (Local Area Network — LAN) обслуживают ограниченное число абонентов и располагаются на ограниченной площади. Примером могут служить сети Ethernet, Token Ring и др.

Глобальные сети (Wide Area Networks — WAN) охватывают большую географическую территорию с огромным количеством абонентов. К глобальным сетям относят Internet, ISDN, X.25, ATM и др.

С точки зрения *управления разделяемыми ресурсами*, или *администрирования*, компьютерные сети разбивают на одноранговые и сети клиент-сервер.

В *одноранговых сетях* пользователь самостоятельно управляет ресурсами своего компьютера, при этом каждый компьютер выполняет функции и клиента (Client — пользователь) и сервера (Server — обслуживающее устройство).

В *сетях клиент-сервер* все функции управления сосредоточены на центральном компьютере (сервере) со специальной сетевой операционной системой (ОС).

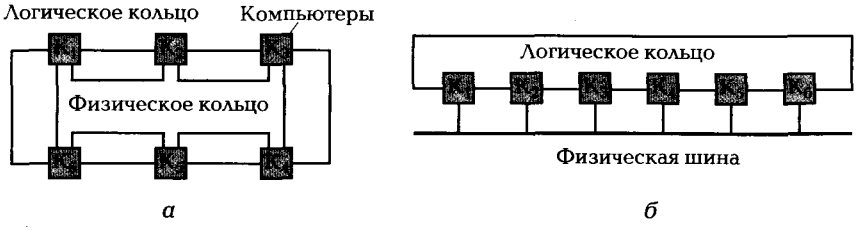


Рис. 1.2. Совпадение (*а*) и различие (*б*) физической и логической топологий сетей

Ознакомимся с другими признаками и наиболее распространенными типами сетей.

Топология сетей. Под *топологией* понимают конфигурацию или геометрическую структуру сети. Различают *физическую топологию*, определяющую правила физических соединений узлов сети или путь прокладки кабелей, и *логическую*, которая обусловливает направления потоков данных между узлами сети. Логическая и физическая топологии относительно независимы друг от друга: обе топологии могут совпадать (рис. 1.2, *а*) или отличаться одна от другой (рис. 1.2, *б*).

К наиболее распространенным относятся следующие физические топологии: шинная, кольцевая, звездообразная, полносвязная (табл. 1.2).

При *шинной топологии* сеть строится путем последовательного соединения отрезков кабеля от одного узла (компьютера) к другому. Совокупность отрезков образует шину (рис. 1.3, *а*). К каждому

Таблица 1.2

Виды топологии	Достоинства	Недостатки
Шинная	Простота и низкие затраты реализации	Сигналы подвержены затуханию. Обрыв кабеля приводит к выходу из строя всей сети
Кольцевая	Простота реализации и устранение неполадок	Требуется больше кабеля, чем для шины. Обрыв кабеля приводит к выходу из строя всей сети. Трудности при подключении нового компьютера

Окончание табл. 1.2

Виды топологии	Достоинства	Недостатки
Звездообразная и древообразная	При отключении компьютера сохраняется работоспособность сети. При использовании активного концентратора происходит усиление сигнала. Простота добавления и удаления компьютеров	Большие финансовые затраты, обусловленные увеличением длины кабеля и покупкой концентраторов
Полносвязная и ячеистая	Высокая надежность работы (отказоустойчивость)	То же

свободному концу шины должна быть подключена оконечная нагрузка Т, называемая *терминатором*. При отсутствии терминаторов происходит отражение сигнала, нарушающее нормальную работу сети. Один из терминаторов должен быть заземлен. Сообщения, посылаемые каждым компьютером, поступают на все подключенные к шине компьютеры. Сетевой адаптер каждого компьютера анализирует заголовки поступающих сообщений, по которым определяет, кому предназначено сообщение. Сообщение, посланное данному компьютеру, обрабатывается, в противном случае — отбрасывается.

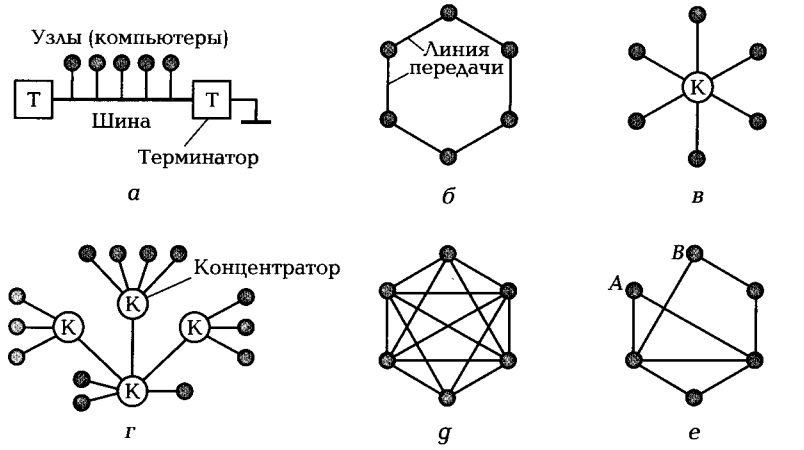


Рис. 1.3. Виды топологии сетей:

а — шинная; *б* — кольцевая; *в* — звездообразная; *г* — древообразная; *д* — полносвязная; *е* — ячеистая

Кольцевая топология (рис. 1.3, *б*) предусматривает, что сигнал проходит в одном направлении. Каждый компьютер принимает сигнал от одного соседа и посылает его другому соседу с требуемыми параметрами.

Звездообразная топология имеет ярко выраженный центральный узел (рис. 1.3, *в*), в качестве которого используется *концентратор* К. К концентратору подключены компьютеры и другие устройства сети. Со «звездой» схожа топология сети в виде *дерева* (рис. 1.3, *г*).

При *полносвязной топологии* (рис. 1.3, *д*) обеспечивается связь каждого компьютера со всеми остальными. Отсутствие некоторых (обычно редко используемых) связей приводит к *ячеистой*, или *неполносвязной топологии* (рис. 1.3, *е*). Ее особенность проявляется в том, что в сети имеется, по крайней мере, два компьютера (*А* и *В*), обмен данными между которыми необходимо осуществлять через транзитный узел.

Сети операторов связи. Под *оператором связи* (Telecommunication Carrier) понимают специализированное предприятие (организацию), владеющее телекоммуникационной сетью для оказания общедоступных услуг и поддерживающее ее работу. Оператор строит свою работу на коммерческой основе, заключая договоры с потребителями услуг. Операторы связи отличаются друг от друга набором предоставляемых услуг; территорией охвата; типом клиентов, на которых ориентируются их услуги; имеющейся в распоряжении инфраструктурой (линиями связи, коммутационным оборудованием, информационными серверами и т.п.). В современном конкурентном телекоммуникационном мире нет строгой иерархии операторов, взаимосвязи между ними и их сетями могут быть достаточно сложными и запутанными. По размерам территории, которую охватывают услуги операторов, выделяют локальных, региональных и национальных операторов связи.

Корпоративные сети (Corporative Network) предназначены для поддержания работы и обслуживания потребностей предприятия (корпорации), которое является владельцем сети, а его сотрудники — пользователями сети. Корпоративной выступает составная сеть, включающая в себя как локальные, так и глобальные сети. Для соединения удаленных ЛС и отдельных компьютеров применяют разнообразные телекоммуникационные средства (первичные сети, радиоканалы, спутниковую связь). Корпоративную сеть принято делить на сети отделов и рабочих групп, сети зданий и кампусов. Корпоративные сети не ограничиваются

только транспортными услугами, поскольку для предприятия не менее важными являются и *информационные услуги*.

Количество пользователей и компьютеров в корпоративной сети может составлять тысячи, а число серверов — сотни. Поскольку нельзя удовлетворить потребности тысяч пользователей с помощью однотипных аппаратных и программных средств, корпоративная сеть является сетью с высокой степенью неоднородности, или *гетерогенной сетью*. В ней используются различные типы компьютеров (от персональных компьютеров до мейнфреймов), несколько типов ОС и множество различных приложений. Неоднородные части корпоративной сети должны работать как единое целое, предоставляя пользователям доступ ко всем необходимым ресурсам. По мере увеличения масштабов сети повышаются требования к ее надежности, производительности, функциональным возможностям, безопасности и защищенности передаваемых данных.

Виртуальные частные сети (Virtual Private Network — VPN) создаются в целях:

- *предоставления удаленного доступа индивидуальным пользователям*, например служащим, находящимся в командировке. Его реализация может быть усложнена такими факторами, как разные ОС и протоколы, установленные на клиентских компьютерах. Клиентские компьютеры VPN должны поддерживать протоколы, используемые сервером (протоколы туннелирования, сетевой и транспортный протоколы), и методы шифрования, принятые в данной VPN;
- *создания экстрасети*, представляющей собой часть ЛС компании. В экстрасети могут храниться технические материалы для заказчиков или совместно используемые документы для партнеров компании, т.е. данные, не требующие защиты. Остальная часть внутренней сети должна быть защищена от внешнего доступа;
- *коммуникации двух офисов*, расположенных на большом расстоянии, без затрат на выделенные прямые каналы.

Виртуальная сеть — это сеть, которая накладывается на реальную физическую сеть путем создания виртуальных каналов источник — получатель. *Виртуальный канал* функционально эквивалентен выделенному логическому соединению точка — точка. Маршрут передачи данных не фиксирован, поэтому виртуальный канал может иметь различную конфигурацию в реальной сети. Данные передаются от узла к узлу, последовательно формируя двухточеч-

ные соединения по способу инкапсуляции данных. Суть *инкапсуляции* состоит в том, что в пакет, передаваемый через транзитные узлы сети, вводятся дополнительные заголовки, которые после прохождения каждого узла удаляются. Таким образом, технология VPN создает логическую сеть, независимую от места расположения терминальных устройств и непосредственных физических соединений. Виртуальный канал обычно создается в публичной сети (Internet) и называется *туннелем*. Частная сеть требует принятия дополнительных мер защиты передаваемой по VPN информации. Требование конфиденциальности особенно важно, потому что пакеты, передаваемые по публичной сети, уязвимы для перехвата при их прохождении через каждый из узлов (серверов) на пути от источника к получателю. Его реализация возлагается на туннели, которые должны поддерживать *аутентификацию* (проверку подлинности) пользователей и *шифрование* данных при их передаче с одного конца туннеля на другой.

Виртуальные частные сети строятся на основе технологий ATM и Frame Relay, рассмотренных в гл. 7.

Гибридные сети. Сеть, в которой используется разнотипный состав, т.е. содержит разные ОС, типы оборудования, протоколы и службы, называется *гибридной*. В современном корпоративном мире даже небольшие ЛС являются гибридными по всем перечисленным признакам, не говоря о такой глобальной сети, как Internet.

Сети с тонкими клиентами. Под *тонким клиентом* (Thin Client) понимают сетевой компьютер с ограниченными вычислительными ресурсами. Технология тонких клиентов позволяет использовать устаревшие или малопроизводительные компьютеры для выполнения многих популярных приложений, для которых нужен быстродействующий процессор и большой объем памяти. Для этого на компьютере устанавливается программное обеспечение, которое обеспечивает соединение с терминальным сервером и выполнение на нем необходимых программ. Тонкому клиенту по сети передаются лишь копии экрана.

1.3. ХАРАКТЕРИСТИКИ СЕТЕЙ И КАЧЕСТВО УСЛУГ

Виды услуг и требований к сетям. Основное предназначение телекоммуникационных сетей — оказание абонентам (клиентам, конечным пользователям сети) определенного набора услуг. Выделяют два вида услуг: транспортные и информационные.

Транспортные услуги состоят в передаче информации от одного абонента (клиента, пользователя) сети другому без внесения в нее каких-либо изменений. Например, транспортной услугой телефонной сети является передача голосового сообщения, компьютерной сети — электронная почта.

Информационные услуги предоставляют абоненту некоторую новую (например, справочную) информацию. Информационные услуги всегда связаны с операциями обработки информации (формирование нужных данных, хранение, поиск и преобразование к требуемому виду). Для их оказания применяются различные информационные средства и технологии (программирование, базы данных, файловые архивы).

Со стороны абонентов сетей существуют требования к *качеству сервисов* (Quality of Service — QoS), предоставляемых им поставщиками услуг. В частности, к поставщикам услуг Internet (Internet Service Provider — ISP) обычно относят организации (компании), которые обеспечивают передачу трафика конечных пользователей, т. е. выполняют только *транспортные* функции, например, поставщики услуг *по поддержке приложений* (Application Service Provider — ASP) предоставляют клиентам доступ к крупным универсальным программным продуктам и др.

Со стороны поставщиков услуг существуют свои требования к сетям. Поставщиков услуг могут интересовать характеристики ресурсов сетей, например, производительность коммуникационных устройств, возможности увеличения числа узлов сети и др.

Выделяют *субъективные требования*, обычно связанные с качеством информационных услуг, которые трудно или невозможно перевести в количественные показатели, и *формализованные требования* в виде конкретных показателей и характеристик качества сетевых услуг, позволяющих дать их количественную оценку.

Наиболее просто (хотя и не всегда) формализуются показатели качества транспортных услуг сети, которые и рассматриваются в дальнейшем.

Для пользователя наибольший интерес представляют три вида показателей: производительность, надежность и безопасность.

Производительность сети. Для ее оценки используют скорость и задержку передачи данных.

Скорость передачи данных — отношение объема переданных данных к длине временно́го интервала. В зависимости от длины интервала, на котором определяется скорость, используются средняя и пиковая скорости.

Задержка передачи данных — время запаздывания между моментом поступления пакета на вход какого-либо сетевого элемента (устройства) или части сети и моментом появления его на выходе этого устройства. Для количественной оценки используют такие статистические показатели, как среднее значение задержки, максимальная задержка, время реакции сети, джиттер, коэффициент вариации и др.

Надежность сетей. Для оценки надежности сетей используют следующие показатели:

- *доля потерянных пакетов* (L) — равна отношению числа потерянных пакетов (N_L) к общему количеству переданных пакетов (N), т. е. $L = N_L/N$;
- *коэффициент готовности* (Availability) — отражает долю времени, в течение которого система или служба сети доступна пользователю, т. е. находится в работоспособном состоянии. Например, коэффициент готовности коммуникационного оборудования телефонных сетей равен 0,99999, что соответствует примерно 5 мин простоя в год;
- *отказоустойчивость* (Fault Tolerance) — характеризует способность системы (сети) скрывать от пользователя отказ отдельных ее элементов.

Безопасность сетей (Security). Существует два вида средств безопасности компьютерных сетей.

1. *Средства защиты внутренних информационных ресурсов.* Эти средства должны защитить от несанкционированного доступа аппаратные ресурсы (серверы, дисковые массивы, маршрутизаторы), программные ресурсы (ОС, системы управления базами данных, почтовые службы) и сами данные, хранящиеся в файлах и обрабатываемые в оперативной памяти. Таким средством является *брандмауэр* (Firewall), устанавливаемый в местах всех соединений внутренней сети с внешней (Internet). Брандмауэр контролирует обмен данными и не пропускает подозрительный трафик во внутреннюю сеть.

2. *Средства защиты информации в процессе ее передачи через сеть.* К ним следует отнести виртуальные частные сети.

Показатели для поставщика услуг. Эти, чаще всего качественные, показатели используются для оценки эффективности сети.

Расширяемость (Expansibility) сети — это способность к расширению функциональных возможностей, добавлению пользователей, компьютеров, приложений, служб, наращиванию длины сегментов кабелей и замены существующей аппаратуры более мощной.

Масштабируемость (Scalability) сети — это способность к наращиванию количества устройств, узлов и протяженности связей сети без снижения ее производительности. Примером хорошо масштабируемой сети является Internet.

Управляемость (Controllability) сети — это возможность централизованного контроля состояния оборудования сети, выявление и разрешение возникающих проблем, анализ производительности и планирование развития сети, а также наличие в сети автоматизированных средств администрирования, взаимодействующих с программным и аппаратным обеспечением сети с помощью коммуникационных протоколов.

Совместимость (Compatibility) сети отражает способность включать в себя самое разнообразное программное и аппаратное обеспечение, поддерживающее разные стеки коммуникационных протоколов, аппаратные средства и приложения. Сеть, состоящая из разнотипных элементов, называется *неоднородной*, или *гетерогенной*. Основной путь построения интегрированных сетей — использование модулей, выполненных в соответствии с открытыми стандартами и спецификациями.

Качество обслуживания. Использование в компьютерных и других телекоммуникационных сетях принципа коммутации пакетов сделало актуальной проблему качества обслуживания (Quality of Service — QoS). Суть проблемы состоит в том, что принцип коммутации требует буферной памяти для хранения пакетов, чтобы избежать их потерь. Буферизация пакетов является основным механизмом поддержания высокой производительности и служит защитой от перегрузок сети при передаче *трафика* (пульсирующего потока данных). Однако буферизация создает очереди, которые вызывают неопределенную задержку пакетов, что весьма нежелательно для чувствительного к задержкам трафика (звук, видео). Методы обеспечения качества обслуживания QoS минимизируют задержки для чувствительного к ним трафика и гарантируют среднюю скорость передачи для эластичного трафика данных. Без их применения невозможна работа таких современных мультимедийных приложений, как IP-телефония, видео- и радиовещание. В настоящее время разработано большое число различных методов и алгоритмов (приоритетные и взвешенные очереди, алгоритмы «дырявого» и «маркерного ведра», резервирование и др.), обеспечивающие качество обслуживания для чувствительного к задержкам и эластичного трафика. К методам обеспечения качества обслуживания примыкают методы *инжиниринга трафика*, которые состоят в выборе рациональных маршрутов прохождения трафика через сеть.

1.4. СЕТЕВЫЕ УСТРОЙСТВА

Оконечные сетевые устройства. К ним относят терминальное (конечное) оборудование данных (Data Terminal Equipment — DTE), выполняющее функции источника и приемника информации, передаваемой по сети.

В настоящее время универсальным оконечным устройством является компьютер, который может быть использован:

- как *рабочая станция* (Workstation), или *клиентский компьютер*, для выполнения различных приложений (программ);
- *сервер* (Server), предоставляющий свои ресурсы (данные, программное обеспечение, периферийное оборудование) другим компьютерам сети;
- *хост* (Host — основной, главный компьютер), представляющий собой компьютер, имеющий свой сетевой IP-адрес.

В качестве оконечных устройств используются также принтеры, плоттеры и другие устройства.

Сетевые адаптеры. Под *сетевым адаптером* (Network Interface Card — NIC), или *сетевой картой*, понимают интерфейсное устройство, связывающее компьютер с линией передачи непосредственно либо через коммуникационное устройство. Назначение сетевого адаптера состоит в передаче и приеме сообщений (данных). Благодаря сетевому адаптеру осуществляется взаимодействие компьютера с другими устройствами сети.

Основные функции адаптера при передаче сообщений:

- прием от центрального процессора блока данных и адреса назначения сообщения;
- получение доступа к линии (среде) передачи;
- формирование кадра (добавление преамбулы, своего адреса в поле адреса источника, кода контроля ошибок) и передача его в линию;
- инициирование повторных попыток в случае обнаружения одновременного обращения (коллизии) к разделяемой линии передачи;
- уведомление центрального процессора о невозможности начать передачу или об успешном ее завершении.

Основные функции адаптера при приеме сообщений:

Рис. 1.4. Формат пакета и кадра

- просмотр заголовков всех кадров, проходящих в линии сообщений, фильтрация из этого потока своих кадров, т. е. адресованных данному узлу;
- прием своих кадров в буфер и проверка на отсутствие ошибок;
- уведомление центрального процессора о приеме корректных кадров;
- передача кадра из локального буфера адаптера в системную память компьютера;
- отбрасывание (игнорирование) ошибочных кадров, сбор статистики их появления.

Для управления сетевым адаптером используется программное средство, называемое *драйвером*.

Модемы. Модем предназначен для передачи информации на большие расстояния с использованием телефонных линий и включает в себя: модулятор и демодулятор.

Модулятор преобразует поступающую от компьютера двоичную информацию в аналоговые сигналы.

Демодулятор извлекает из принятого модулированного сигнала закодированную двоичную информацию и передает ее в компьютер.

Модем устанавливается между компьютером и телефонной линией, которая соединяет пользователя с провайдером услуг Internet или сервером удаленного доступа частной сети. Для доступа в Internet или корпоративную сеть через телефонную сеть модем пользователя посылает вызов модему, находящемуся на сервере удаленного доступа (Remote Access Server — RAS). Модем любого типа является устройством *последовательного действия*, в котором биты данных передаются по одному один за другим.

Коммуникационные устройства. Известно много различных *коммуникационных*, или *коммутирующих*, *устройств*, таких как повторители, мосты, концентраторы, маршрутизаторы и шлюзы. Соответствие коммутирующих устройств уровням стандартной сетевой модели OSI (см. гл. 2) приведено в табл. 1.3.

Таблица 1.3

№	Уровень	Устройство
7	Прикладной	Шлюз приложения
6	Представления	
5	Сеансовый	
4	Транспортный	Транспортный шлюз
3	Сетевой	Маршрутизатор
2	Канальный	Мост, коммутатор
1	Физический	Повторитель, концентратор

Рассмотрение коммутирующих устройств с точки зрения семиуровневой модели OSI позволяет выявить, какая часть информации исходного сообщения используется промежуточными сетевыми устройствами для выбора маршрута в процессе его передачи от отправителя (прикладной уровень) к получателю (физический уровень). Подготовленные отправителем данные (рис. 1.4) последовательно передаются:

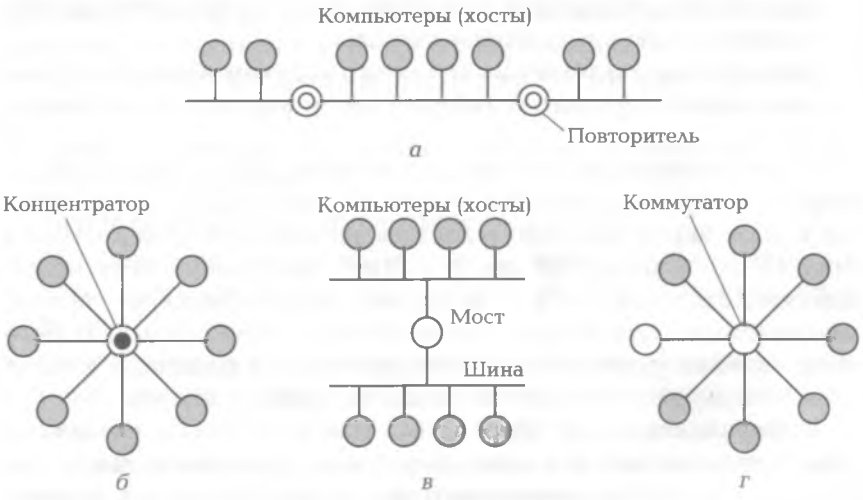


Рис. 1.5. Коммутирующие устройства:
а — повторитель; *б* — концентратор; *в* — мост; *г* — коммутатор

1) на *транспортный уровень*, который добавляет к ним свой заголовок (например, заголовок TCP — протокола управления передачей);

2) *сетевой уровень*, который, в свою очередь, также добавляет свой заголовок (пакета), в результате чего формируется пакет сетевого уровня (например, IP-пакет);

3) *канальный уровень*, где формируется кадр путем добавления еще одного заголовка (кадра) и концевика в виде контрольной суммы (CRC-кода);

4) *физический уровень* для транспортировки по сети.

Рассмотрим особенности коммутирующих устройств и выявим, как они соотносятся с пакетами и кадрами.

Повторители (Repeaters) являются коммуникационными устройствами самого нижнего, *физического уровня*. Простейший повторитель представляет собой двухпортовое аналоговое устройство для физического соединения различных сегментов кабеля ЛС в целях увеличения общей длины сети (рис. 1.5, *а*). Каждый порт имеет собственный *трансивер*, состоящий из передатчика и приемника. Повторитель улучшает качество передаваемого сигнала: восстанавливает амплитуду и мощность выходного сигнала, уменьшает длительность фронтов и т.п. В сети Ethernet допускается установка четырех повторителей, что позволяет увеличить длину кабеля до 2 500 м.

Концентраторы (Concentrator), или хабы (Hub), как и повторители, работают на физическом уровне, однако отличаются от них тем, что имеют несколько электрически связанных входов-выходов (портов), к которым подключены линии передачи. Все линии должны работать с одинаковыми скоростями. На рис. 1.5, *б* электрическая связь внутри коммутатора обозначена крупной точкой. Кадры, прибывающие на какую-либо линию (вход), передаются на все остальные линии (выходы). Если одновременно по разным линиям (входам) придут два кадра, то из-за наличия электрической связи в концентраторе произойдет *столкновение* (коллизия).

Концентраторы Ethernet имеют от 8 до 72 портов. Трансивер каждого порта помимо передатчика и приемника содержит детектор коллизий, с помощью которого можно обеспечить доступ к сети, а также изолировать порт, на котором обнаруживаются непрерывные ошибки (коллизии).

Логическая структуризация сети осуществляется с помощью мостов, коммутаторов, маршрутизаторов и шлюзов. Рассмотрим мосты и коммутаторы, работающие на *канальном уровне*.

Мосты (Bridges) соединяют две (рис. 1.5, *в*) или более ЛС, называемых также *подсетями*, *сегментами сети* или *доменами коллизий*. Главная функция моста состоит в ретрансляции данных (кадра) из одного сегмента сети в другой. Мост не вносит изменений в пакеты данных, однако способен уменьшить избыточный трафик. В отличие от повторителя или концентратора он анализирует адрес назначения кадра. При этом:

а) если адрес назначения поступающего кадра относится к *тому же* сегменту, то кадр мостом игнорируется;

б) если адрес назначения *известен* мосту и относится к *другому* сегменту, мост транслирует этот кадр в соответствующий порт;

в) если адрес назначения еще *не известен* мосту, кадр транслируется во все порты, кроме того, откуда он пришел, а незнакомый адрес сохраняется для дальнейшего использования, т. е. в ходе работы мост самообучается. После самообучения мост передает кадры только в сегмент назначения, уменьшая тем самым общий объем передаваемых по сети данных.

Широковещательные и многоадресные кадры также транслируются во все порты. Мост позволяет изменять логическую структуру сети при сохранении физического расположения узлов и связей между ними. Логическое деление на подсети повышает безопасность данных, ограничивая доступ к ним отдельных пользователей.

Современные мосты (как и концентраторы) укомплектованы сетевыми платами, рассчитанными обычно на четыре или восемь входов определенного типа. При наличии нескольких плат мост способен работать с сетями разных типов.

Коммутаторы (Switch) являются усовершенствованными мостами и для маршрутизации также используют адреса кадров. Каждый коммутатор оснащен специализированным процессором, благодаря чему общая производительность коммутатора превышает производительность традиционного моста, имеющего один процессорный блок. Однако в отличие от мостов, соединяющих целые сети, коммутаторы чаще всего используют для соединения отдельных компьютеров (рис. 1.5, *г*), поэтому коммутаторы имеют гораздо больше разъемов для сетевых плат, чем мосты. Каждый порт является областью столкновений (коллизий). Чтобы предотвратить коллизии, каждый порт коммутатора снабжен буфером для хранения пришедших кадров, поэтому коллизии могут возникнуть только при переполнении буфера. Для предотвращения коллизий современные коммутаторы начинают пересылать кадры сразу после получения их заголовков, т. е. они не используют про-

токолы с ожиданием. Такие коммутаторы называют *сквозными*. При этом чаще всего используется *аппаратная* реализация алгоритма без ожидания, тогда как в мостах традиционно присутствует процессор, *программно* реализующий маршрутизацию с ожиданием.

Маршрутизаторы (Router) относятся к *сетевому* уровню модели OSI и имеют существенные отличия от мостов и стандартных концентраторов. Основная функция маршрутизатора состоит в чтении заголовков пакетов сетевых протоколов и в принятии решения о дальнейшем маршруте следования пакета. На маршрутизатор прибывает пакет, сформированный сетевым уровнем (на рис. 1.4 выделен цветом), в котором отсутствует заголовок кадров и концевик (CRC). Пакет передается программному обеспечению маршрутизатора, которое анализирует *заголовок пакета*, и в соответствии с ним выбирает дальнейший путь пакета.

Появление маршрутизаторов обусловлено ограничениями мостов и коммутаторов по топологии связей и другим показателям. Благодаря использованию составных числовых адресов (с указанием номеров подсетей, компьютеров и собственных портов) маршрутизаторы более надежно и эффективно изолируют трафик отдельных частей сети друг от друга. Кроме локализации трафика маршрутизаторы способны выполнить многие другие полезные функции, в частности, они могут: работать в сети с *замкнутыми* контурами, осуществляя при этом выбор рационального маршрута из нескольких возможных; связывать в *единую сеть* подсети, построенные с использованием разных сетевых технологий, например Ethernet и X.25.

Транспортные шлюзы служат для соединения компьютеров, использующих различные транспортные протоколы, ориентированные на работу с установлением соединения, например TCP/IP и ATM. В этом случае транспортный шлюз может копировать пакеты, одновременно приводя их к нужному формату.

Шлюзы приложений работают с форматами и содержимым пакетов на более высоком уровне. Например, шлюз E-Mail может переводить электронные письма в формат SMS-сообщений для мобильных телефонов.

Среды передачи данных. Основной составной частью телекоммуникационных сетей является *физическая среда* (Medium), или *среда передачи данных*, по которой передаются сигналы. В качестве среды передачи данных используются коаксиальный кабель, кабель на основе витых пар, оптоволоконный кабель и беспроводная среда (свободное пространство). Подробное описание сред передачи данных приведено в гл. 5.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. В чем состоит смысл следующих терминов: «телекоммуникационная сеть», «компьютерная сеть», «конвергенция», «сетевая архитектура», «сетевая технология», «спецификация», «топология», «расширяемость сети», «масштабируемость сети», «управляемость сети», «совместимость сети», «рабочая станция», «сервер», «хост», «сетевой адаптер», «сетевая карта», «модем», «повторитель», «концентратор», «мост», «коммутатор», «маршрутизатор», «транспортный шлюз», «шлюз приложений», «среда передачи данных»?
2. Какие компоненты входят в состав телекоммуникационной сети?
3. Каковы основные классификационные признаки телекоммуникационных сетей?
4. Какие основные топологии сетей вам известны? Дайте их сравнительную оценку.
5. Что представляют собой сети операторов связи, корпоративные сети, виртуальные частные сети, гибридные сети и сети с тонкими клиентами? Дайте их краткую характеристику
6. Какие виды услуг предоставляют телекоммуникационные сети и в чем они состоят?
7. Какими показателями оцениваются производительность и надежность сети?
8. Какие средства используют для повышения качества обслуживания?
9. Что такое типовые сетевые устройства? Дайте их краткую характеристику. На каких уровнях применяются типовые коммуникационные устройства?

Глава 2

КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ СЕТЕЙ

2.1. СТАНДАРТИЗАЦИЯ И СЕТЕВЫЕ МОДЕЛИ

Проблема совместимости и стандартизация. Современная телекоммуникационная сеть представляет собой сложный комплекс разнообразных программных и аппаратных средств, а также коммуникационного оборудования. Для построения сети и ее нормального функционирования необходимо обеспечить конструктивную, коммуникационную, электрическую, программную, алгоритмическую и другую совместимость всего комплекса используемых в сети устройств и программ.

С точки зрения совместимости сеть должна обладать определенными свойствами или удовлетворять соответствующим требованиям, наиболее важными из которых являются *расширяемость*, *масштабируемость* и *управляемость* (см. подразд. 1.3).

Требования совместимости невозможно выполнить без принятия всеми производителями общих договоренностей или правил изготовления оборудования. Такие правила должны быть закреплены в стандартах, рекомендациях и других документах, поэтому развитие всей компьютерной отрасли (а не только сетей) отражено в стандартах. Любая новая технология только тогда находит применение, когда ее содержание закреплено в соответствующем стандарте.

Стандартизация и открытые системы. Под *стандартизацией* понимают сведение множества различных изделий к небольшому числу типовых образцов. *Стандарт* утверждается компетентным органом и представляет собой нормативно-технический документ в виде спецификации. Под *спецификацией* понимают формализованное описание аппаратных и (или) программных компонентов, их характеристик, условий эксплуатации и способов взаимодействия с другими компонентами. Необходимость стандартизации привела к концепции *открытых систем*. К открытым системам относятся аппаратные и программные компоненты, построенные

в соответствии с общедоступными, опубликованными (открытыми) спецификациями. Примером открытой системы может служить Internet, который объединил в себе самое разнообразное оборудование и программное обеспечение огромного числа сетей, разбросанных по всему миру. В разработке стандартов этой сети принимали участие различные научные организации, а также производители аппаратных средств и программного обеспечения.

Классификация стандартов. В работе по стандартизации телекоммуникационных сетей принимает участие большое число различных организаций, фирм — изготовителей оборудования и программного обеспечения, а также научных учреждений, ассоциаций, министерств и ведомств. Выделяют четыре группы стандартов:

1) *международные*, к которым относятся стандарты Международной организации по стандартизации (International Standards Organization — ISO), Международного союза электросвязи (International Telecommunications Union — ITU) и др.;

2) *национальные* — отечественные стандарты, стандарты американского национального института стандартов (American National Standards Institute — ANSI); стандарты, разработанные Национальным центром компьютерной защиты (National Computer Security Center — NCSC) Министерства обороны США и др.;

3) *специальных комитетов и объединений*, создаваемых несколькими компаниями, например, стандарты, разрабатываемые специально созданным объединением *ATM Forum*, насчитывающем около 100 коллективных участников, или стандарты союза *Fast Ethernet Alliance*;

4) *отдельных фирм*, например, стек протоколов архитектуры сетевых систем (Systems Network Architecture — SNA) компании *IBM* или графический интерфейс OPEN LOOK для Unix-систем компании *Sun*.

Концепция семиуровневой модели. В компьютерных сетях идеологической базой стандартизации является многоуровневый подход к разработке средств сетевого взаимодействия. На основе этого подхода была разработана стандартная *семиуровневая модель взаимодействия открытых систем*.

Организация взаимодействия между устройствами компьютерной сети является сложной задачей, для решения которой при построении модели ISO использовался *принцип декомпозиции*, согласно которому:

- одна сложная задача была разбита на семь более простых задач, образующих семь отдельных уровней;

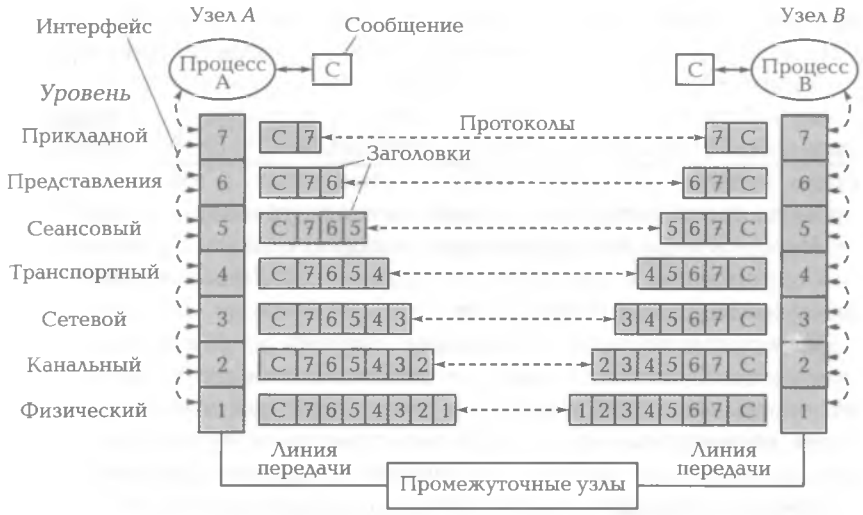


Рис. 2.1. Модель взаимодействия открытых систем ISO/OSI

- для решения задачи некоторого уровня могут быть использованы средства непосредственно примыкающего нижележащего уровня;
- полученные результаты выполненной работы могут быть переданы только соседнему вышележащему уровню.

Так как в процессе обмена сообщениями участвуют два узла сети (компьютера), необходимо организовать согласованную работу двух иерархий в двух направлениях (рис. 2.1): горизонтальном и вертикальном.

В *горизонтальном направлении* происходит протокольный обмен между двумя узлами ($A \leftrightarrow B$) одного уровня. Для обмена оба участника должны принять ряд соглашений. Например, для физического уровня необходимо согласовать способ кодирования электрических сигналов, метод контроля достоверности и т. п. Такие соглашения в виде формализованных правил, определяющих формат и последовательность передачи сообщений, которыми обмениваются сетевые компоненты, лежащие на одном уровне, но в разных узлах, называются *протоколом*.

В *вертикальном направлении* обмен осуществляется в отдельном узле (*A* или *B*) от одного уровня к другому. Модули, находящиеся в одном узле на двух соседних уровнях, также взаимодействуют друг с другом в соответствии с четко определенными пра-

вилами, которые называют *интерфейсом*. Интерфейс определяет услуги, предоставляемые данным уровнем соседнему уровню.

Таким образом, средства каждого уровня должны отрабатывать свой собственный *протокол*, а также *интерфейсы* с соседними уровнями. При этом протоколы определяют правила взаимодействия модулей одного уровня в разных узлах, а интерфейсы — 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 не только компьютерами, но и такими сетевыми устройствами, как концентраторы, мосты, коммутаторы, маршрутизаторы и т.д. В зависимости от типа устройства в нем должны быть *встроенные средства* (аппаратные и (или) программные), реализующие тот или иной набор протоколов.

Протоколы нижних уровней часто реализуются комбинацией программных и аппаратных средств, а протоколы верхних уровней, как правило, чисто программными средствами.

Другие сетевые модели. Получившая широкое распространение семиуровневая модель OSI не является единственной. Самая первая сетевая модель DoD (Department of Defense — Министерство обороны США) была разработана в 1970-х гг. [12, 13]. Позднее она получила название TCP/IP (Transmission Control Protocol/Internet Protocol), поскольку разрабатывалась вместе с протоколом TCP/IP как часть проекта сети ARPAnet. Это более простая модель, чем OSI. Она содержит только *четыре* уровня, которые можно приближенно отразить на *семь* уровней модели OSI (рис. 2.2).

Некоторые поставщики сетевых ОС используют для описания работы компонентов этих систем собственные сетевые модели.

Уровни модели DoD (TCP/IP)	Уровни модели OSI
Приложений	Прикладной Представления Сеансовый
Обмена между компьютерами	Транспортный
Межсетевой	Сетевой
Сетевого интерфейса	Канальный Физический

Рис. 2.2. Соответствие моделей DoD и OSI

Примером такой модели может служить сетевая модель Microsoft Windows для Windows NT/2000 [13].

2.2. СЕМИУРОВНЕВАЯ СЕТЕВАЯ МОДЕЛЬ

Рассмотрим назначение отдельных уровней сетевой модели, или модели ISO/OSI, и средства поддержки, начиная с наивысшего уровня (см. рис. 2.1).

Прикладной уровень (Application Layer). Это высший уровень модели, который организует взаимодействие прикладных программ пользователя с процессами модели OSI, обеспечивая им набор определенных сетевых услуг (передача файлов, обмен почтовыми сообщениями, доступ к принтеру, управление сетью и т.д.). Взаимодействие сообщения с высшим уровнем модели осуществляется через прикладной программный интерфейс (Application Program Interface — API).

Назначение, задачи и функции прикладного уровня определяются набором протоколов, с помощью которых пользователи сети получают доступ к сетевым ресурсам. Например, FTP (File Transfer Protocol) используется для передачи файлов между компьютерами, на которых могут быть установлены разные ОС или платформы. При этом клиентская программа FTP предназначена для организации соединения и загрузки файлов с сервера, а программное обеспечение FTP-сервера используется на компьютере, передающем файлы.

Уровень представления (Presentation Layer). Этот уровень обеспечивает требуемую форму представления передаваемой по сети информации без изменения ее содержания. На этом уровне анализируются представление символов, формат страниц и графическое кодирование вместе с различными правилами шифрования. При управлении экраном терминала реализуются и другие функции, например, очистка экрана, защита от стирания некоторых частей экрана и обозначение на экране особо важных полей (в частности, с помощью мерцания). Средствами данного уровня протоколы прикладных уровней могут преодолеть синтаксические различия в представлении данных. Благодаря этому информация, передаваемая прикладным уровнем одной системы, будет понятна прикладному уровню в другой системе.

При передаче на этом уровне могут выполняться:

- *шифрование данных*, благодаря которому обеспечивается секретность обмена данными сразу для всех прикладных служб.

Примером такого протокола является SSL (Secure Socket Layer — уровень защищенных гнезд-сокетов), обеспечивающий секретный обмен сообщениями для протоколов прикладного уровня стека TCP/IP;

- *сжатие данных*, т.е. уменьшение объема данных в целях их быстрой передачи по сети;
- *преобразование данных* из одного протокола в другой для передачи их между разными платформами и операционными системами.

На принимающем компьютере уровень представления обеспечивает распаковку, расшифровку и другие преобразования данных в формат, пригодный для пользовательских приложений и передачи данных на прикладной уровень.

Уровень представления могут поддерживать *редиректор*, представляющий собой программу, которая определяет средство (локальный компьютер или сетевое устройство) обработки запросов, и *шлюз* в виде устройства или программы, служащий точкой соединения между двумя разными сетями.

Сеансовый уровень (Session Layer). Данный уровень обеспечивает координацию связи между двумя узлами (компьютерами) сети, т.е. поддержание диалога между процессами определенного типа. Для этого предусмотрено большое число функций по организации передачи данных и по синхронизации процедур взаимодействия.

Сеансовый уровень выполняет следующие функции:

- отвечает за установление сеанса связи между передающим и принимающим узлами (компьютерами), организует сеанс обмена данными, управляет приемом и передачей пакетов, обеспечивает завершение сеанса;
- осуществляет контроль за степенью завершения длинных передач, что позволяет избежать повторной пересылки данных при разрывах связи и возобновить передачу с прерванного места. Для этого устанавливаются точки проверки для синхронизации потока данных к приложению, т.е. в потоке данных размещаются маркеры. Если в канале связи произошел сбой, то повторно передаются только данные, начиная с последнего маркера;
- обеспечивает управление диалогом для того, чтобы фиксировать, какая из сторон в настоящий момент является активной;
- устанавливает и разрывает диалоги приложения с приложением;

- проверяет режим связи (одно- или двунаправленный);
- определяет категории (приоритеты) услуг и генерирует сообщения о неполадках у себя и на вышестоящих уровнях;
- выполняет задачи обеспечения безопасности и распознавания имен.

На практике функции этого уровня часто объединяют с функциями прикладного уровня и реализуют в одном протоколе.

Транспортный уровень (Transport Layer). Этот уровень занимает центральное место в иерархии уровней сети. Он является *пограничным* уровнем между вышележащими уровнями, в сильной мере зависящими от приложений, и нижележащими уровнями, привязанными к конкретной сети. Сообщением является *пакет данных* протокола транспортного уровня.

По сути транспортный уровень связывает промежуточные системы (Intermediate System — IS), обеспечивающие передачу пакетов между отправителем и получателем с использованием нижних уровней, и оконечные системы (End System — ES), работающие на верхних уровнях.

Назначение транспортного уровня — обеспечение качественной передачи сообщений от отправителя к получателю и контроль ошибок. Модель OSI определяет *пять классов* транспортного сервиса (услуг), который обеспечивает требуемые пропускную способность, задержку прохождения, уровень достоверности; предоставляет возможность восстановления прерванной связи; обладает способностью к обнаружению ошибок передачи (таких как искажение, потеря и дублирование пакетов) и их управлению.

Выбор класса сервиса транспортного уровня зависит от степени надежности, обеспечиваемой вышележащими и нижележащими уровнями. Например, если качество каналов передачи связи очень высокое и вероятность возникновения ошибок, не обнаруженных протоколами более низких уровней, невелика, то целесообразно воспользоваться одним из *облегченных* сервисов транспортного уровня без многочисленных проверок, квитирования и других приемов повышения надежности. В противном случае следует обратиться к наиболее *развитому* сервису транспортного уровня, который работает с использованием средств обнаружения и устранения ошибок, включая предварительное установление логического соединения, контроль доставки сообщений по контрольным суммам и циклической нумерации пакетов, установление тайм-аутов доставки и т. п.

Основные функции транспортного уровня. В их число входят:

- разбиение передаваемых данных на пакеты;
- сборка принимаемых пакетов и передача их в нужной последовательности на сеансовый уровень, поскольку в большой маршрутизируемой сети пакеты могут достигать приемника не в том порядке, в каком передавались;
- определение путей передачи пакетов;
- контроль передачи данных, обнаружение и исправление ошибок передачи данных, вызванных искажениями, потерями или дублированием пакетов;
- согласование сетевых уровней различных несовместимых сетей;
- отображение логических (символьных) имен на логические сетевые адреса с использованием системы разрешения имен (Domain Name System — DNS).

Используется два режима передачи пакетов: с установлением и без установления соединения.

При режиме *с установлением соединения* в начале передачи устанавливается соединение между источником и приемником. В этом режиме передача может идти без нумерации пакетов, поскольку каждый из них идет за предшественником по тому же пути. По окончании передачи соединение разрывается.

В режиме без *установления соединения* требуется нумеровать пакеты, поскольку они могут теряться, повторяться, приходить не по порядку.

Транспортные протоколы. Протоколы *четырех нижних* уровней, которые называют сетевым транспортом или транспортной подсистемой, решают задачу транспортировки сообщений с заданным уровнем качества в составных сетях с произвольной топологией и различными технологиями. Протоколы *трех верхних* уровней, используя нижележащую транспортную подсистему, решают задачи предоставления прикладных сервисов.

Как правило, все протоколы, начиная с транспортного уровня и выше, реализуются программными средствами оконечных узлов сети — компонентами их сетевых ОС.

Сетевой уровень (Network Layer). Этот уровень служит для организации совместной работы нескольких сетей с разной архитектурой при их объединении в единую сеть, называемую *составной*. Технология, позволяющая осуществить такое объединение, назы-

вается *технологией межсетевого взаимодействия* (Internetworking). Локальная сеть с одной архитектурой (Ethernet, FDDI, Token Ring, ATM или Frame Relay) не способна обеспечить передачу данных в сеть с другой архитектурой, что обусловлено разным форматом используемых кадров, логикой работы протоколов и другими причинами. Еще больше отличий можно обнаружить между архитектурами локальных и глобальных сетей. Таким образом, для организации и координации работы в сетях, построенных на основе различных архитектур, необходимы *дополнительные средства*. Такие средства предоставляет сетевой уровень в виде протоколов и специальных устройств.

Сетевой уровень отвечает за доставку пакетов данных отправителя одной сети получателю другой сети. Сети соединяются между собой специальными устройствами, называемыми *маршрутизаторами*. Маршрутизатор собирает информацию о топологии межсетевых соединений и на ее основании пересылает пакеты в сеть назначения. При пересылке пакетов происходит несколько транзитных передач между сетями. Последовательность маршрутизаторов, или путь, через который проходит пакет, называется *маршрутом*. Составление (выбор, определение) наилучшего пути, или *маршрутизация*, является одной из главных задач сетевого уровня. Маршрутизация резко повышает эффективность использования физических каналов, поскольку пакеты одного сообщения могут доставляться разными путями, хотя пользователи сети этого и не замечают. На сетевом уровне работает большинство протоколов маршрутизации.

Особенности работы. Весь путь передаваемого сообщения через составную сеть разбивается на участки от одного маршрутизатора до другого, причем каждый участок соответствует пути через отдельную сеть. Данные, поступающие на сетевой уровень (от вышележащего транспортного), снабжаются заголовком сетевого уровня. Совокупность данных и заголовка образует *пакет*. Заголовок пакета имеет унифицированный формат и содержит его адрес назначения. В пределах данной составной сети каждый узел имеет собственный уникальный адрес, который называют *сетевым адресом узла*. Наряду с сетевым адресом на нижележащем канальном уровне каждому узлу назначается *аппаратный MAC-адрес*, т. е. узлы составной сети имеют два адреса. Маршрут пакета определяется на основании адреса назначения, указанного в пакете на сетевом уровне, и описывается последовательностью маршрутизаторов (или сетей), через которые должен пройти пакет. Маршрутизатор извлекает пакет из прибывшего кадра, и после

обработки передает пакет в следующую сеть, предварительно упаковав его в кадр канального уровня, соответствующий формату этой сети.

Устройства сетевого уровня. К ним относятся *маршрутизаторы* и *коммутаторы* сетевого уровня. Одной из функций маршрутизатора является физическое соединение сетей, поэтому маршрутизатор имеет несколько сетевых интерфейсов, которые можно считать узлами разных сетей. К каждому интерфейсу подключается одна сеть. Маршрутизаторы строятся на базе специализированных аппаратных платформ. В состав их программного обеспечения входят протокольные модули сетевого уровня. Маршрутизатор может быть реализован программно на базе универсального компьютера.

Канальный уровень (Data Link Layer — уровень звена данных). Назначение канального уровня — поддержание интерфейсов с двумя соседними уровнями, для чего он разделен на два подуровня: управления логической связью и управления доступом к среде.

Подуровень управления логической связью (Logical Link Control — LLC) определяет логическую топологию сети, которая может не совпадать с физической топологией. На этом подуровне осуществляются установка и поддержка виртуального канала связи. Подуровень LLC скрывает от вышестоящих уровней подробности технической реализации сети, благодаря чему сетевой уровень не видит различий между локальными сетями Ethernet, Token Ring, ARCnet, FDDI.

Подуровень управления доступом к среде (Media Access Control — MAC) устанавливает правила использования физического (нижележащего) уровня узлами сети. На этом подуровне распознаются электрические сигналы (биты данных, способы кодирования, маркеры), обнаруживаются коллизии (столкновения сигналов в линии связи), выявляются и исправляются ошибки. Подуровень MAC работает с так называемыми *MAC-адресами*, каждый из которых представляет собой уникальный (его нельзя изменить) физический адрес устройства.

Особенности работы канального уровня состоят в том, что сетевой уровень узла отправителя передает канальному уровню *пакет*, в котором указан адрес узла назначения (получателя). Канальный уровень создает *кадр* и *инкапсулирует* (помещает) в него пакет. Коммутаторы сети продвигают (Forwarding) исходный пакет в узел получателя согласно адресу назначения. Для обнаружения и коррекции ошибок канальный уровень добавляет к

кадру контрольную сумму (Frame Check Sequence — FCS), которая вычисляется по некоторому алгоритму. По значению FCS узел назначения определяет, искажены или нет данные кадра в процессе передачи по сети. Однако прежде чем послать кадр физическому уровню для непосредственной передачи данных в сеть, подуровень MAC проверяет доступность разделяемой среды. Если разделяемая среда не занята, кадр передается средствами физического уровня в узел назначения. Физический уровень узла назначения передает полученные биты своему канальному уровню, который группирует биты в кадры, снова вычисляет контрольную сумму полученных данных и сравнивает результат с переданной контрольной суммой.

Если значения контрольных сумм совпадают, то кадр считается правильным. В противном случае фиксируется ошибка. При наличии ошибки может быть назначена повторная передача поврежденных кадров.

Отметим, что в *локальных сетях* канальный уровень обеспечивает доставку кадра между любыми узлами сети, а в *глобальных сетях* — только между узлами, соединенными индивидуальной линией связи.

Протоколы канального уровня реализуются компьютерами, мостами, коммутаторами (или коммутирующими концентраторами) и маршрутизаторами. В компьютерах выполнение функций канального уровня возлагается на сетевые адаптеры и их драйверы.

Физический уровень (Physical Layer). Это самый нижний уровень сетевой модели OSI. Единицей передачи данных является *бит*.

Назначение и основные особенности. На физический уровень возлагается обеспечение взаимодействия (интерфейса, согласования) физических объектов (сигналов, узлов и линий связи сети) при передаче сообщений. Его главной задачей является формирование и доставка сигналов в виде последовательности биттов узлу назначения с использованием различных аппаратных средств. На физическом уровне определены (заданы):

- сигналы, их виды (электрические, световые, аналоговые, цифровые и др.), характеристики (крутизна фронтов импульсов, уровни напряжения, способы бинарного кодирования и др.) и способы передачи (синхронный, асинхронный и др.);
- физические, механические и электрические характеристики линий связи, к которым относятся: тип кабелей и разъемов; разводка контактов в разъемах, физическая топология и др.;

- аппаратные средства, их типы (сетевые адаптеры, модемы, повторители, концентраторы и др.) и характеристики (скорость, пропускная способность и др.).

Основные функции и их реализация. Физический уровень можно отождествлять со средствами непосредственной доставки информации потребителю. В связи с этим к функциям этого уровня относятся все операции, связанные с формированием, преобразованием и передачей сигналов по линиям связи, для реализации которых используется широкий набор различных аппаратных средств. На оконечных узлах функции физического уровня выполняются сетевыми адаптерами и (или) модемами, на промежуточных узлах — повторителями, мостами, концентраторами и другими устройствами.

Физический уровень поддерживается протоколами (спецификациями, описаниями), определяющими требования к сигналам, средам передачи и аппаратным средствам, а также механические, электрические, функциональные и процедурные характеристики, необходимые для установления, поддержания и расторжения физических соединений.

2.3. СТЕКИ ПРОТОКОЛОВ

Иерархически организованный набор протоколов, достаточный для организации взаимодействия узлов в сети, называется *стеком коммуникационных протоколов* (Stack — набор, комплект). Коммуникационные протоколы могут быть реализованы как программно, так и аппаратно. Протоколы нижних уровней часто реализуются комбинацией программных и аппаратных средств, а протоколы верхних уровней, как правило, только программными средствами. Качество всей совокупности протоколов, составляющих стек, влияет на эффективность взаимодействия устройств в сети.

Известно большое число стеков коммуникационных протоколов. Рассмотрим два наиболее важных из них.

Стек TCP/IP. Протокол управления передачей или межсетевой протокол (Transmission Control Protocol/Internet Protocol — TCP/IP) разработан для разнородных вычислительных сетей. Стек протоколов TCP/IP постоянно развивается и является наиболее распространенным протоколом сетевого и транспортного уровней для сетей различных размеров и конфигураций.

Состав стека. Стек состоит из трех базовых наборов протоколов: сетевого уровня IP, управления передачей и дейтаграмм пользователя.

Протокол сетевого уровня IP (Internet Protocol) отвечает за передачу и маршрутизацию сообщений между узлами Internet. Протокол IP определяет правила, по которым данные разбиваются на пакеты, передающиеся между оконечными системами и маршрутизаторами. Текущая версия — 4.0 (IPv4), внедряемая — 6.0 (IPv6).

Основные особенности новой версии протокола IPv6 по сравнению с IPv4 состоят в следующем [12]:

- поле адреса имеет длину 16 байт, что обеспечивает практически неограниченный запас интернет-адресов (2^{16}), т.е. решает основную проблему, поставленную при разработке протокола;
- если у протокола IPv4 заголовок пакета содержал 13 полей, то в новой версии IP он состоит всего из 7. Поэтому маршрутизаторы могут значительно быстрее обрабатывать пакеты. В новом заголовке некоторые поля стали необязательными. Используемый способ представления необязательных параметров упростил для маршрутизаторов пропуск не относящихся к ним параметров, что также ускорило обработку пакетов;
- более надежным, чем в нынешнем варианте IPv4, стало обеспечение безопасности с помощью используемых методов аутентификации и конфиденциальности;
- если в заголовке пакета IPv4 для представления услуг отведено 8-разрядное поле, которое практически не использовалось, то в новой версии при ожидаемом росте мультимедийного трафика выделяется значительно больше разрядов.

Протокол управления передачей (Transmission Control Protocol — TCP) — широко используемый в Internet сетевой протокол транспортного уровня. Предоставляет конечным пользователям службу *с установлением* логического соединения. Гарантирует доставку передаваемых пакетов данных в нужной последовательности, но трафик при этом очень неравномерен, так как пакеты испытывают всевозможные задержки.

Протокол дейтаграмм пользователя (User Datagram Protocol — UDP) является сетевым протоколом транспортного уровня. Он предоставляет конечным пользователям службу *без установления* логического соединения. Отдельные пакеты передаются с использованием IP как можно быстрее (без проверки на правильность передачи и гарантий доставки). При этом часть пакетов может терять-

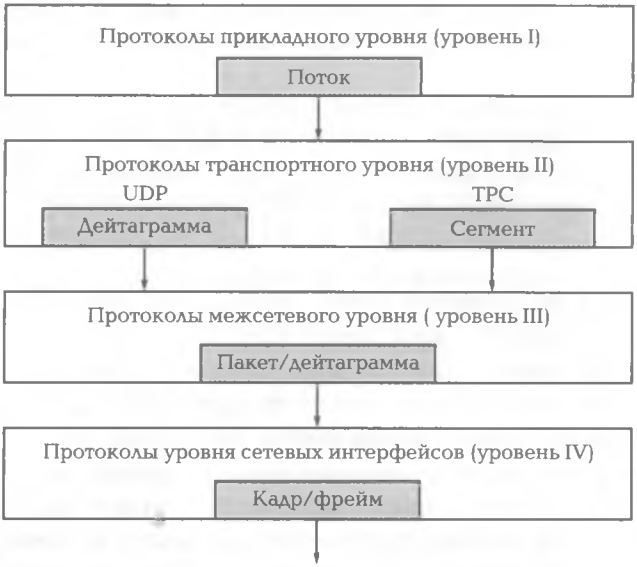


Рис. 2.3. Блоки передаваемых данных

ся. Однако передаваемое сообщение не прерывается, что важно, например, при передаче речи для обеспечения ее разборчивости.

Единицы данных. Каждый коммуникационный протокол оперирует некоторой единицей (или блоком) передаваемых данных (Protocol Data Unit — PDU). Названия этих единиц иногда закрепляются стандартом, а часто просто определяются традицией. Названия единиц PDU, получивших наиболее широкое распространение в протоколах стека TCP/IP, приведены на рис. 2.3. Поясним смысл, который вкладывается в эти названия.

Поток данных, или *поток*, — данные, поступающие от приложений на вход протоколов транспортного уровня — UDP и TCP.

Дейтаграмма, или *датаграмма*, — единица данных протокола UDP транспортного уровня. Обычно дейтаграммой называют данные, которыми оперируют протоколы без установления соединений. К таким протоколам относится и протокол IP межсетевого уровня, поэтому его единицу данных также называют дейтаграммой. Однако очень часто на уровне III используется и другой термин — *пакет*.

Сегмент — другая единица данных транспортного уровня, полученных протоколом TCP из входного потока.

Кадр, или фрейм (Frame), — единица данных, в которую упаковываются IP-пакеты для последующей пересылки их через отдельные сети составной сети. При этом не имеет значение название, используемое для этой единицы данных в каждой отдельной сети, т. е. для стека TCP/IP *фреймом* называют *кадр* сети Ethernet, *ячейку* сети ATM и *пакет* сети X.25.

Многие протоколы, входящие в пакет TCP/IP, предназначены для сбора информации или устранения неполадок. Пакет протоколов включает в себя также дополнительные компоненты, не обязательные в процессах сетевой коммуникации, например утилиты прикладного уровня, также входящие в состав пакета TCP/IP.

Особенности стека TCP/IP. Когда речь идет о построении больших (глобальных) сетей, этому стеку протоколов отдается предпочтение по сравнению с другими протоколами, так как он с момента создания ориентирован на Internet и наделен многими полезными свойствами. К таким свойствам следует отнести:

- *способность фрагментировать пакеты.* Большая составная сеть часто состоит из (под) сетей, построенных на совершенно разных принципах, и каждая из (под) сетей может иметь собственное значение единицы (длину) передаваемых данных. При переходе из одной сети в другую может возникнуть необходимость уменьшить длину данных. Указанное свойство протокола позволяет разделить (фрагментировать) передаваемый пакет (кадр) на несколько частей;
- *гибкую систему адресации* (три уровня адресов: символьные, логические и физические), позволяющую проще, чем другие протоколы аналогичного назначения, включать в составную сеть сети разных технологий;
- *экономное использование широковещательных рассылок.* Это свойство наиболее полезно при работе на медленных линиях связи, характерных для территориальных сетей;
- *интерпретацию функций самого нижнего уровня* (сетевых интерфейсов). Стек TCP/IP в отличие от других многоуровневых стеков *освобожден* от выполнения большого количества функций канального и физического уровней OSI. На нижний уровень стека, как указано выше, возлагается лишь ответственность за организацию взаимодействия с (под) сетями составной сети, которая требует выполнения более простых процедур. Эта особенность делает составную сеть TCP/IP открытой для включения дополнительной сети с любой технологией передачи данных. При этом для каждой новой технологии должны быть раз-

работаны собственные интерфейсные средства. Обычно при появлении новой технологии локальных или глобальных сетей она быстро включается в стек TCP/IP путем разработки соответствующего документа стандарта Internet, определяющего метод инкапсуляции IP-пакетов в ее кадры.

Однако широкие функциональные возможности протоколов стека TCP/IP требуют для своей реализации больших вычислительных затрат. Гибкая система адресации и отказ от широковещательных рассылок (или их ограничение) приводят к наличию в IP-сети разнообразных централизованных служб: доменных имен (Domain Name System — DNS), динамического конфигурирования (Dynamic Host Configuration Protocol — DHCP) и др. Каждая из этих служб направлена на облегчение администрирования сети, но в то же время сама требует пристального внимания со стороны администраторов. Несмотря на это, по общему признанию, стек TCP/IP является самым популярным стеком протоколов, который широко используется как в глобальных, так и в локальных сетях. В настоящее время осуществляется переход на новую версию IPv6, которая снимет многие накопившиеся проблемы.

Протоколы и приложения, входящие в стек TCP/IP, приведены в табл. 2.1.

Таблица 2.1

Аббревиатура, полное название	Назначение	Уровень модели OSI
NFS — Network File System (приложение)	Используется для передачи файлов по сети (предназначается для компьютеров UNIX)	Прикладной Представления Сеансовый
Telnet — Telecommunications Network (приложение)	Позволяет рабочей станции эмулировать терминал и подключаться к мейнфреймам, серверам Internet и маршрутизаторам	То же
OSI и прикладной HTTP — Hypertext Transfer Protocol	Используется для передачи данных в сети World Wide Web	Представления
SMTP —Simple Mail Transfer Protocol	Используется для передачи электронной почты	То же
FTP — File Transfer Protocol	Используется для передачи и приема файлов	Представления Сеансовый

Окончание табл. 2.1

Аббревиатура, полное название	Назначение	Уровень модели OSI
RPC —Remote Procedure Call (приложение)	Позволяет удаленному компьютеру выполнять процедуры на другом компьютере (например, на сервере)	Сеансовый
TCP — Transmission Control Protocol	Ориентирован на установление соединений, что повышает надежность передачи данных	Транспортный
UDP — User Data Protocol	Протокол без установления соединений; используется как альтернатива TCP в тех случаях, когда не требуется высокая надежность	То же
DNS — Domain Name System (приложение)	Поддерживает таблицы, связывающие IP-адреса компьютеров с их именами	»
ICMP — Internet Control Message Protocol	Используется для генерирования отчетов об ошибках в сети, в частности, при передаче данных через маршрутизаторы	Сетевой
IP — Internet Protocol	Управляет логической адресацией	То же
OSPF — Open Shortest Path First (протокол)	Используется маршрутизаторами для обмена информацией (данными по маршрутизации)	»
PPP —Point-to-Point protocol	Используется как протокол удаленного доступа в сочетании с технологиями глобальных сетей	»
RIP — Routing Information Protocol	Используется при сборе данных по маршрутизации для обновления таблиц маршрутизации	»
SLIP — Serial Line Internet Protocol	Используется как протокол удаленного доступа в сочетании с технологиями глобальных сетей	»
ARP — Address Resolution Protocol	Обеспечивает разрешение IP-адресов в MAC-адреса	Сетевой Канальный

Стек IPX/SPX. Стек протоколов разработан фирмой *Novell* для сетей NetWare в начале 1980-х гг. и ориентирован на использование с различными ОС в локальных сетях. От других протоколов он отличается весьма скромными требованиями к вычислительным ресурсам и неэффективным использованием пропускной способности каналов связи, поэтому никогда не имел применения в глобальных сетях. К концу 1990-х гг. стандартный стек Internet TCP/IP фактически вытеснил IPX/SPX из локальных вычислительных сред. По состоянию на 2012 год поддержка стека IPX/SPX операционными системами продолжает сокращаться. Однако в связи широким распространением в России сетей Ethernet интерес к нему сохраняется.

Общая структура стека IPX/SPX. *Физический и канальный* уровни этого стека способны работать в локальных сетях Ethernet, Token Ring, FDDI и других на том же оборудовании, сетевых картах и кабелях, что и стек TCP/IP, используя все популярные протоколы этих уровней.

Различия начинаются с *сетевого* уровня модели OSI, представленного протоколом IPX, который аналогично протоколу IP стека TCP/IP занимается доставкой сообщений узлам сети без установления соединения. Используемый стеком дейтаграммный способ обмена сообщениями не гарантирует надежной доставки информации, однако позволяет экономно расходовать вычислительные ресурсы. Протокол IPX совместно с протоколами обмена маршрутной информацией RIP и NLSP занимается вопросами адресации и маршрутизации пакетов. При этом для адресации используются поля в заголовке пакета, а информация, поставляемая протоколами RIP либо NLSP, — для передачи пакетов компьютеру назначения или следующему маршрутизатору. Таким образом, протокол IPX обеспечивает выполнение трех функций: задание адреса, установление маршрута и рассылка дейтаграмм.

За надежную доставку информации отвечает протокол SPX, расположенный на *транспортном* уровне. Он является аналогом протокола TCP в стеке TCP/IP. Протокол SPX работает с установлением соединения и обладает способностью восстанавливать потерянные или поврежденные пакеты. Совместно с другими протоколами нижних уровней SPX осуществляет прием и передачу данных, сбор информации о состоянии сети и существующих маршрутах.

На верхних (*прикладном*, *представительском и сеансовом*) уровнях модели OSI работают два протокола:

- *протокол NCP*, который является протоколом взаимодействия сервера NetWare и оболочки рабочей станции. Он реализует ар-

хитектуру клиент-сервер. Протокол NCP позволяет рабочей станции производить подключение к серверу, отображать каталоги сервера на локальные буквы дисководов, просматривать файловую систему сервера, копировать удаленные файлы, изменять их атрибуты, а также осуществлять разделение сетевого принтера между рабочими станциями;

- *протокол SAP*, как и протокол RIP, позволяет маршрутизаторам обмениваться маршрутной информацией, а сетевым устройствам — информацией об имеющихся сетевых сервисах. С помощью протокола SAP каждый компьютер, который готов предоставить какую-либо службу для клиентов сети, объявляет об этом широковещательно по сети, указывая в SAP-пакетах тип службы (например, файловая) и свой сетевой адрес. Протокол SAP позволяет значительно уменьшить административные работы по конфигурированию клиентского программного обеспечения, так как всю необходимую информацию клиенты получают из объявлений SAP.

Протоколы, входящие в состав стека IPX/SPX приведены в табл. 2.2.

Таблица 2.2

Аббревиатура — Полное название	Назначение	Уровень модели OSI
NCP — NetWare Core Protocol — протокол ядра NetWare	Часть ОС обеспечивает обмен данными между клиентами и серверами при обращении к приложениям или открытым файлам, находящимся на сервере NetWare	Прикладной Представления Сеансовый
SAP — Service Advertising Protocol — про-токол извещения об услугах	Позволяет клиентам NetWare идентифицировать серверы и сетевые службы, имеющиеся на них. Серверы генерируют широковещательные пакеты SAP каждые 60 с, а клиенты используют их для обнаружения ближайшего сервера	То же
SPX — Sequenced Packet eXchange — последовательный обмен пакетами	Предоставляет прикладным программам механизм передачи данных, ориентированный на соединения	Транспортный

Продолжение табл. 2.2

Аббревиатура — Полное название	Назначение	Уровень модели OSI
IPX — Internetwork Packet eXchange — межсетевой обмен пакетами	Используется как основной протокол передачи данных для приложений Ethernet. Позволяет применять любые типы фреймов (кадров): Ethernet 802.2, Ethernet 802.3, Ethernet II и Ethernet SNAP	Сетевой
NLSP — NetWare Link Services Protocol — протокол коммуникационных услуг	Обеспечивает пакеты IPX информацией о маршрутизации	То же
RIP — Routing Information Protocol — протокол маршрутной информации	Собирает информацию о маршрутизации для серверов, которые обеспечивают работу служб маршрутизации	»
LSL — Link Support Layer — уровень поддержки соединения	Используется вместе с ODI-драйвером для поддержки нескольких протоколов на одном сетевом адаптере. ODI (Open Data-Link Interface — открытый интерфейс связи) для транспортных протоколов, позволяющий им бесконфликтно разделять одну и ту же сеть. Содержит драйверы для различных сетей	Канальный
MLID — Multiple Link Interface Driver — протокол коммуникационных услуг	Соединяет два или несколько каналов в одну телекоммуникационную линию (например, два терминальных адаптера ISDN). В сетях Ethernet протокол MLID в сочетании с сетевым адаптером рабочей станции позволяет определить уровень конфликтов в сети, в сетях с маркерным кольцом он координирует передачи маркера	Канальный (подуровень MAC)

Окончание табл. 2.2

Аббревиатура — Полное название	Назначение	Уровень модели OSI
Все популярные протоколы этих уровней	Ethernet, Token Ring, FDDI и др.	Канальный Физический

Особенности работы. Протоколы верхнего уровня NCP и SAP, взаимодействуя с приложениями пользователя, формируют сообщения (см. табл. 2.2), для передачи которых пользуются услугами протокола последовательного обмена пакетами SPX, состоящими из заголовка и поля данных. Протокол SPX использует метод взаимодействия с установкой логического соединения и имеет средства обеспечения гарантированной доставки передаваемых данных. Для управления передачей данных используются поля заголовков пакетов IPX и SPX. Последовательный обмен пакетами опирается на средства передачи данных по сети протокола IPX. Пакет протокола SPX инкапсулируется в IPX-пакет. При этом SPX-заголовок является дополнением к заголовку IPX-пакета.

Для адресации используются сетевые адреса протокола IPX, включающие в себя три компонента:

- номер сети, имеющий фиксированную длину 4 байт, которая для локальных сетей является избыточной;
- номер узла (6 байт), представляющий собой MAC-адрес сетевого адаптера или порта маршрутизатора;
- номер сокета (Socket) длиной 2 байт, позволяющий идентифицировать приложение, которое передает свои сообщения по протоколу IPX.

Номер сети задается администратором на серверах, а номер узла автоматически считывается из сетевого адаптера компьютера. На клиентском компьютере номер сети определяется из серверных объявлений SAP или локального маршрутизатора.

Для определения адреса маршрутизатора используется специальный запрос, который передается на заранее определенный номер сокета. Такой запрос может быть отправлен клиентом широковещательно. В этом случае все маршрутизаторы должны сообщить ему свои MAC-адреса, которые используются в качестве адреса следующего маршрутизатора.

Недостатком IPX-адресации является ограничение длины адреса узла в 6 байт, по-скольку при большей длине адреса пакет узлу не доставляется.

В заключение укажем причины, ограничивающие применение протокола IPX в больших сетях:

- из-за отсутствия полей в заголовках, с помощью которых маршрутизатор может разбить слишком большой пакет на части, пакеты большой длины отбрасываются. Для последовательного уменьшения размера пакета используется протокол верхнего уровня NCP, на что тратится время;
- из-за отсутствия поля качества сервиса маршрутизатор не может автоматически выполнять требования приложения к качеству передачи трафика;
- сравнительно небольшая максимальная длина поля данных пакета в 546 байт при длине заголовка в 30 байт делает достаточно большими накладные расходы на служебную информацию;
- время жизни пакета для большой сети недостаточное (ограничено числом 15);
- широковещательные рассылки могут привести к перегрузке сети.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. В чем состоит смысл следующих терминов: «стандартизация», «стандарт», «спецификация», «открытая система», «протокол», «стек коммуникационных протоколов», «интерфейс»?
2. Какова суть проблемы совместимости и как она решается?
3. На каком принципе базируется организация взаимодействия между устройствами компьютерной сети и в чем заключается его суть?
4. Какие уровни сетевой модели ISO/OSI и средства ее поддержки вы знаете? Дайте краткую характеристику каждого уровня.
5. Из каких базовых наборов протоколов состоит стек протоколов TCP/IP?
6. Какими основными свойствами обладает стек TCP/IP?
7. Какими единицами передаваемых данных оперирует стек TCP/IP?
8. Какие особенности имеет стек протоколов IPX/SPX?

Глава 3

ФОРМИРОВАНИЕ И ОБРАБОТКА СИГНАЛОВ

3.1. СИГНАЛЫ КАК СПОСОБ ПРЕДСТАВЛЕНИЯ ИНФОРМАЦИИ

Информация, сообщения, сигналы, данные. Одна из основных функций компьютерной сети состоит в передаче информации по каналу связи.

Под *информацией* будем понимать сведения об объектах и явлениях окружающей среды, их параметрах, свойствах и состоянии, которые поступают в виде сообщений (речи, текста, изображения, графиков, цифровых данных, таблиц и т. п.). При работе с информацией всегда имеются источник и потребитель. Пути и процессы, обеспечивающие передачу сообщений от источника к потребителю, называют *информационными коммуникациями*. Информация может быть передана на расстояние с помощью сообщения.

Сообщение является составной частью информации. Его можно рассматривать как форму представления (речь, текст, изображение, цифровые данные, графики, таблицы и т. п.) и как способ существования (передача сведений по линии связи) информации. Для сообщения характерно наличие отправителя и получателя информации, а также используемая среда для ее доставки в виде линии передачи.

Сигнал (от лат. *signum* — знак) представляет собой форму сообщения, преобразованного в целях его отображения, передачи и регистрации. Сигнал переносит сообщение (информацию) на расстояние с использованием физической среды передачи. Сигнал всегда является функцией времени, даже если сообщение таковым не является, например неподвижное изображение, передаваемое по телевизионному каналу.

Данные следует рассматривать как зарегистрированные признаки не используемой информации об объекте, которые хранятся в каком-либо месте. Когда же эти данные начинают использоваться (для уменьшения неопределенности об объекте), они пре-

вращаются в информацию, т.е. используемые данные являются информацией. Например, информацией принято считать поток компьютерных данных (компьютерный трафик), передаваемых по линии связи.

Таким образом, информация является общим понятием, включающим в себя сообщения, сигналы и данные.

Сигналы и их роль. Под *сигналом* понимают физический процесс (или явление), несущий сообщение (информацию) о каком-либо другом процессе, событии, состоянии объекта наблюдения либо передающий команды управления, указания, оповещения.

Для телекоммуникационных сетей сигналы играют основополагающую роль, поскольку являются средством транспортировки (доставки) сообщений от одного абонента к другому. Процесс транспортировки включает в себя две важные фазы: преобразование исходной информации (данных) в сигналы на передающем узле сети и обратное преобразование сигналов к исходной (или другой) форме информации на приемном узле. В зависимости от конкретной ситуации прямое и обратное преобразования имеют различные содержание и названия: аналого-цифровое и цифро-аналоговое преобразование, кодирование и декодирование, модуляция и демодуляция, компрессия и декомпрессия, скремблирование и дескремблирование. Особенности каждого из них рассматриваются далее.

Типичными для электронных устройств сигналами являются напряжения на входных и выходных зажимах или токи входной и выходной цепей устройства. Такие сигналы называются *электрическими*. С помощью входных и выходных сигналов можно определить вид функционального преобразования, выполняемого устройством, а также его основные параметры и характеристики.

Классификация сигналов. Рассмотрим классификационные признаки, представляющие интерес для дальнейшего изложения.

По непрерывности сигналов как функции времени можно выделить сигналы континуальные и дискретные.

Континуальные (от лат. *continuum* — непрерывный) сигналы обычно называют *аналоговыми*, поскольку они являются аналогом реального физического процесса. Аналоговые сигналы используются в аппаратуре радиосвязи и телевидения, в звуковоспроизводящей аппаратуре и др.

К *дискретным* (от лат. *diskretus* — разделенный, прерывистый) относят *импульсные* и *цифровые* сигналы. Особенность цифровых сигналов проявляется в том, что они, имея импульсную форму, не-

сут в себе информацию, которую можно трактовать как некоторую последовательность двоичных цифр.

По использованию дополнительных периодических колебаний сигналы делят на две группы: первичные и модулированные.

Первичные (*исходные*, *немодулированные*) *сигналы* непосредственно отражают передаваемые сообщения. Наиболее ярким примером таких сигналов являются электрические колебания в цепи *микрофона*, представляющие собой копию исходного звукового сообщения. На приемном пункте исходное звуковое сообщение выделяется путем непосредственного воздействия сигнала на *телефон* (без каких-либо дополнительных преобразований). Примером цифрового сигнала может служить 7-битная последовательность, несущая в себе информацию о десятичных цифрах. При приеме такой последовательности на 7-сегментном индикаторе высвечивается десятичная цифра. Главная *особенность* первичных сигналов состоит в том, что каждому абоненту сети для передачи сообщения требуется индивидуальная линия связи.

Модулированные сигналы для транспортировки сообщения (первичного сигнала) используют дополнительно гармонические колебания или периодическую последовательность импульсов прямоугольной формы. *Модуляцией* называют процесс управления параметрами несущих колебаний с помощью первичного сигнала. При использовании гармонических колебаний в зависимости от управляемого параметра различают амплитудную, частотную и фазовую модуляцию. С помощью модулированных сигналов можно передавать несколько сообщений по одной линии связи, поэтому одной линией связи (средой передачи) могут пользоваться многие абоненты.

Первичные сигналы и гармонические колебания. В цифровой технике *первичным сигналом* является последовательность из 0 и 1, для представления которой, как правило, используются сигналы прямоугольной формы. В качестве примера на рис. 3.1, *а*, *б* показано два способа представления временно́й последовательности в виде 4-разрядного двоичного числа 1011 : наличие прямоугольного импульса соответствует 1, отсутствие — 0.

Помимо сигналов прямоугольной формы особого внимания заслуживают *гармонические колебания* по двум причинам:

1) с их помощью можно выявить спектральный состав цифровых сигналов, представив их как периодическую последовательность прямоугольных импульсов (показано далее) в виде суммы гармоник. Определив ширину спектра цифрового сигнала, можно

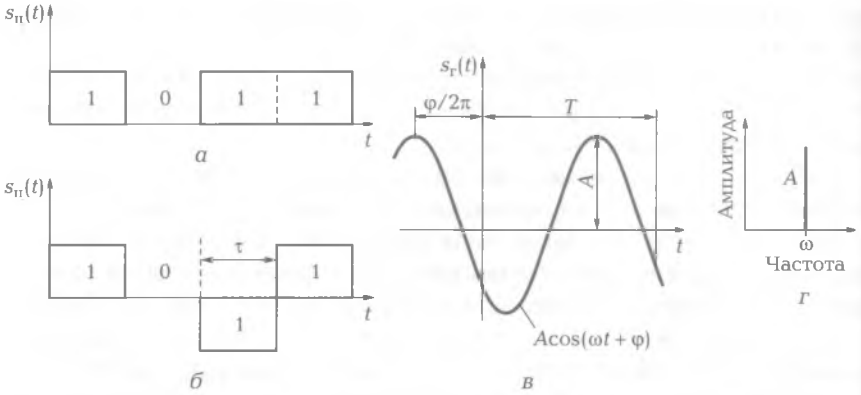


Рис. 3.1. Представление цифровых сигналов $s_ц(t)$ (*а*, *б*) и гармонического колебания $s_г(t)$ (*в*, *г*)

задать требования к полосе пропускания линии связи, одному из важнейших ее показателей;

2) гармонические колебания находят применение в качестве средства доставки сообщений по каналам радиосвязи, а также в модемах при передаче по телефонным каналам.

Гармоническое колебание можно представить:

- во *временной форме* в виде графика (рис. 3.1, *в*) или следующего аналитического выражения:

$$s_г(t) = A\cos(\omega t + \varphi),$$

где A — амплитуда (напряжения или тока); ω — круговая частота, $\omega = 2\pi/T$, где T — период; φ — начальная фаза;

- в *спектральной форме* как дискретную графическую зависимость в координатах амплитуда — частота (рис. 3.1, *г*).

Представление периодических сигналов. Периодический сигнал $s_T(t)$ любой формы можно записать в виде тригонометрического ряда Фурье, представляющего собой сумму гармонических колебаний с кратными частотами:

$$s_T(t) = A_0 + \sum_{n=1}^{\infty} A_n \cos(n\omega t + \varphi_n).$$

Суть ряда Фурье проиллюстрирована на рис. 3.2. На примере сигнала $s_T(t)$ прямоугольной формы показано, что использование двух гармоник лучше отображает форму импульса, чем одна (см.

рис. 3,2, *а* и *в*). Таким образом, увеличением числа гармоник n можно приблизить форму сигнала $s_n(t)$ к прямоугольным импульсам $s_T(t)$. Рост числа гармоник расширяет частотный спектр сигнала и требует увеличения полосы пропускания ($\omega_п$) линии связи (см. рис. 3.2, *б* и *г*). Неудовлетворение этого требования приведет к искажению формы принимаемого сигнала.

Цифровая форма представления аналоговых сигналов. Переход от аналоговой формы $s_а(t)$ представления сигналов к цифровой форме $s_ц(t)$ включает в себя два основных этапа (рис. 3.3).

1. Возможный диапазон изменения мгновенных значений аналогового сигнала $s_а(t)$ разбивается (квантуется) на 2^N равных частей, где N — разрядность двоичного числа. Для сигнала $s_а(t)$, изображенного на рис. 3.3, *а*, выбрано $N = 3$. Осуществляется преобразование (дискретизация) аналогового сигнала $s_а(t)$ в отсчеты, для чего через равные временные интервалы дискретизации (T)

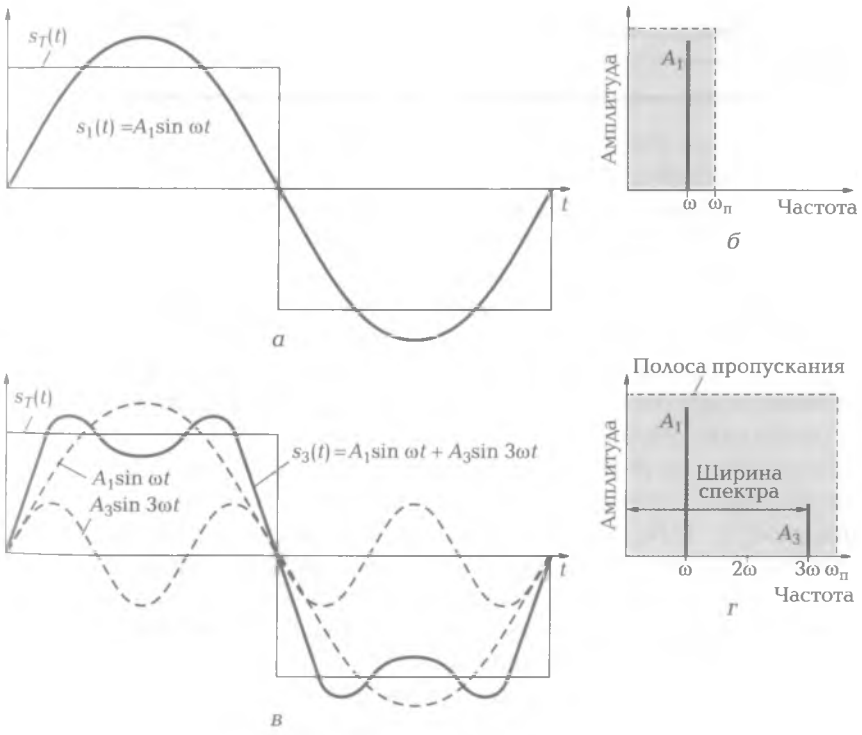


Рис. 3.2. Представление периодических колебаний одной (*а*, *б*) и двумя (*в*, *г*) гармониками

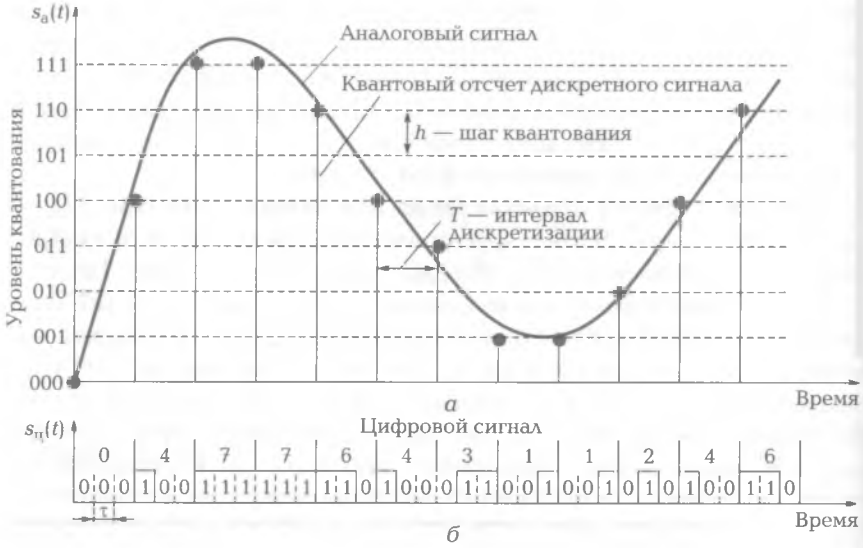


Рис. 3.3. Дискретизация аналогового сигнала (*а*) и его цифровой эквивалент (*б*)

определяются его целочисленные значения. В результате формируется периодическая последовательность коротких прямоугольных импульсов с периодом T, амплитуда которых может принимать только квантованные значения kh, где $k = 0, 1, 2, ...$; h — шаг квантования по уровню. Как видно из рис. 3.3, *а*, дискретизация сопровождается *ошибкой*, однако при большом числе N уровней квантования она незначительна.

2. На каждом интервале дискретизации T квантованная по уровню величина преобразуется в последовательность импульсов, отражающих двоичное число. Для этого интервал дискретизации разбивается на N равных частей (тактов). Если разряд двоичного числа равен 1, то на данном такте формируется импульс длительностью $\tau = T/N$. При нулевом значении разряда импульс пропускается. На рис. 3.3, *б* для $N = 3$ приведена последовательность импульсов (на каждом временно́м интервале T), которая представляет собой цифровой сигнал $s_ц(t)$, отражающий двоичные числа, а выше — его десятичные эквиваленты.

Сигналы, представленные совокупностью чисел, стали называть *цифровыми*. Представление сигналов *двоичными* числами, состоящими из нулей и единиц, обусловлено простотой их описания, технической реализации и обработки.

Переход от аналогового сигнала к цифровому реализуют с помощью аналого-цифрового преобразователя (АЦП), а от цифрового к аналоговому — цифроаналогового преобразователя (ЦАП).

Модулированные сигналы. Рассмотрим особенности модулированных сигналов для случая, когда передаваемое сообщение (первичный сигнал) представляет собой низкочастотное гармоническое колебание

$$s_\Omega(t) = A_\Omega \cos(\Omega t + \Phi), \tag{3.1}$$

а средством транспортировки сообщения от одного абонента сети к другому служит высокочастотное гармоническое колебание

$$s_\omega(t) = A_\omega \cos(\omega t + \varphi). \tag{3.2}$$

Различают три основных вида модуляции: *амплитудную* (АМ) при изменении по закону передаваемого сообщения амплитуды высокочастотного колебания $A_{АМ}(t)$, *частотную* (ЧМ) — при изменении частоты $\omega_{ЧМ}(t)$ и *фазовую* (ФМ) — при изменении фазы $\varphi_{ФМ}(t)$.

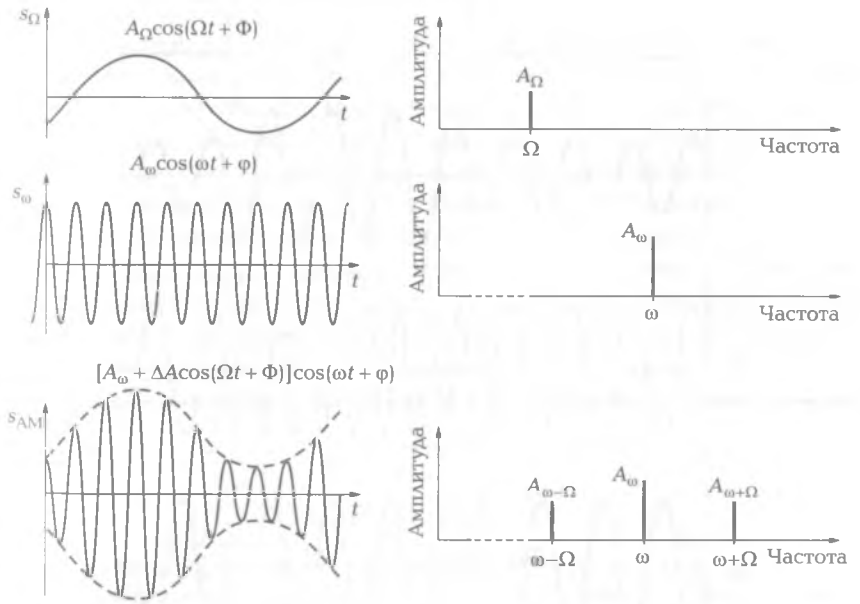


Рис. 3.4. Амплитудная модуляция:

а — первичный сигнал; *б* — несущей частоты; *в* — амплитудно-модулированный сигнал

Модулированные колебания занимают определенный спектр частот. В качестве примера оценим ширину спектра частот АМ-колебания, для чего представим его в виде

$$s_{AM}(t) = A_{AM}(t)\cos(\omega t + \varphi) = [A_\omega + \Delta A\cos(\Omega t + \Phi)]\cos(\omega t + \varphi) =$$
$$= A_\omega\cos(\omega t + \varphi) + A_{\omega+\Omega}\cos[(\omega + \Omega)t + \varphi + \Phi)] +$$
$$+ A_{\omega-\Omega}\cos[(\omega - \Omega)t + \varphi - \Phi)]. \qquad (3.3)$$

Для наглядности на рис. 3.4 дано *временно́е* и *спектральное* представление первичного сигнала [см. формулу (3.1)], несущей [см. формулу (3.2)] и амплитудно-модулированного сигнала [см. формулу (3.3)]. Выражение (3.3) свидетельствует о том, что спектр АМ-колебания состоит из *несущего* колебания и двух боковых составляющих. Ширина его спектра равна 2Ω — разности частот боковых составляющих. Спектр ЧМ- и ФМ-колебаний гораздо шире.

Различные виды двухуровневого (0, 1) цифрового сигнала $s_ц(t)$ при амплитудной, частотной и фазовой модуляции показаны на рис. 3.5. Для восстановления импульсной последовательности ис-

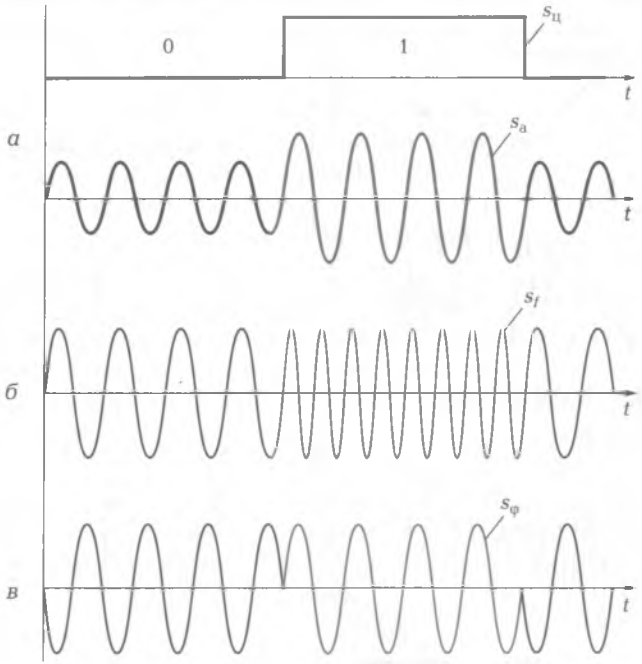


Рис. 3.5. Виды модуляций:
а — амплитудная; *б* — частотная; *в* — фазовая

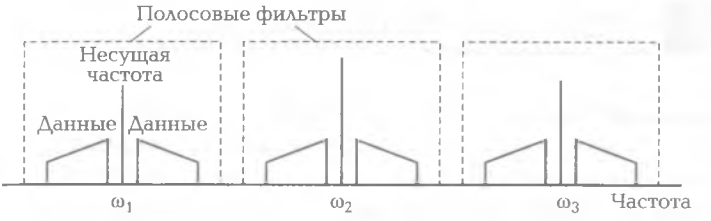


Рис. 3.6. Принцип частотного разделения каналов

пользуются амплитудные, частотные и фазовые дискриминаторы (различители).

Способы разделения каналов. Известно два способа разделения каналов.

1. *Частотный способ.* С помощью модулированных сигналов можно организовать несколько каналов связи по одной линии передачи, для чего каждый *n*-й канал связи должен работать на своей несущей частоте, не мешая другим каналам. В этом случае на приемном конце линии сообщения могут быть выделены с помощью полосовых *фильтров*, настроенных на центральную частоту $n\omega$ (рис. 3.6).

2. *Временной способ.* Сущность этого способа рассмотрим на примере 3-канальной системы, в которой сообщения представляют собой 4-битные последовательности. Система включает в себя передатчик, мультиплексор, линию связи, демультиплексор и приемник (рис. 3.7). Данные хранятся в буферной памяти передатчика. При передаче сообщения по каналу 1 мультиплексор и демультиплексор одновременно на время *T* подключаются к выводам 1 передатчика и приемника соответственно. Данные считываются из буферной памяти передатчика и по линии передаются в буферы канала 1 приемника. Затем линия последовательно подключается к выводам 2 и 3.

Рис. 3.7. Принцип временно́го разделения каналов

3.2. КОДИРОВАНИЕ СИГНАЛОВ

Основные понятия. Под *кодом* понимают символьное представление информации, а под *кодированием* — переход по определенному алгоритму от исходной формы символьного представления к новой форме. *Декодирование* — обратное преобразование.

Код можно характеризовать тремя основными параметрами:

1) *основанием*, представляющим собой число m различных элементарных символов (или алфавит), из которых составляется код. При $m = 2$ код называется двоичным или бинарным, при $m = 3$ — троичным, при $m = 4$ — четверичным и т.д. В цифровой технике используется *двоичный код*, при котором одним из элементарных символов является 1, другим — 0;

2) *значностью*, которая определяется числом n символов алфавита, образующим кодовую комбинацию. Код называется *равномерным*, если в кодовых комбинациях используется постоянное число символов, и *неравномерным* в противном случае. Примером равномерного кода является код Бодо ($n = 5$), неравномерного — код Морзе (разное n);

3) *максимальным числом N возможных кодовых комбинаций*, которое при заданных m и n выражается следующим соотношением: $N = m^n$. Например, при $m = 2$ и $n = 3$ получим восемь кодовых комбинаций:

000 001 010 011 100 101 110 111.

Требования к кодированию. К основным требованиям следует отнести:

- уменьшение уровня низкочастотной (и постоянной) составляющей в спектре передаваемых сообщений;
- обеспечение синхронизации между передатчиком и приемником;
- обнаружение и по возможности исправление битовых ошибок.

Низкочастотная составляющая. Ее наличие обусловлено тем, что передаваемое сообщение представляет собой длинную последовательность из нулей и единиц. Для наглядности будем полагать, что нулю соответствует низкий уровень напряжения, единице — высокий. Если на некотором временно́м интервале в последовательности преобладают нули, то среднее значение напряжение будет близким к нулю; если же преобладают единицы, то среднее значение будет соответствовать некоторому постоян-

ному напряжению. В связи с этим появляется низкочастотная составляющая, которая приближается к постоянному напряжению, из-за чего многие линии связи, не обеспечивающие прямого гальванического соединения между приемником и источником, могут оказаться неработоспособными.

Синхронизация передатчика. Пересылка сообщений по цифровым каналам осуществляется отдельными порциями, в отведенные такты одинаковой длительности, и приемник старается считать поступивший бит данных в середине каждого такта, т.е. он должен синхронизировать свои действия с передатчиком (рис. 3.8). Отсутствие синхронизма между передатчиком и приемником может привести к ошибкам. Темным цветом на рис. 3.8 выделены ошибочные биты при сдвиге принимаемой последовательности битов на один тактовый интервал. Использование отдельной линии связи для передачи тактовых импульсов в компьютерных сетях нецелесообразно, поэтому в сетях для синхронизации используют так называемые *самосинхронизирующиеся коды*, которые несут в себе информацию для приемника о том, в какой момент времени нужно осуществлять безошибочное распознавание очередного бита.

Распознавание и исправление искаженных данных. Чаще всего они осуществляются на канальном, сетевом, транспортном или прикладном уровнях. Однако распознавание ошибок на физическом уровне экономит время, так как приемник не ждет полного помещения кадра в буфер, а отбраковывает его сразу при распознавании ошибочных битов внутри кадра.

Требования, предъявляемые к кодам, являются противоречивыми, поэтому каждый из рассматриваемых в дальнейшем способов кодирования обладает своими достоинствами и недостатками.

Классификация способов кодирования. По назначению различают *логическое кодирование данных* (Data Encoding), используемое для уменьшения уровня низкочастотных составляю-

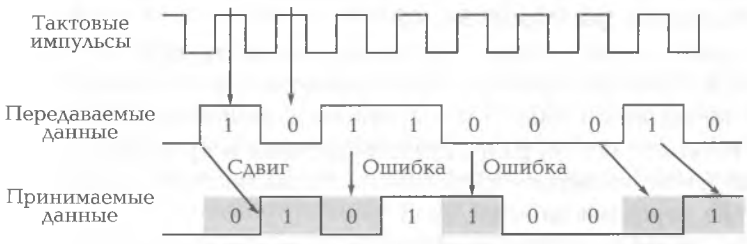


Рис. 3.8. Ошибки при отсутствии синхронизации данных

щих потенциальных кодов (избыточные коды и скремблирование), и *физическое*, или *сигнальное*, *кодирование* (Signal Encoding), предназначенное для представления дискретных символов (результатов логического кодирования) в электрические или оптические сигналы, передаваемые по линии связи.

По способности поддержки синхронизма передатчика и приемника различают самосинхронизирующиеся коды и коды, не обладающие такой способностью.

Многие классификационные признаки кодов связаны с особенностями отображения логического нуля и единицы.

В зависимости от информативного параметра различают *потенциальный способ кодирования* (или код), при котором информативным параметром является *постоянный уровень* напряжения на всем тактовом интервале, например, высокий уровень соответствует логической единице, низкий — логическому нулю, и *импульсный*, при котором информативным параметром является *перепад* напряжения.

По полярности кодовых импульсов различают следующие способы кодирования:

- *униполярный* (unipolar), когда для одного из логических значений используется импульс одной полярности, а другое значение представлено нулевым уровнем;
- *полярный* (polar), при котором логические 1 и 0 представляются двумя разными полярностями напряжения;
- *биполярный* (bipolar), при котором фиксируются три значения (положительное, нулевое и отрицательное).

Потенциальные коды. При кодировании без возврата к нулю (Non Return to Zero — NRZ) состояние может измениться только на границе тактового интервала. Известно два вида NRZ-кодов: *недифференциальный*, в котором уровни сигнала непосредственно отражают значение бита (рис. 3.9, *а*); *дифференциальный*, в котором состояние меняется в начале битового интервала для 1 и не меняется для 0 (рис. 3.9, *б*).

К достоинству метода NRZ следует отнести простоту реализации и достаточно четкую распознаваемость логических 0 и 1. Однако метод не обладает способностью самосинхронизации и требует гальванической развязки передатчика и приемника с линией связи из-за наличия постоянной составляющей напряжения в спектре передаваемого сигнала.

Модификацией рассмотренных кодов является NRZ-код с инверсией при единице (Non Return to Zero with ones In-

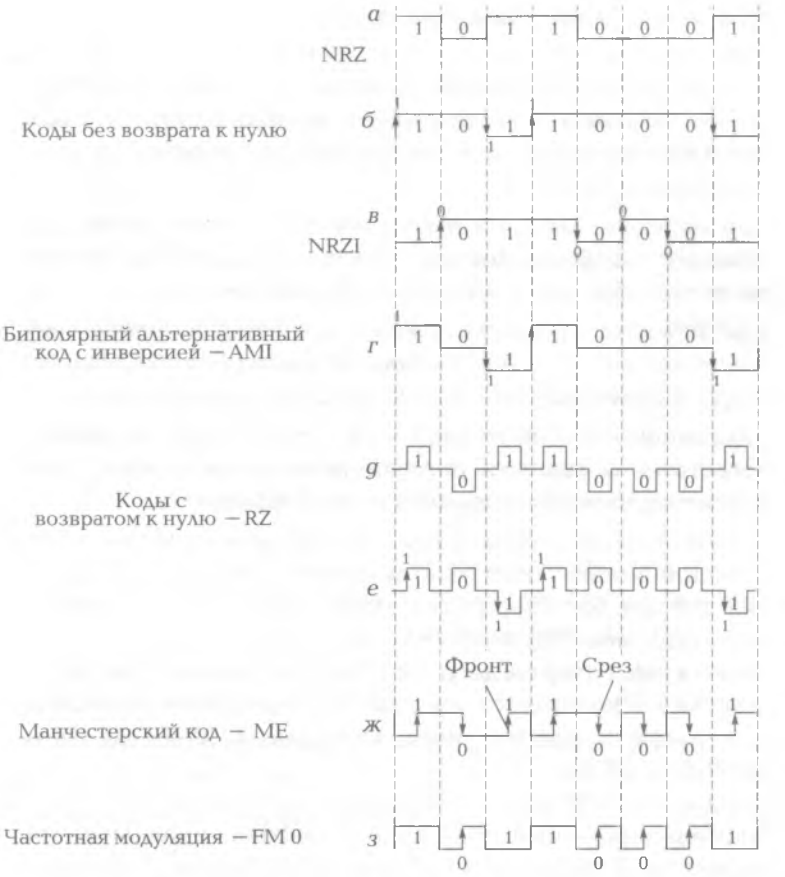


Рис. 3.9. Потенциальные (*а*—*е*) и импульсные (*ж*, *з*) коды

verted — NRZI), в котором состояние изменяется на противоположное в начале битового интервала при передаче логического 0 и остается неизменным при передаче 1 (рис. 3.9, *в*). Возможна обратная кодировка.

Биполярный код с альтернативной инверсией (Alternate Mark Inversion — AMI) — это трехуровневый код (рис. 3.9, *г*), в котором *нулевое напряжение* используется для кодирования логического нуля, а *двумя уровнями напряжения* (положительным и отрицательным) кодируется логическая единица, причем напряжение каждой последующей единицы имеет противоположный знак по сравнению с предыдущей.

Особенности AMI-кода состоят в том, что:

- при передаче длинной последовательности *единиц* код обладает способностью самосинхронизации, при этом в спектре отсутствует постоянная составляющая напряжения, так как сигнал представляет собой последовательность чередующихся разнополярных импульсов;
- при передаче длинной последовательности *нулей* сигнал представляет собой нулевое (или близкое к нулю) напряжение, поэтому способность самосинхронизации пропадает;
- при передаче *чередующихся единиц и нулей* основная гармоника имеет частоту $F_0 = N/4$ Гц (для NRZ-кода $F_0 = N/2$ Гц), что приводит к более высокой пропускной способности линии;
- нарушение строгой очередности в полярности сигналов свидетельствует о наличии ошибки (появлении ложного импульса или исчезновении полезного импульса данных).

Использование дополнительного уровня в AMI-коде требует увеличения мощности передатчика (примерно на 3 дБ) для обеспечения той же достоверности приема битов, что является общим недостатком многоуровневых кодов.

В модифицированном AMI-коде (Modified AMI — MAMI) логический 0 кодируется импульсами чередующейся полярности, а 1 — нулевым напряжением. Близкими к AMI-кодам являются коды B8ZS и HDB3.

Коды с возвратом к нулю (Return to Zero — RZ) имеют недифференциальный (рис. 3.9, *д*) и дифференциальный (рис. 3.9, *е*) варианты. В некоторый определенный момент битового интервала состояние всегда возвращается к нулю. Эти коды относятся к самосинхронизирующимся кодам, так как на каждом тактовом интервале происходит изменение уровня напряжения. Однако в дифференциальном коде отсутствует привязка единиц и нулей к определенному состоянию.

Импульсные коды. Помимо рассмотренных выше потенциальных кодов в сетях используются импульсные коды, в которых данные представлены перепадами напряжения (фронтом и срезом импульса). Ярким примером импульсных кодов является манчестерский код.

Манчестерское кодирование (Manchester Encoding) предусматривает, что текущий бит определяется по направлению смены состояния в середине битового интервала. На рис. 3.9, *ж* приведен манчестерский код (Manchester Code — MC) для случая, когда для кодирования логической 1 используется перепад напря-

жения от низкого уровня к высокому, а логического 0 — перепад от высокого уровня к низкому.

Манчестерский код имеет следующие особенности:

- обладает самосинхронизирующими способностями, так как сигнал изменяется, по крайней мере, один раз за такт передачи одного бита данных;
- отсутствует постоянная составляющая;
- основная гармоника при передаче последовательности из N единиц или нулей имеет частоту $F_0 = N$ Гц, а при передаче чередующихся единиц и нулей — $N/2$ Гц, как и у кодов AMI и NRZ;
- используются два уровня сигнала.

Известен *дифференциальный* вариант манчестерского кода, когда текущее значение одного бита (например, 0) определяется по фронту импульса в начале битового интервала, а значение другого бита (1) — по фронту и срезу импульса в середине интервала.

Частотная модуляция (Frequency Modulation 0 — FM 0) представляет собой самосинхронизирующийся полярный код, для которого характерны следующие признаки (рис. 3.9, *з*):

- на *границе* каждого битового интервала состояние изменяется на противоположное;
- при передаче 0 в *середине* битового интервала состояние меняется на противоположное;
- при передаче 1 в течение битового интервала состояние остается неизменным.

Логическое кодирование. Логическое кодирование предназначено для устранения длинных последовательностей битов из единиц или нулей, приводящих к постоянному напряжению и потере синхронизма, и используется для улучшения свойств потенциальных кодов типа AMI, NRZI или 2Q1B. Рассмотрим два вида кодов с использованием логического кодирования.

Избыточные коды. Особенности построения избыточных кодов и их использования для устранения постоянной составляющей при кодировании рассмотрим на примере двоичного кода 4B/5B (B — binary). В основе избыточного кодирования лежит:

- разбиение последовательности битов входного потока на отдельные 4-битные символы;
- представление каждого входного 4-битного символа новым (выходным) 5-битным символом. При этом получается двукратная избыточность, поскольку $2^4 = 16$ входных комбинаций пред-

ставляются символами из набора, содержащего $2^5 = 32$ комбинации;

- отбор для выходного потока 16-ти таких комбинаций, которые не содержат большого количества нулей. Остальные 16 комбинаций не пригодны для кодирования данных (Code Violation — нарушение кода). Они могут быть использованы в качестве служебных символов для поддержания синхронизации, выделения служебных полей кадров и иных целей.

Далее приведена таблица перекодировки 16 входных символов (от 0000 до 1111) в выходные, а также кодов восьми служебных символов, выбранных из оставшихся 16 комбинаций (табл. 3.1).

Символы кода 4B/5B длиной 5 бит гарантируют, что при любом их сочетании в выходном потоке не могут встретиться более трех нулей подряд. Кроме устранения постоянной составляющей и придания коду свойства самосинхронизации, избыточный код позволяет приемнику обнаружить искаженные биты. Действительно, если приемник встречает запрещенную комбинацию, значит, на линии произошло искажение сигнала.

Использование таблицы перекодировки является очень простой операцией, поэтому этот подход не усложняет сетевые адаптеры и интерфейсные блоки коммутаторов и маршрутизаторов.

Таблица 3.1

№ п/п	Входной символ	Выходной символ	№ п/п	Входной символ	Выходной символ	№ п/п	Служебный символ	Выходной символ
0	0000	11110	8	1000	10010	1	Jdle	11111
1	0001	01001	9	1001	10011	2	J	11000
2	0010	10100	10	1010	10110	3	K	10001
3	0011	10100	11	1011	10111	4	T	01101
4	0100	01010	12	1100	11010	5	R	00111
5	0101	01011	13	1101	11011	6	S	11001
6	0110	01110	14	1110	11100	7	Quit	00000
7	0111	01111	15	1111	11101	8	Halt	00100

Отметим, что известны избыточные коды с *тремя* состояниями сигнала. Например, в коде 8В/6Т для кодирования 8 бит входного символа используется код из шести символов, каждый из которых имеет три состояния. Для кода 8В/6Т на $2^8 = 256$ входных комбинаций приходится $3^6 = 729$ выходных (для кода 4В/5В — 16 и 32).

Скремблирование. Другой метод логического кодирования состоит в изменении битов входного (исходного) потока таким образом, чтобы уравнять вероятность появления единиц и нулей в выходном потоке (на линии). Устройства, выполняющие такую операцию, называются *скремблерами*. Скремблирование осуществляется по известному алгоритму, поэтому в приемнике с помощью дескремблера восстанавливается исходная последовательность битов. Скремблирование заключается в побитном вычислении результирующего кода на основании биттов входного потока (кода) и полученных в предыдущих тактах битов выходного потока кода [7].

3.3. КОМПРЕССИЯ-ДЕКОМПРЕССИЯ ДАННЫХ

Общие сведения. Количество или объем передаваемых цифровых сообщений (данных) выражается следующим соотношением:

$$V = vT, \tag{3.4}$$

где v — скорость передачи, Кбит/с; T — время передачи, с.

Как следует из соотношения (3.4), уменьшение объема V позволяет при заданной скорости v сократить время передачи T, а при заданном времени передачи T увеличить скорость v передаваемых сообщений. В связи с этим при транспортировке данных по сетям часто поступают следующим образом. На передающем узле выполняют *компрессию* (сжатие) данных, уменьшая их объем до некоторого значения V_{min}, чтобы передать данные по сети с большей скоростью. Поскольку уменьшение объема сопровождается потерей информации, на *приемном* узле выполняется обратная операция по восстановлению исходной информации, называемая *декомпрессией данных*.

В сетях используют следующие виды сжатия данных:

- *статическое*, когда данные сначала компрессируются программным способом, например, с помощью популярных архиваторов типа WinRAR или WinZip, а затем отсылаются в сеть;

- *динамическое*, реализуемое программно-аппаратными средствами в процессе передачи информации;
- *адаптивное*, позволяющее в зависимости от типа данных выбрать тот или иной алгоритм компрессии.

Рассмотрим некоторые методы компрессии (декомпрессии) данных.

Метод десятичной упаковки. Если все данные в передаваемом кадре состоят из десятичных цифр, то можно существенно сократить его длину. Дело в том, что три старших бита всех ASCII-кодов десятичных цифр содержат комбинацию 011, поэтому при обычном кодировании десятичного числа вместо 7 бит ASCII-кода потребуется только 4 бит. Для реализации метода в заголовок кадра достаточно поместить соответствующий управляющий символ.

Метод относительного кодирования. Отличительной особенностью этого метода является то, что вместо обычного кодирования цифр кодируются отклонения между двумя последовательными цифрами. При этом передаются опорное значение и сами отклонения. Такой метод используется при цифровом кодировании голоса, когда в каждом такте передается только разница между соседними замерами голоса.

Статистическое кодирование. Для представления текстовых символов в ASCII-коде (равномерный код) используется постоянное количество битов. Частота появления букв в тексте при этом не учитывается. Однако статистический анализ показывает, что в стандартном тексте на русском языке, состоящем из 1 000 символов, буква О встречается гораздо чаще (в среднем 95 раз), чем буква Ф (два раза). Поэтому целесообразно часто встречающиеся символы алфавита кодировать меньшим числом битов, а редко встречающиеся — бóльшим. При таком кодировании общее число битов в передаваемом тексте будет уменьшено, что сократит объем передаваемой информации. Для построения *неравномерных кодов* алфавита используют специальные алгоритмы (например, алгоритм Хофмана).

Словарный метод сжатия. При этом методе на основе обработанной информации составляется специальный словарь-таблица, в который записываются часто повторяющиеся последовательности битов (слова) и их коды (номера). При новом появлении аналогичных слов производится обращение к соответствующей ячейке таблицы и передается не последовательность битов, а только ее номер, что значительно сокращает объем передаваемой информации. Структурная схема одного из алгоритмов сжатия, называемого LZW (по фамилиям авторов — Lempel, Ziv, Welch), приведена

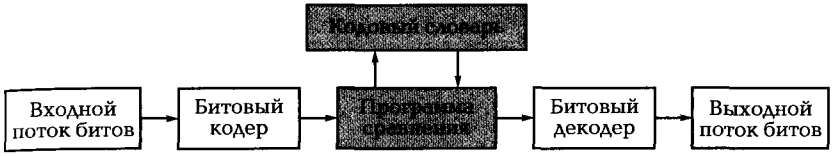


Рис. 3.10. Реализация словарного метода сжатия

на рис. 3.10. В результате поток битов на выходе, направляемый в канал связи, оказывается в несколько раз меньшим по объему, чем входной поток. Такой алгоритм по сжатию информации особенно эффективен при передаче по цифровому каналу связи цветных фотографий и телевизионных изображений. В частности, он использовался при передаче по узкополосному радиоканалу фотографий с поверхности Марса, позволяя получить на Земле снимки высокого качества.

Метод кодирования длины последовательности (Run-Lengh Encoding — RLE). Метод RLE основан на учете часто повторяющихся и следующих друг за другом одинаковых символов. Например, последовательность символов в виде AAAAAABBBCCCC будет передана как 6A3B4C, что при 8-разрядном коде сократит число передаваемых битов со 104 до 48. Этот метод дает ощутимый выигрыш при передаче изображений с одинаковыми цветовыми участками.

Следует отметить, что такие устройства коммуникационного оборудования, как модемы, мосты, коммутаторы и маршрутизаторы, поддерживают протоколы динамической компрессии с коэффициентом сжатия до 1 : 8, т. е. позволяет сократить объем передаваемых данных до восьми раз. Коэффициент компрессии зависит от типа передаваемых данных. Графические и текстовые данные имеют больший коэффициент сжатия, чем коды программ. Кроме того, существуют стандартные протоколы компрессии, например V.42bis, а также большое число нестандартных фирменных протоколов.

3.4. ОБНАРУЖЕНИЕ И ИСПРАВЛЕНИЕ ОШИБОК

При передаче информации по линиям связи по разным причинам возникают ошибки. В последнее время все большее распространение получает беспроводная среда передачи данных, в которой из-за высокого уровня помех может создаваться большее ко-

личество ошибок по сравнению с кабельной средой, поэтому в системах радиосвязи широко применяются коды с исправлением ошибок. В сетях с медным или оптоволоконным кабелем, обладающих низким уровнем ошибок, более подходящим способом борьбы с ошибками является их обнаружение и повторная передача данных. Методы обнаружения ошибок основаны на введении в состав передаваемого блока данных избыточной служебной информации, которую принято называть *контрольной последовательностью кадра* (Frame Check Sequence — FCS), позволяющей с некоторой степенью вероятности судить о достоверности принятых данных.

Контрольная сумма вычисляется как функция от основной информации, причем не обязательно путем суммирования. Принимающая сторона повторно вычисляет контрольную сумму кадра по известному алгоритму и в случае ее совпадения с контрольной суммой, вычисленной передающей стороной, делает вывод о том, что данные были переданы через сеть корректно. Рассмотрим несколько распространенных алгоритмов вычисления контрольной суммы, отличающихся вычислительной сложностью и способностью обнаруживать ошибки в данных.

Принципы обнаружения и исправления ошибок. Чтобы распознавать и устранять ошибки при передаче сообщений, необходимо знать, что представляют собой эти ошибки, чем отличаются два кода одинаковой разрядности, с помощью каких операций можно преобразовать один код в другой.

Рассмотрим два байта (рис. 3.11):

- 1100 0110 — исходный, посылаемый в линию связи;
- 1001 0011 — искаженный, принятый в узле назначения.

Как видно из рис. 3.11, *а*, байты различаются значениями в разрядах 2, 4 и 6. Составим *байт ошибки*, в котором неискаженным битам (0, 1, 3, 5, 7) назначим нулевые значения, а искаженным (2, 4, 6) — единичные значения. В этом случае для определения байта ошибки следует над исходным и искаженным байтами выполнить

Разряды (биты)		7	5	3	1	0
Исходный байт	⊕	1	1	0	0	0	1	1	0
Искаженный байт		1	0	0	1	0	0	1	0
Байт ошибки		0	1	0	1	0	1	0	0

а

Разряды (биты)		7	6	5	4	3	2	1	0
Искаженный байт	⊕	1	0	0	1	0	0	1	0
Байт ошибки		0	1	0	1	0	1	0	0
Исходный байт		1	1	0	0	0	1	1	0

б

Рис. 3.11. Выявление (*а*) и исправление (*б*) ошибки

логическую операцию, которая имеет следующие названия: *неравнозначность*, сложение по модулю 2, исключающее ИЛИ (XOR). По своей сути эта операция сравнивает два бита, причем в случае их неравенства результатом является единица ($0 \oplus 1 = 1$, $1 \oplus 0 = 1$), в противном случае ($0 \oplus 0 = 0$, $1 \oplus 1 = 0$) — нуль. С помощью операции неравнозначности можно восстановить искаженный байт (см. рис. 3.11, *б*).

Общее число d битовых позиций с разными значениями разрядов двух сравниваемых сообщений называется *интервалом Хэмминга*. Для приведенного примера интервал Хэмминга $d = 3$.

Принципы построения корректирующих кодов. Допустим, что передаваемое сообщение (кадр) состоит из m бит данных и r дополнительных (контрольных) разрядов, т.е. общая длина сообщения составляет n бит ($n = m + r$). Тогда из 2^n возможных кодовых комбинаций данные допускают только 2^m. Число недопустимых комбинаций равно $2^n - 2^m = 2^{m+r} - 2^m = 2^m(2^r - 1)$.

Появление в принятом сообщении недопустимой комбинации свидетельствует об ошибке. Рассмотрим два случая.

Случай 1. Использование для обнаружения ошибок бита четности.

Рассмотрим код, в котором к данным присоединяется один дополнительный бит, называемый *битом четности*. Значение бита четности выбирается таким образом, чтобы общее число битов со значением 1 в кодированном слове было четным. В этом случае любая одиночная ошибка приведет к нечетному количеству единичных битов. Действительно, при изменении в сообщении 0 на 1 появляется дополнительная единица; изменение 1 на 0 приведет к уменьшению единиц. Однако наличие двух ошибок в сообщении сохраняет четное количество единиц, поэтому такой код может использоваться только для обнаружения *одиночных* ошибок.

Случай 2. Код с исправлением ошибок для 4-битных слов. Рассмотрим три пересекающихся круга *A*, *B* и *C*, которые создают семь секторов (рис. 3.12). Закодируем слово из 4 бит 1100, для чего в четыре сектора занесем по одному биту (см. рис. 3.12, *а*). В каждый из трех пустых секторов добавим по одному биту с таким значением, чтобы в каждом круге (*A*, *B* и *C*) находилось четыре числа (0, 0, 1 и 1), которые в сумме дают четное число 2. Добавленные биты помечены на рис. 3.12, *б* кружочками и называются *битами четности*. В результате получено 7-битное слово, состоящее из 4 бит данных и 3 бит четности. Если, например, теперь в секторе *AB* бит изменится с 0 на 1 (см. рис. 3.12, *в*), то будет зафиксирована ошибка, так как в кругах *A* и *B* нарушится четность (появятся

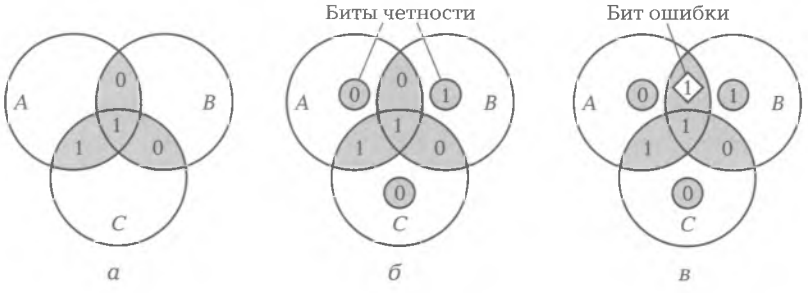


Рис. 3.12. Действие кода с исправлением ошибок:
а — исходное слово; *б* — слово с битами четности; *в* — выявление бита ошибки

три единицы вместо двух). Для исправления ошибки путем изменения только одного бита необходимо вернуть биту ошибки в секторе *AB* прежнее значение 0. Этот способ позволяет обнаружить и исправить ошибку.

Для обнаружения ошибок широко используются полиномиальные коды, а также код Хемминга, дающий возможность не только выявлять, но исправлять ошибки [7].

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. В чем состоит смысл следующих терминов: «информация», «сообщение», «сигнал», «данные», «модуляция», «кодирование», «скремблирование», «контрольная последовательность кадра»?
2. Какие основные виды сигналов вам известны? Дайте их краткую характеристику.
3. Почему широко используются гармонические колебания?
4. Чем обусловлен широкий спектр импульсных сигналов?
5. Каким образом осуществляется переход от аналоговых сигналов к цифровым?
6. Какие виды модуляции находят широкое применение?
7. Как определяется ширина спектра амплитудно-модулированного колебания?
8. Какие способы разделения каналов используют на практике и в чем состоит их суть?
9. Какими параметрами характеризуется код?
10. Какие основные требования предъявляются к кодированию?
11. Каковы основные способы кодирования? Дайте их краткую характеристику.

12. В чем состоят особенности потенциальных и импульсных кодов?
13. Какие виды логического кодирования используются на практике и в чем заключаются их особенности?
14. Для чего предназначена компрессия-декомпрессия данных и какие методы используются на практике?
15. В какой среде передачи данных наблюдается наиболее высокий уровень ошибок и как с ними борются?
16. На чем базируются принципы обнаружения и исправления ошибок и принципы построения корректирующих кодов?

Глава 4

БАЗОВЫЕ СЕТЕВЫЕ ТЕХНОЛОГИИ

4.1. МЕТОДЫ ДОСТУПА К СЕТИ

Общие сведения. При использовании одной линии передачи (связи) несколькими абонентами (источниками сообщений) возникает проблема раздельного подключения (доступа) к ней. Для решения этой проблемы разработано большое число различных методов, определяющих строгие правила доступа к разделяемой среде передачи данных. Их можно разбить на три группы.

1. *Селективные методы.* Особенность этих методов состоит в том, что передача начинается после получения соответствующего разрешения. Например, при *циклическом опросе* центральное устройство по очереди направляет разрешение каждой рабочей станции (компьютеру), после получения которого можно начать передачу. В методе *с передачей маркера* (или токена) разрешение передается от станции к станции.

2. *Методы, основанные на принципе соперничества.* Каждая станция перед началом передачи пытается получить доступ к линии связи. Ситуация одновременного обращения к одному каналу передачи называется *коллизией* (Collision — столкновение). Для ее разрешения должна соблюдаться определенная дисциплина. Эту группу составляют методы состязаний: с прослушиванием линии связи до передачи; с прослушиванием до передачи и во время передачи; с прогнозированием столкновений; с обучающим прогнозированием столкновений и др.

3. *Методы с резервированием времени.* Передача возможна только в течение тех интервалов времени, которые заранее выделены (зарезервированы) для данной рабочей станции. Резервирование производится в начале соединения, а также в любой нужный пользователю момент.

По способу доступа различают два вида методов: со случайным и детерминированным доступом.

Методы со случайным доступом основаны на соперничестве. Они строятся с учетом возможности возникновения конфликтов и обусловливают способы их разрешения. Методы устойчивы к отказам сетевого оборудования, однако не гарантируют быстрого доступа.

Методы с детерминированным доступом определяют четкий порядок предоставления доступа абонентам сети и практически полностью исключают конфликты. К ним относятся селективные и кольцевые методы.

По принципу управления различают централизованные и децентрализованные (распределенные) методы доступа к среде передачи.

В *централизованных методах* все управление доступом сосредоточено в одном (центральном) узле сети, который всегда имеет возможность предоставить право на передачу только одному абоненту. Достоинством централизованных методов является отсутствие конфликтов, а их недостатком — возможность отказов в доступе при большом числе запросов.

В *децентрализованных* (*распределенных*) *методах* единый центр управления отсутствует и управление доступом полностью предоставлено абонентам сети, т.е. каждый узел самостоятельно обнаруживает и предотвращает все возможные конфликты. К достоинству методов следует отнести высокую устойчивость к отказам и большую гибкость управления (табл. 4.1).

В качестве примера рассмотрим распространенный метод коллективного доступа с опознаванием несущей и обнаружением коллизий (Carrier Sense Multiple Access with Collision Detection — CSMA/CD).

Метод CSMA/CD. Этот метод основан на принципе соперничества и находит применение в сетях Ethernet.

Организация доступа к среде и передачи сообщений. Прежде чем начать передачу, сетевой адаптер прослушивает линию связи, чтобы выявить, свободна она в данный момент времени или нет. Если в среде передачи обнаруживается сигнал, то передача на некоторое время откладывается. Затем предпринимается повторная попытка получить доступ к среде передачи (путем прослушивания). Если линия свободна, то сетевой адаптер начинает передачу *кадра*, представляющего собой единицу данных, пересылаемых в сети Ethernet от одной станции к другой. Признаком незанятости среды является отсутствие в ней сигналов.

Станция инициирует передачу кадра. Кадр данных всегда сопровождается преамбулой из семи одинаковых байтов 10101010 и

Таблица 4.1

Группа	Методы доступы	Достоинства	Недостатки
1	Селективные	Отсутствие конфликтов	Дополнительные аппаратные средства
	На принципе соперничества	Простота реализации	Наличие коллизий. Применяется только в сетях с логической общей шиной
	С резервированием времени	Обеспечивают гарантированный доступ	Нерациональный расход предоставляемого на доступ времени, снижающий производительность сети
2	Случайные	Простота и низкая стоимость цепей доступа. Устойчивы к отказам сетевого оборудования	Отсутствует гарантия быстрого доступа. Неопределенное время прохождения кадра, резко возрастающее при увеличении нагрузки на сеть, что ограничивает их применение в системах реального времени
	Детерминированные	Ограниченное время прохождения кадра, мало зависящее от нагрузки	Дополнительные аппаратные средства
3	Централизованные	Отсутствие конфликтов	Возможность отказов в доступе при большом числе запросов
	Децентрализованные	Высокая устойчивость к отказам и большая гибкость управления	Значительные аппаратные затраты

8-го байта 10101011. Преамбула служит для вхождения приемника в синхронизацию с передатчиком. Две последние единицы в 8-м байте свидетельствуют о том, что преамбула закончилась и следующий бит является началом кадра. В первых шести байтах кадра содержится адрес передающей станции и станции назначения. Все подключенные к линии станции записывают байты передаваемого кадра в свои внутренние буферы. Станция назначения обна-

руживает собственный адрес и продолжает записывать содержимое кадра в свой внутренний буфер, после чего приступает к обработке данных. Остальные станции прекращают прием кадра.

После окончания передачи кадра все станции сети обязаны выдержать *технологическую паузу*, необходимую для приведения сетевых адаптеров в исходное состояние, а также для предотвращения монопольного захвата среды одной станцией. Длительность паузы, или *межпакетного интервала* (Inter Packet Gap — IPG), равна 9,6 мкс. После ее окончания станции могут инициировать передачу своего кадра, поскольку линия связи свободна.

Возникновение, обнаружение и обработка коллизий. Механизм прослушивания линии связи и наличие межпакетного интервала между кадрами не исключают коллизии, для возникновения которой не обязательно, чтобы несколько станций начали передачу *абсолютно* одновременно. В реальных условиях инициирование передачи двумя и более станциями после проверки занятости линии связи происходит неодновременно, пусть с очень коротким, но конечным интервалом времени, поэтому в линию связи может поступать несколько сигналов.

Для обнаружения коллизии все станции, инициирующие передачу, контролируют линию связи. Каждая станция сравнивает передаваемый и наблюдаемый сигналы, и если они отличаются, то фиксируется факт *обнаружения коллизии* (Collision Detection — CD). Станция, обнаружившая коллизию, сразу прерывает передачу своего кадра и посылает в сеть специальную последовательность из 32 бит, называемую *jam-последовательностью*. Такая мера повышает эффективность обнаружения коллизии всеми станциями сети.

После обнаружения коллизии передающая станция должна прекратить передачу в течение короткого интервала времени, т. е. сделать *случайную паузу*. Затем она может снова инициировать (предпринять попытку) передачу кадра. Случайная пауза в сети Ethernet может принимать значения от 0 до 52,4 мс. Если 16 последовательных попыток передачи кадра вызывают коллизию, то передатчик должен прекратить попытки и отбросить этот кадр. Описанная процедура обработки коллизии носит название *усеченного экспоненциального двоичного алгоритма отсрочки*.

Иллюстрация метода. Рассмотрим сеть из трех станций, подключенных к линии связи (рис. 4.1). Пусть станция 2 прослушивает линию связи (ПЛС) и обнаруживает, что линия свободна. В этом случае она инициирует передачу и данные поступают в линию связи «Передача С2». Если в это же время попытается начать

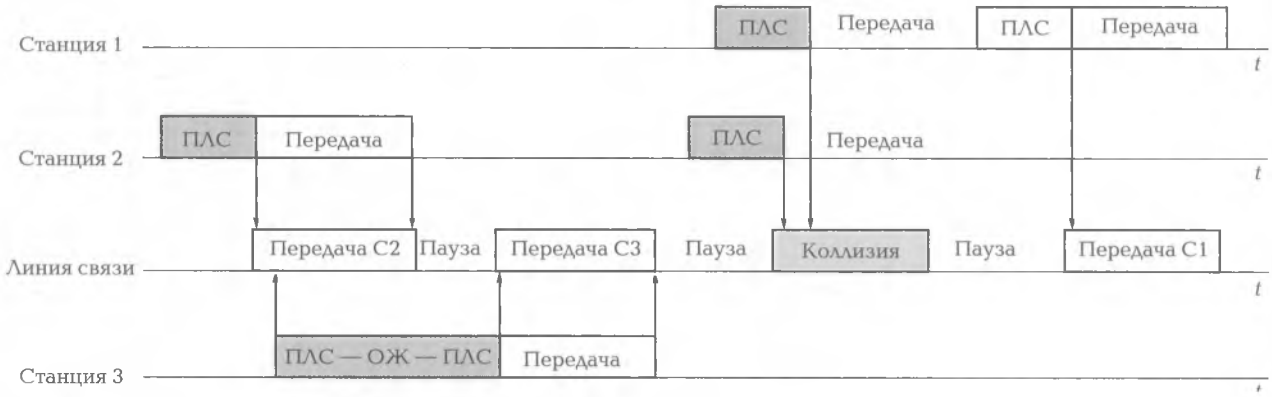


Рис. 4.1. Метод доступа CSMA/CD:
ПЛС – прослушивание линии связи; ОЖ — ожидание

передачу станция 3, то такая попытка будет отвергнута, поскольку при прослушивании обнаружится занятость (наличие сигналов «Передача С2» линии. Станция 3 переходит в режим «Ожидание» до освобождения линии («Пауза») и после вторичного прослушивания получает доступ к линии «Передача С3».

Теперь допустим, что по завершении передачи С3 во время паузы предпринимают попытку передать свои данные станции 1 и 2. Прослушивание показывает, что линия связи свободна и станции 1 и 2 инициируют передачу («Передача»). В этом случае возникает коллизия, так как сигналы обеих станций поступают в линию. Как показано на рис. 4.1, линией связи завладеет станция 1 («Передача С1») после ее прослушивания во время случайной паузы.

4.2. МЕТОДЫ КОММУТАЦИИ И ПЕРЕДАЧИ ДАННЫХ

Общие сведения. В больших сетях невозможно предоставить каждой паре абонентов свой собственный канал связи для постоянного монопольного владения, поэтому при организации канала всегда применяют какой-либо способ временного соединения линий связи между отдельными узами сети, реализуемого с помощью коммутаторов. Абоненты соединяются с коммутаторами индивидуальными линиями связи, каждая из которых используется в любой момент времени только одним, закрепленным за этой линией абонентом. Между коммутаторами (узлами сети) линии связи разделяются несколькими абонентами, т.е. используются совместно. Существует два распространенных метода коммутации: *коммутация каналов* (Circuit Switching), при которой канал создается на время одного сеанса связи между двумя абонентами, и *коммутация пакетов* (Packet Switching), когда канал формируется для передачи одного или нескольких пакетов данных.

Коммутация каналов. Выявим особенности способа коммутации каналов на примере сети (рис. 4.2), сопровождая изложение пояснениями из области *телефонии*. При этом способе коммутации составной физический канал между двумя абонентами образуется путем последовательного соединения отдельных линий передачи с помощью коммутаторов, для чего предварительно одним из абонентов выполняется процедура установления соединения. Допустим, что абонент А1 хочет установить связь с абонентом В1. В этом случае выполняется такая последовательность действий:

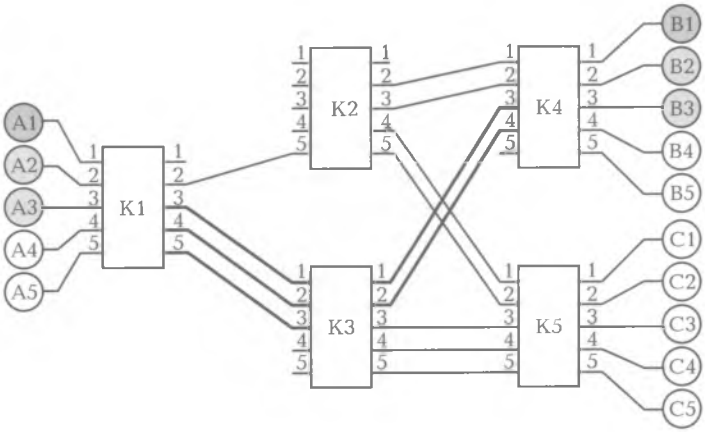


Рис. 4.2. Иллюстрация принципа коммутации каналов

1) абонент (узел) A1 посылает запрос на установление соединения коммутатору K1 с указанием адреса назначения абонента B1 (звонок по телефонному номеру);

2) коммутатор K1 выбирает маршрут для создания составного канала и передает запрос следующему коммутатору, например K2. В свою очередь коммутатор K2 передает запрос коммутатору K4, который направляет его абоненту B1;

3) абонент B1, приняв запрос на установление соединения, направляет по уже установленному каналу ответ исходному узлу A1, после чего процедура установления соединения завершается и узлы A1 и B1 могут обмениваться по нему данными (вести телефонный разговор).

Таким образом, для создания канала запрос должен сам пройти весь маршрут от A1 до B1, чтобы удостовериться, что все необходимые линии связи, а также конечный узел B1 свободны. При прохождении маршрута в каждом из коммутаторов K1, K2, K4 выполняется соединение входа с требуемым выходом и запоминается информация о том, что соответствующая линия связи выделена (зарезервирована) для соединения абонентов A1 и B1. Например, в коммутаторе K1 вход 1 соединяется с выходом 2, а в коммутаторе K2 в зависимости от алгоритма работы возможно соединение вход 5 — выход 2 или вход 5 — выход 3.

Важной особенностью коммутации каналов является возможность *отказа* в установлении соединения. Отказ фиксируется в случае занятости вызываемого абонента или всех возможных

маршрутов. Если после установления связи между абонентами А1 и В2 поступят два запроса от абонентов А2 и А3 на установление соединений с абонентами В2 и В3, то они могут быть удовлетворены, но не через коммутатор К2, а только через коммутатор К3. Если же затем последует запрос на соединение абонентов А4 и В4, то этот запрос не будет выполнен из-за нехватки линий связи. Между К1 и К4 существует только три связи: одна связь К1 → К2 → К4 и две связи К1 → К3 → К4. Таким образом, чем больше в данный момент установлено в сети соединений, тем больше вероятность отказа в запросе на установление нового соединения.

После того как установлено соединение абонентов А и В, в их полное распоряжение поступает канал, обладающий фиксированной пропускной способностью. Абоненты не могут передавать данные в сеть со скоростью, превышающей пропускную способность линии. При меньшей скорости передачи недоиспользуется пропускная способность канала.

Поскольку сети с коммутацией каналов обеспечивают между коммутаторами (К1 и К4) одновременную передачу данных нескольких абонентских каналов, можно с помощью мультиплексирования увеличить пропускную способность абонентских каналов. Например, объединяя в один канал три линии связи, можно в три раза увеличить скорость передачи между абонентами коммутаторов К1 и К5. Мультиплексирование в сетях с коммутацией каналов имеет особенности, обусловленные тем, что все объединяемые линии связи должны проходить по одному маршруту. В настоящее время для мультиплексирования абонентских каналов используются две технологии: *частотного* мультиплексирования (Frequency Division Multiplexing — FDM) и мультиплексирования *с разделением времени* (Time Division Multiplexing — TDM).

Коммутация пакетов. Технология коммутации каналов не обеспечивает эффективного использования среды передачи данных из-за пульсирующего характера трафика. Например, передача речевых сообщений по предоставленному двум абонентам цифровому каналу ведется с постоянной скоростью 64 Кбит/с независимо от того, говорят они или молчат, хотя во время каждой паузы можно было бы передавать дополнительную информацию. Работа пользователей компьютеров в Internet также чередуется периодами интенсивного (при загрузке web-страницы) и ослабленного (при поиске нужной информации) трафика. Количественно неравномерность трафика оценивается *коэффициентом пульсации* трафика отдельного пользователя сети, который принимается рав-

Рис. 4.3. Передача сообщений с коммутацией пакетов

ным отношению максимально возможной скорости (интенсивности) обмена данными к среднему значению и может достигать до 100 : 1. Для повышения эффективности передачи компьютерного трафика (уменьшения коэффициента пульсации) используется *технология передачи с коммутацией пакетов*, суть которой состоит в следующем (рис. 4.3):

1) передаваемое сообщение разбивается на небольшие пакеты (от 46 до 1 500 байт);

2) каждый пакет снабжается *заголовком* с адресной информацией, необходимой для доставки пакета узлу назначения; *номером пакета*, который будет использоваться узлом назначения для сборки сообщения; *концевиком* (или трейлером — trailer), содержащим контрольный код CRC для обнаружения ошибок;

3) пакеты передаются по сети как независимые информационные блоки. Коммутаторы сети принимают пакеты от конечных узлов и на основании адресной информации передают их друг другу, а в итоге — узлу назначения.

Пакетные коммутаторы (в отличие от коммутаторов каналов) содержат *буферную память* для временного хранения пакетов, а также *коммутирующий блок* (рис. 4.4, *а*), в состав которого входят интерфейсные процессоры (для каждого порта) и центральный процессор, координирующий их работу. Пакетному коммутатору буферизация необходима в целях:

- *принятия решения о продвижении пакета*. Принимаемый пакет последовательно бит за битом заносится в буфер входного порта для проверки контрольной суммы в целях выявления ошибок. Если проверка фиксирует отсутствие искажений, то коммутатор начинает обрабатывать пакет. По адресу назначения он определяет следующий коммутатор;

- *согласования скоростей поступления пакетов и их коммутации.* Если коммутирующий блок не успевает обрабатывать пакеты, то организуются входные очереди;
- *согласования скоростей передачи данных внешних каналов*, подключенных к портам пакетного коммутатора. В том случае, когда скорость поступления пакетов канала, подключенного к входному порту, превышает пропускную способность канала, подключенного к выходному порту, необходимо организовать выходную очередь (см. рис. 4.4, *а*), иначе пакеты будут потеряны.

Организацию обмена в сети с коммутацией пакетов, содержащей четыре 4-портовых пакетных коммутатора, иллюстрирует схема на рис. 4.4, *б*. Поток данных, поступающий от каждого из оконечных узлов сети (компьютеров К) на коммутаторы, распределен во времени неравномерно. Однако коммутаторы 2, 4 благодаря наличию в них буферной памяти позволяют более равномерно загрузить магистральный канал, соединяющий коммутаторы 1 и 3 верхнего уровня, т.е. получить более низкий коэффициент

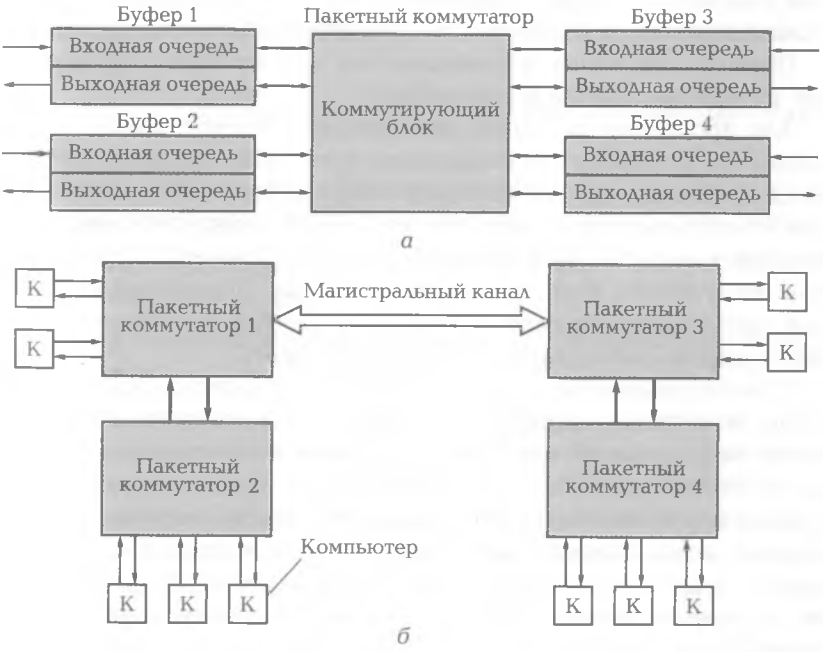


Рис. 4.4. Пакетный коммутатор (*а*) и организация обмена с коммутацией пакетов (*б*)

пульсации трафика на магистральном канале, чем на каналах абонентского доступа.

Дейтаграммная передача. Этот способ передачи данных не требует предварительного создания канала между двумя абонентами и ускоряет доставку данных. Он основан на независимой передаче отдельных пакетов между узлами сети, т.е. каждый пакет является независимой единицей передачи, называемой *дейтаграммой* (Datagram). Процедура обработки пакета определяется только значениями его параметров. Никакая информация об уже переданных пакетах сетью не хранится и в ходе обработки очередного пакета не учитывается. Решение о продвижении пакета коммутатор принимает на основе *таблицы коммутации* (маршрутизации, продвижения), которая содержит набор адресов назначения и адресную информацию, однозначно определяющую следующий по маршруту (транзитный или оконечный) узел.

Передача с установлением виртуального канала. Под *виртуальным каналом* (Virtual Channel) понимают предварительно проложенный фиксированный маршрут, соединяющий два оконечных узла в сети с коммутацией пакетов. Различают два вида виртуальных каналов: постоянный и динамический.

Постоянный канал прокладывается администратором сети путем ручной настройки коммутаторов.

Для прокладки *динамического канала* узел-источник посылает запрос на установление соединения с указанием *адреса* назначения и *метки* для идентификации потока данных. На пути следования от отправителя до получателя запрос в каждом коммутаторе оставляет запись с пояснением, каким образом коммутатор должен обслуживать пакет с известной меткой. Созданный виртуальный канал идентифицируется такой же меткой. Метки потока данных и виртуального канала должны совпадать.

При последующей передаче пакетов они всегда направляются по проложенному маршруту. В случае отказа действующего соединения виртуальный канал прокладывается по новому маршруту, который обойдет отказавшие участки сети. Время, затраченное на установление виртуального канала, компенсируется быстрой передачей всего потока пакетов, поскольку коммутаторы не анализируют адреса оконечных узлов (как при дейтаграммной передаче), а по метке распознают принадлежность пакета к данному виртуальному каналу.

При передаче данных по виртуальному каналу адрес узла назначения не указывается, так как его функции выполняет *метка*.

Каждый коммутатор считывает значение метки из заголовка поступившего пакета и, просмотрев свою таблицу коммутации, определяет, на какой выходной порт передать этот пакет. Таблица коммутации в сетях с виртуальными каналами содержит записи только о проходящих через коммутатор виртуальных каналах. Кроме того, заголовок пакета вместо длинного адреса имеет компактный идентификатор потока, поэтому на обработку пакетов коммутатор затрачивает не много времени.

4.3. АДРЕСАЦИЯ УЗЛОВ СЕТИ

Общие сведения. Одной из важнейших проблем при передаче сообщений является адресация узлов сети, или сетевых интерфейсов. *Узлом сети* называют оконечное (или промежуточное) устройство, наделенное одним или несколькими адресами, а *сетевым интерфейсом* — точку сопряжения устройства с сетью. Множество различных адресов можно классифицировать по следующим признакам.

По числу адресуемых узлов (интерфейсов) различают адреса:

- *уникальные*, используемые для обращения к отдельным узлам сети;
- *произвольной рассылки*, представляющие собой группу адресов, которые позволяют обратиться к любому из узлов этой группы;
- *групповые*, обеспечивающие одновременный доступ ко всем узлам выделенной группы;
- *широковещательные*, предназначенные для обращения ко всем узлам сети.

По способу описания адреса подразделяют на *числовые*, представленные в виде *N*-разрядного числа в двоичной или другой системе счисления, например 129.26.255.255 или 81.1A.FFFF, и *символьные*, для описания которых используются буквы латинского алфавита. Символьный адрес обычно несет смысловую нагрузку и легко запоминается.

По принципу организации адресного пространства, под которым понимают множество всех допустимых адресов в рамках некоторой схемы адресации, выделяют организации адресного пространства:

- *линейную* (или плоскую), при которой в качестве адреса используется вся совокупность чисел от 0, 1, 2, ... до некоторого значения $2N - 1$, где N — разрядность адреса. Примером линейной организации могут служить рассматриваемые ниже MAC-адреса, предназначенные для однозначной идентификации узлов в ЛС;
- *иерархическую*, при которой адресное пространство представляет собой вложенные друг в друга подгруппы, которые, последовательно сужая адресуемую область, в конце концов, определяют отдельный сетевой интерфейс. При трехуровневой организации адрес конечного узла задается тремя идентификаторами: идентификатором группы (G), в которую входит данный узел; идентификатором подгруппы (P) и идентификатором узла (U), однозначно определяющим его в подгруппе. Иерархическая организация адресации позволяет при заданных G и P использовать в качестве адреса только его младшую часть U.

В процессе пересылки сообщения, как правило, применяются различные способы адресации. Например, для пользователей удобно адресовать узлы (компьютеры) иерархическими символьными именами. Для ускорения передачи сообщения из одной сети в другую символьные имена автоматически заменяются числовыми адресами. После доставки сообщения в сеть назначения вместо иерархического числового адреса используется линейный аппаратный адрес компьютера.

Преобразование адресов из одного вида в другой осуществляется согласно специальным вспомогательным протоколам, которые называются *протоколами разрешения адресов*. Для установления соответствия между адресами различных типов используются централизованный и распределенный подходы.

При *централизованном подходе* в сети выделяются специальные компьютеры для хранения таблиц соответствия имен различных типов. Такие компьютеры называются *серверами имен*. Компьютеры-клиенты обращаются к серверу имен с запросами, чтобы по символьному имени найти числовой номер (адрес) необходимого компьютера.

При *распределенном подходе* в каждом компьютере хранятся все назначенные ему адреса. Чтобы определить аппаратный адрес компьютера-приемника по его иерархическому числовому адресу, компьютер-источник посылает в сеть широковещательный запрос с известным ему адресом. Все компьютеры сети сравнивают содержащийся в запросе адрес с собственным адресом, и тот ком-

пьютер, у которого оба адреса совпали, посылает ответ, содержащий искомый аппаратный адрес.

Одной из особенностей стека TCP/IP является гибкая система адресации, в которой используется три типа адресов: *локальные* (или аппаратные) MAC-адреса, *IP*-адреса и *символьные* доменные имена.

MAC-адресация. MAC-адреса назначаются сетевым адаптерам и сетевым интерфейсам маршрутизаторов и являются уникальными адресами. С их помощью осуществляется централизованное управление доступом к среде передачи (Media Access Control — MAC) на канальном уровне.

Формат MAC-адресов. Адрес представляет собой двоичное число длиной 6 байт (или 48 бит), которое записывают в виде шести пар шестнадцатеричных цифр, разделенных тире или двоеточиями. В формате адреса (рис. 4.5, *а*) *старшие* три байта представляют код производителя, присвоенный организацией IEEE (Institute of Electrical and Electronics Engineers), например, компания *3COM* имеет код производителя 00-20-AF, а *младшие* три байта присваивает сам производитель для идентификации своей продукции, что позволяет ему выпустить 2^{24} изделий (сетевых адаптеров).

Формат MAC-адреса сети Ethernet имеет обратный порядок расположения битов в байте: младший бит байта изображается в самой левой позиции поля, а старший бит — в самой правой (рис. 4.5, *б*). Однако при передаче битов в линию связи сохраняется общепринятый порядок их следования.

Обработка адресов при передаче сообщений. Если физический адрес принятого пакета отличается от адреса

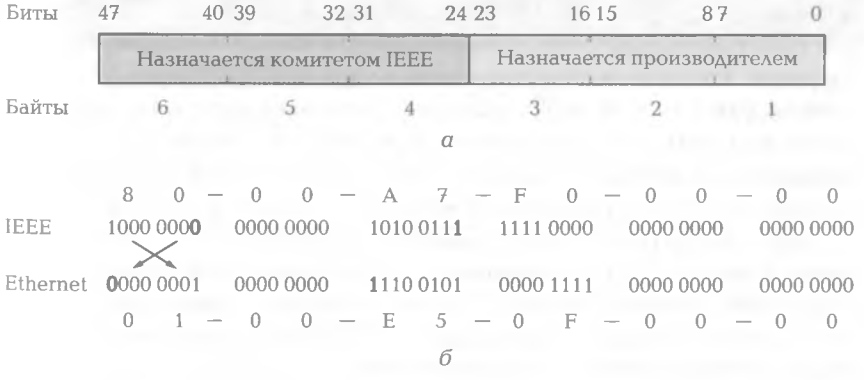


Рис. 4.5. Формат MAC-адреса сети Ethernet (*а*) и порядок расположения битов в байте (*б*)

компьютера, то полученный пакет отбрасывается сетевым интерфейсом на канальном уровне и остальная часть стека протоколов его не обрабатывает.

При *совпадении адресов* пакет принимается и передается на более высокие уровни, где обрабатывается в соответствии со своим назначением.

При *широковещательной* рассылке данных пакет, посланный по адресу FF-FF-FF-FF-FF-FF, получают все компьютеры. Такой пакет направляется вверх по стеку протоколов для обработки и выяснения адресата. Ответ дает только тот компьютер, для кого предназначено полученное сообщение. Остальные компьютеры отбрасывают такой пакет после его обработки и выяснения, что он предназначен не для них.

IP-адресация. В больших сетях необходима собственная система адресации, не зависящая от способов адресации в отдельных сетях (подсетях) и позволяющая однозначно идентифицировать (определять) любой узел (интерфейс, сетевой адаптер, хост) всей сети. Такой системе удовлетворяет IP-адресация. Любой IP-адрес имеет длину 32 бит (разряда), разделенные на *префикс* (старшие биты) и *хост-часть* (младшие биты). Префикс определяет номер сети, хост-часть — номер узла.

Максимальное число различимых IP-адресов равно 2^{32}, или 4 294 967 296. Одна из основных задач при построении системы IP-адресации состоит в том, чтобы разделить адресное пространство между сетями и узлами. Рассмотрим некоторые способы ее решения.

Классовая IP-адресация. Для разделения составной сети на сети и узлы введены классы A, B, C и D (рис. 4.6) с фиксированным числом номеров сетей. Классы отличаются числом разрядов, выделенных для идентификации сетей. Например, для класса A выделено семь разрядов, поэтому количество сетей не должно превышать $2^7 = 128$, а число узлов в сети — $2^{24} \approx 64$ млн. Поскольку адреса не могут состоять из одних нулей или единиц и, кроме того, некоторые разряды отводятся для служебных целей, в реальных условиях максимальное количество сетей и узлов имеет меньшее значение (табл. 4.2).

Адрес может быть представлен в двоичной или шестнадцатеричной форме. Однако наиболее распространенной формой представления IP-адреса является запись в виде четырех десятичных чисел, разделенных точками (рис. 4.7). Каждое десятичное число отражает байт (октет) и соответствует его значению.

Для идентификации класса используются старшие биты адреса, а для идентификации сети — старшие байты. Приведенный на

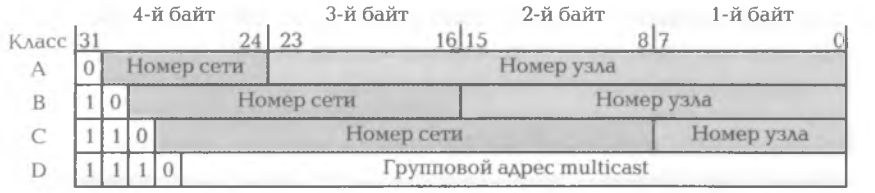


Рис. 4.6. Формат IP-адреса

рис. 4.7 адрес относится к классу B (идентификатор 10), имеет номер сети 32 778 (128.10) и номер узла 542 (2.30). В табл. 4.2 для каждого класса помимо идентификаторов приведены диапазон номеров сети и максимальное число сетей и узлов. Эти данные свидетельствуют о том, что сети класса A относятся к большим сетям, класса C — к малым, а сети класса B занимают среднее положение.

Адреса классов A, B и C являются *индивидуальными адресами* (Unicast Address) и используются для идентификации отдельных узлов (сетевых интерфейсов). Адреса класса D относятся к адресам многоабонентской доставки сообщений (Multicast Address), которые идентифицируют группу узлов, принадлежащих в общем случае разным сетям. Входящий в группу адрес наряду с обычным индивидуальным IP-адресом дополнительно получает групповой адрес, который помещается в поле адреса назначения IP-пакета. Если при отправке пакета в этом поле указан адрес класса D, то такой пакет должен быть доставлен всем узлам, которые входят в группу. Один и тот же узел может входить в несколько групп.

Таблица 4.2

Класс	Идентификатор		Диапазон номеров сети	Число сетей	Число узлов на сеть
	класса	сети (префикс)			
A	0	4-й байт	1.0.0.0 — 126.0.0.0	126	16 777 216
B	10	3-й, 4-й байты	128.0.0. — 191.255.0.0	16 384	65 535
C	110	2-, 3-, 4-й байты	192.0.0.0 — 223.255.255.0	2 097 152	254
D	1110	—	224.0.0.0 — 247.255.255.255	—	—

Двоичная форма	1000 0000	0000 1010	0000 0010	0001 1110
Шестнадцатеричная форма	8 0.	0 A.	0 2.	1 D
Десятичная форма	128.	10.	2.	30

Рис. 4.7. Форматы записи IP-адреса

Достоинство классовой адресации состоит в том, что кроме IP-адреса узла не требуется никакой дополнительной информации. Однако этот способ может обеспечить только указанное в табл. 4.2 число сетей и узлов, т.е. он не позволяет эффективно использовать небольшое по современным меркам 32-разрядное адресное пространство из-за фиксированного его разделения на адреса сетей и узлов. Бесполезная потеря адресов потребовала разработки способов *бесклассовой адресации* [7].

Символьная адресация. Используемая на сетевом и транспортном уровнях адресация IP-пакетов является неудобной для конечного пользователя, поскольку нужно помнить последовательность из четырех чисел. Для работы на высших уровнях принята *символьная адресация*, построенная по иерархическому доменному принципу. Символьные адреса обычно несут некую смысловую нагрузку и их гораздо легче запоминать. Например, для обращения к web-узлу компании *Xerox* следует ввести символическое имя `www.xerox.com`, после чего браузер (Browser — программа просмотра, навигатор) автоматически преобразует имя хоста в IP-адрес 208.134.240.50.

В стеке TCP/IP применяется доменная система имен, которая имеет иерархическую древовидную структуру с использованием в имени произвольного количества составных частей. Дерево начинается с корня, выше располагаются домены первого

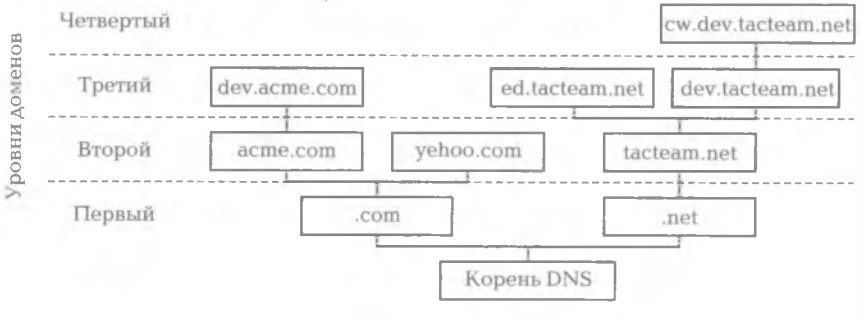


Рис. 4.8. Древовидная структура доменной системы имен

уровня (.com, .net), далее домены второго уровня и т.д. (рис. 4.8). При этом в состав имен каждого следующего уровня входит полное имя предыдущего. Составные части доменного имени отделяются друг от друга точкой. При записи доменного имени сначала указывается старшая составляющая самого высокого уровня, затем последовательно составляющие более низкого уровня. Запись начинается с самой младшей составляющей, а заканчивается самой старшей. *Домен* (Domain) *имен* образуют имена, у которых совпадают одна или несколько старших составных частей. Например, ed.**tacteam.net** и dev.**tacteam.net** образуют домен. Домены верхнего уровня разделяются:

- *по региональному признаку*, например, ru — Россия, ua — Украина, usa — США, uk — Великобритания и др.;
- *типу организаций*, например, com — коммерческие организации, org — некоммерческие организации, edu — школы, колледжи и вузы, net — организации, поддерживающие сети, и др.

Для адресации узла (компьютера, маршрутизатора) сети TPC/IP необходимо от символьного имени перейти к IP-адресу. Для этого используется централизованная *служба имен доменов* (Domain Name System — DNS), а также протокол разрешения адресов (Address Resolution Protocol — ARP) [7].

4.4. ПРИНЦИПЫ, АЛГОРИТМЫ И ПРОТОКОЛЫ МАРШРУТИЗАЦИИ

Принципы маршрутизации. Под *маршрутизацией* понимают совокупность средств, обеспечивающих оптимальный путь (маршрут) следования пакета данных из одного узла составной сети в любой другой. Объединение пакетных подсетей, работающих по своим собственным правилам, в составную сеть осуществляется через *шлюзы*. Каждый шлюз способен принять пакет из одной сети и доставить его по указанному адресу в другую сеть. В результате трансляции пакетов через последовательность шлюзов обеспечивается сквозная маршрутизация пакетов по всей сети.

Механизм доставки пакетов. Рассмотрим механизм, реализуемый IP-протоколом межсетевого обмена в сетях с коммутацией пакетов. Любое сообщение, отправляемое по сети, разделяется на фрагменты, которые снабжаются адресами отправителя и получателя, а также номером каждого пакета, входящего в со-

став сообщения. Такая система адресации позволяет каждому шлюзу выбирать маршрут, основываясь на текущей информации о состоянии сети. При этом каждый пакет может пройти от отправителя к получателю по своему собственному маршруту. Так как каждый пакет несет в себе информацию о своем месте в сообщении, последовательность доставки пакетов в оконечный узел не играет роли. Получатель расставит все фрагменты прибывшего пакета согласно их порядковым номерам.

Реализация механизма доставки. Одним из требований, предъявляемым к составным сетям, является обеспечение ее живучести и надежной доставки сообщений. Этим требованиям, как указано ранее, не удовлетворяют устройства канального уровня (коммутаторы и мосты), соединяющие два сегмента сети и локализующие трафик в пределах каждого из них. Для сетей со сложной конфигурацией были разработаны специальные средства — *маршрутизаторы* (Routers). При объединении разнородных сетей с различными сетевыми протоколами они обеспечивают эффективное разделение трафика с использованием альтернативных путей между узлами сети.

Маршрутизаторы отличаются количеством и типами своих портов. Они могут быть использованы: для эффективного управления трафиком в локальной сети Ethernet при наличии большого числа сегментов; для соединения сети типа Ethernet с сетями другого типа, например Token Ring, FDDI; для обеспечения выходов ЛС на глобальную сеть и других целей.

Маршрутизаторы управляют трафиком на основе протокола сетевого (более высокого по сравнению с коммутаторами) уровня, когда нужно решать задачу максимально эффективной и быстрой доставки отправленного пакета по назначению в сетях со сложной топологией и большим числом узлов при наличии избыточных путей.

Классификация алгоритмов маршрутизации. Под *алгоритмом маршрутизации* обычно понимают последовательность действий выбора наилучшего для заданного критерия маршрута источник — узел назначения при пересылке пакета.

Рассмотрим некоторые классификационные признаки алгоритмов маршрутизации, которые отражают их свойства и особенности.

По степени обновляемости маршрутов выделяют статические и динамические алгоритмы маршрутизации.

Статические алгоритмы маршрутизации основаны на ручном составлении таблиц маршрутизации администратором сети до на-

чала маршрутизации. Заданные маршруты сохраняются до тех пор, пока администратор сети не изменит их. Алгоритмы применяются в только небольших сетях с простой топологией связей.

В *динамических, или адаптивных, алгоритмах маршрутизации* таблицы маршрутизации, а следовательно, и сами маршруты постоянно обновляются в соответствии с меняющейся топологией сети.

По количеству используемых маршрутов различают *одномаршрутные* и *многомаршрутные* алгоритмы. Многомаршрутные алгоритмы делают возможной мультиплексную передачу трафика по многочисленным линиям. Пакет пересылается по маршруту, обладающему наивысшим приоритетом. Этот маршрут обычно является основным, а остальные — резервными.

По иерархии систем маршрутизации можно выделить алгоритмы одно- и двухуровневых систем. В *одноуровневой системе* все маршрутизаторы равноправны по отношению друг к другу. В *двухуровневой системе* выделяют базовые (Backbone) и небазовые маршрутизаторы. Сеть разбивают на отдельные домены, связь между которыми могут поддерживать только базовые маршрутизаторы. Небазовые маршрутизаторы могут обмениваться сообщениями с базовыми маршрутизаторами лишь внутри своего домена, поэтому их алгоритмы маршрутизации гораздо проще.

По месту расположения средства выбора маршрута различают алгоритмы с расположением средства в *маршрутизаторе* и в *оконечном узле*. Расположение средств в оконечном узле более предпочтительно, так как позволяет сразу выбрать полный и, как правило, наилучший маршрут пакета, однако требует определенного времени для поиска трафика.

Показатели алгоритмов. Для сравнительной оценки алгоритмов маршрутизации (и самих маршрутов) используются показатели, называемыми *метриками*. Метрики позволяют получить количественную оценку оптимальности того или иного маршрута, т.е. выявить предпочтительность одного маршрута по сравнению с другими. Наиболее распространенными метриками являются:

- *длина маршрута*, которая в большинстве случае оценивается количеством маршрутизаторов, через которые продвигался пакет к узлу назначения. Каждый такой маршрутизатор-ретранслятор называется *хопом* (от hop — прыжок, скачок);
- *задержка* маршрутизации, под которой обычно понимают интервал времени, необходимый для пересылки пакета от источника до узла назначения через составную сеть. Задержка зави-

сит от многих факторов (от полосы пропускания промежуточных каналов сети, от очереди в порт каждого маршрутизатора на пути передвижения пакета, от перегруженности сети на всех промежуточных каналах сети, от расстояния, на которое необходимо переместить пакет) и поэтому является наиболее общим и полезным показателем;

- *надежность*, характеризующая степень отказоустойчивости канала связи (маршрута). Единицей измерения может служить число ошибок на число переданных битов;
- *полоса пропускания*, характеризующая пропускную способность канала связи (маршрута), например 64 Кбайт/с.

Для оценки эффективности сложные алгоритмы маршрутизации при выборе маршрута может быть использован комбинированный (гибридный) показатель, включающий в себя несколько показателей (метрик) с разными весовыми коэффициентами.

Протоколы маршрутизации. В сетях со сложной топологией и большим количеством альтернативных маршрутов протоколы маршрутизации позволяют автоматизировать построение таблиц маршрутизации и отыскивать новые маршруты при отказах или появлении новых линий связи и маршрутизаторов. Различают два вида протоколов: внутренние и внешние. *Внутренние протоколы* применяют только в пределах определенной автономной системы, к которым обычно относят внутренние сети компаний. Их называют протоколами внутреннего шлюза. *Внешние протоколы* предназначены для переноса маршрутной информации между автономными системами, связанными через Internet.

В качестве первого протокола внутреннего шлюза в Internet использовался протокол дистанционно-векторной маршрутизации RIP (Routing Information Protocol — протокол маршрутной информации), который успешно работал в небольших сетях с числом промежуточных маршрутизаторов не более 15. Преемником RIP с 1990 г. стал протокол маршрутизации OSPF (Open Shortest Path First), который поддерживается многочисленными производителями маршрутизаторов и стал главным протоколом внутреннего шлюза [12].

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. В чем состоит смысл следующих терминов: «технологическая пауза», «межпакетый интервал», «*jam*-последовательность», «коэффициент пульсаций», «концевик», «дейтаграмма», «вир-

туальный канал», «узел сети», «широковещательный адрес», «маршрутизация», «метрика», «хоп»?

2. Какие основные методы доступа к сети вам известны? Приведите их особенности и дайте сравнительную оценку.
3. Как осуществляется доступ к сети и организуется передача сообщений по методу CSMA/CD?
4. Как возникают, обнаруживаются и обрабатываются коллизии?
5. В чем заключается принцип организации обмена в сети с коммутацией каналов?
6. Какова сущность принципа организации обмена в сети с коммутацией пакетов?
7. Для чего предназначена и в чем состоит адресация узлов сети?
8. По каким основным признакам классифицируют адреса?
9. Какие подходы используют при адресации?
10. В чем состоит суть и какие особенности имеют MAC- и IP-адресация?
11. Что такое маршрутизация и какие основные средства используются для ее реализации?
12. В чем состоит механизм доставки и как он осуществляется?
13. Какова классификация алгоритмов маршрутизации?
14. Какие показатели используются для алгоритмов маршрутизации?
15. В чем состоят особенности внутренних и внешних протоколов маршрутизации?

Глава 5

СЕТЕВОЕ ОБОРУДОВАНИЕ

5.1. ЛИНИИ СВЯЗИ И ИХ ХАРАКТЕРИСТИКИ

В общем случае *линию связи* (Line) можно представить как совокупность аппаратных средств, обеспечивающих передачу информации между двумя абонентами и включающих в себя:

- *оконечное оборудование данных* (Data Terminal Equipment — DTE), представляющее собой устройство (например, компьютер), передающее и (или) принимающее данные;
- *аппаратуру передачи данных* (Data Communications Equipment — DCE), т. е. пограничное (интерфейсное) оборудование для обеспечения совместимости (согласования, сопряжения) передаваемых двоичных данных с каналом связи. Аппаратуру передачи данных традиционно включают в состав линии связи;
- *физическую среду*, по которой передаются данные;
- *промежуточную аппаратуру*, используемую для усиления, мультиплексирования, выбора маршрута, демультиплексирования в процессе передачи данных от одного абонента к другому.

Базовый материал о сетевых устройствах представлен в подразд. 1.4, поэтому в этой главе основное внимание будет уделено линиям связи, конкретной реализации некоторых коммуникационных устройств и их использованию в компьютерных сетях.

В зависимости от конкретных условий часто используют такие синонимы термина «линия связи», как звено (Link), канал связи (Channel), составной канал (Circuit) или просто ограничиваются термином «среда передачи данных».

Среды передачи данных. Главное отличие любой телекоммуникационной системы от других систем состоит в том, что основной составной ее частью является физическая среда (Medium), или среда передачи данных, по которой передаются сигналы. Различают проводную и беспроводную среды (рис. 5.1).

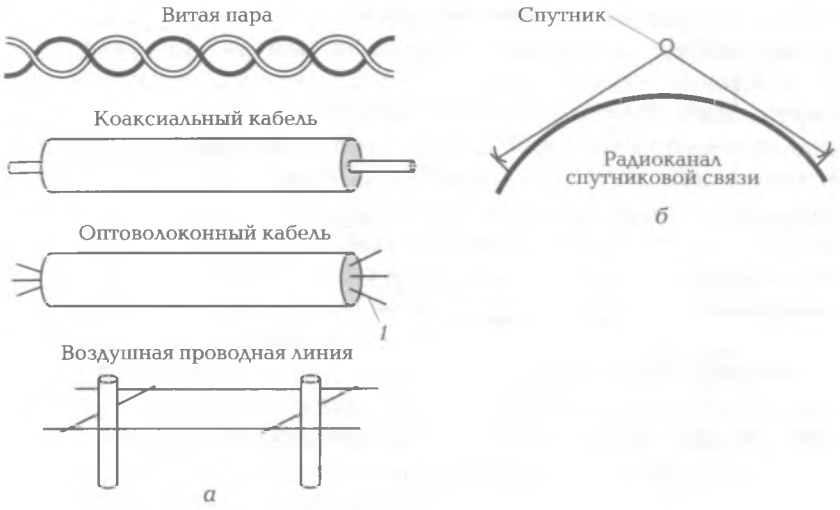


Рис. 5.1. Среды передачи данных:
а — проводная среда: *1* — оптоволокно; *б* — беспроводная среда

В проводной среде (см. рис. 5.1, *а*) для передачи сигналов используют два вида линий связи: кабельные и воздушные.

Кабельные линии составляются из отдельных отрезков кабеля, оснащенного разъемами для быстрого соединения с сетевым оборудованием. Кабель состоит из проводников, заключенных в слои изоляции. Находят применение три основных типа кабеля: кабели на основе скрученных пар медных проводов (витая пара), коаксиальные кабели с медной жилой и оптоволоконные кабели.

Воздушные линии представляют собой висящие в воздухе медные или алюминиевые провода, проложенные между столбами. По воздушным линиям передаются телефонные и телеграфные сигналы, но при отсутствии других возможностей они используются также для передачи компьютерных данных. Из-за низких скоростных показателей и помехозащищенности проводные линии связи повсеместно заменяются кабельными.

Беспроводная среда (см. рис. 5.1, *б*) представляет собой свободное пространство (земная атмосфера и космос), позволяющее с помощью передатчиков и приемников радиосигналов организовать бесчисленное множество линий (каналов) связи для передачи сообщений с использованием электромагнитных колебаний в широком диапазоне частот. Электромагнитный спектр приведен на рис. 5.2. Там же показано его практическое использование.

Рис. 5.2. Электромагнитный спектр и его использование

Характеристики линий связи. К характеристикам линий связи относят: частотные характеристики, пропускную способность, помехоустойчивость и волновое сопротивление.

Частотные характеристики. В подразд. 3.2 показано, что для передачи импульсных (цифровых) сигналов с минимальными искажениями необходима определенная полоса частот. Вносимые искажения можно оценить по амплитудно-частотной (АЧХ) и фазочастотной (ФЧХ) характеристикам. Постоянство амплитуды и линейная зависимость фазы от частоты в пределах от 0 до ∞ свидетельствуют об отсутствии искажений. В этом идеальном случае передаваемые по линии импульсы сохраняют свою форму и получают только постоянный временной сдвиг (запаздывание). Реальная АЧХ (рис. 5.3) позволяет определить *полосу пропускания* (Band-

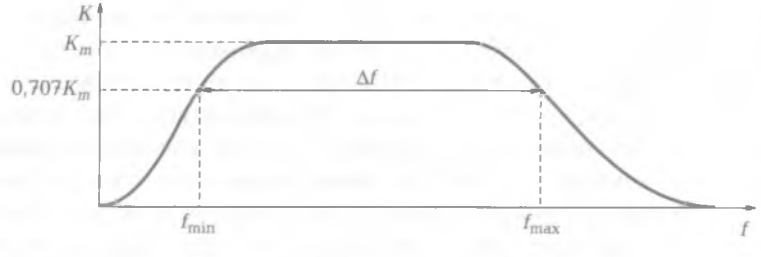


Рис. 5.3. Амплитудно-частотная характеристика и полоса пропускания

width) линии, или канала, связи. Под полосой пропускания понимают диапазон частот, в котором мощность гармонических колебаний уменьшается не более чем в два раза по отношению к мощности на средних частотах, что соответствует уменьшению амплитуды напряжения (тока) в $\sqrt{2}$ раз. Для количественной оценки полосы пропускания можно использовать АЧХ в виде зависимости коэффициента передачи напряжения от частоты $K(f)$, которая приведена на рис. 5.3. Полоса пропускания $\Delta f = f_{min} - f_{max}$, где f_{min}, f_{max} — граничные частоты диапазона, в котором коэффициент передачи по напряжению не менее 0,707 K_m, где K_m — коэффициент передачи на средних частотах.

Затухание (Attenuation) кабельной линии связи определяется как относительное уменьшение амплитуды напряжения или мощности сигнала на передаваемой частоте, т.е. представляет собой точку на АЧХ. Затухание обычно измеряется в децибелах (дБ, decibel — dB) и вычисляется по формуле

$$K_P = 20\log_{10}U_{вых}/U_{вх} \text{ или } K_P = 10\log_{10}P_{вых}/P_{вх},$$

где $U_{вых}$, $U_{вх}$, $P_{вых}$, $P_{вх}$ — напряжение и мощность сигнала на выходе и входе линии соответственно.

Пропускная способность (Throughput). Этот показатель характеризует скоростные свойства линии (канала) связи, которые зависят не только от характеристик самой линии, но от способа передачи данных. В связи с этим нельзя говорить о пропускной способности линии связи, если для нее не задан протокол физического уровня. Для *цифровых* линий связи протокол физического уровня определен и задает битовую скорость передачи данных в битах в секунду (бит/с), поскольку данные передаются в последовательном коде *побитно*. Поэтому пропускная способность линии связи традиционно оценивается такими единицами, как килобит в секунду (Кбит/с), мегабит в секунду (Мбит/с), гигабит в секунду (Гбит/с) и т.д.

Интуитивно понятно, что пропускная способность каким-то образом должна быть связана с полосой пропускания, поскольку фронты импульсов прямоугольной формы формируются высокочастотными составляющими спектра. Если граничная частота f_{max} полосы пропускания линии связи меньше частот передаваемого сигнала, то последние вообще не будут приняты на другом ее конце. В теории связи известны соотношения, позволяющие по заданной скорости передачи данных оценить пропускную способность линии.

Помехоустойчивость. Под помехоустойчивостью линии связи понимают ее способность противостоять влиянию как вну-

тренних, так и внешних помех, создаваемых во внешней среде или на внутренних проводниках самого кабеля. Наименее устойчивыми к помехам являются радиолинии, большей устойчивостью обладают кабельные линии и самой высокой — волоконно-оптические линии, малочувствительные к внешнему электромагнитному излучению.

Волновое сопротивление. Кабель можно представить электрической цепью с распределенными параметрами (емкостью, индуктивностью и сопротивлением), по которой распространяется сигнал в виде электромагнитной волны. В каждом сечении кабеля электромагнитная волна встречает сопротивление. Так как кабель является однородной средой, его сопротивление в каждом сечении имеет постоянное значение и называется *волновым сопротивлением*. Таким образом, волновое сопротивление — это *кажущееся* сопротивление, которое испытывает электромагнитная волна при распространении вдоль кабеля. Его значение определяется геометрией проводников кабеля и диэлектрическими свойствами материала изоляции. Рассмотрим особенности процессов распространения сигнала, представив кабель отрезком однородной линии (рис. 5.4). Посланный передатчиком одиночный импульс распространяется вдоль линии с определенной для данного кабеля скоростью, встречая в каждом ее сечении волновое сопротивление ρ. Если сопротивление включенного на концах линии приемника, $R = \rho$ (см. рис. 5.4, *а*), то импульс поглотится приемником, т.е. энергия импульса полностью выделится на сопротивлении R. В том случае, когда сопротивление на концах линии отличается от ρ, среда становится неоднородной, поэтому импульс по достижении конца линии, отразившись от неоднородной среды, начнет распространяться в противоположном направлении. В случае короткого замыкания линии ($R = 0$) импульс при отражении изменяет полярность (см. рис. 5.4, *б*), при разомкнутой линии ($R = \infty$) полярность импульса сохраняется (см. рис. 5.4, *в*).

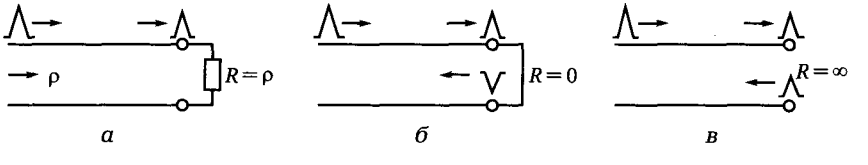


Рис. 5.4. Прохождение сигнала по линии связи:
а — для $R = \rho$; *б* — $R = 0$; *в* — $R = \infty$

5.2. КАБЕЛЬНЫЕ СРЕДЫ ПЕРЕДАЧИ ДАННЫХ

Кабели на витой паре (Twisted Pair Cable — TPC). Витая пара представляет собой два скрученных изолированных медных провода диаметром порядка 1 мм, помещенных в защитную оболочку, и обладает следующими особенностями:

1) при скручивании проводники идут под некоторым углом друг к другу, что снижает емкостную и индуктивную связь между ними. Благодаря этому уменьшаются *перекрестные помехи*. Их уровень тем меньше, чем мельче шаг скрутки. Кроме того, при прохождении сигнала уменьшаются внешние излучения;

2) при включении по дифференциальной схеме снижается чувствительность к наводкам от внешних полей благодаря сохранению симметрии;

3) для витой пары увеличивается погонное затухание кабеля и время распространения сигнала. Однако витая пара способна передавать сигнал без ослабления мощности на расстояние, составляющее несколько километров.

Различают витые пары двух типов: неэкранированные и экранированные.

Неэкранированные витые пары (Unshielded Twisted Pair — UTP) используются в системах телефонной связи и в большинстве сетей Ethernet. Их популярность обусловлена такими факторами, как низкая стоимость кабеля, наличие стандартных разъемов, гибкость и легкость установки, возможность использования топологии звезды, обладающей многими достоинствами.

В *экранированных витых парах* (Shielded Twisted Pair — STP) экран выполнен из плетеных медных жилок или фольги и заключен в защитную изоляционную оболочку, что уменьшает влияние внешних электромагнитных помех. Однако он увеличивает стоимость кабеля и затухание сигналов.

Витые пары благодаря довольно высокой пропускной способности и небольшой цене используются в качестве среды передачи во всех современных компьютерных сетевых технологиях, а также в аналоговой и цифровой телефонии. В основе построения сетей на витой паре лежит звездообразная физическая топология. Наиболее широкое распространение получили неэкранированные кабели в противоположность громоздким дорогим экранированным кабелям из витых пар.

Коаксиальный кабель (Coaxial Cable). Электрическими проводниками кабеля являются центральная жила и экранирующая

оплетка. При этом *частотные свойства кабеля* определяют диаметр жилы и внутренний диаметр оплетки, а также диэлектрическую проницаемость изоляции между ними, а *затухание* сигнала в кабеле и его *волновое сопротивление* зависят от материала, сечения проводников и изоляции. Коаксиальный кабель практически не создает электромагнитных помех и малочувствителен к внешним помехам. Конструкция кабеля асимметрична, поэтому он используется только при асимметричной передаче сигналов. В телекоммуникациях применяется *толстый* желтый кабель Ethernet, имеющий посеребренную центральную жилу толщиной 2 мм и двойной слой экранирующей оплетки.

Главный недостаток коаксиального кабеля — ограниченная пропускная способность. Наибольшее ее значение, достигнутое в локальных сетях Ethernet 10Base2 и 10Base5, составляет 10 Мбит/с. Коаксиальные кабели не включаются в современные стандарты и не рекомендуются для применения при установке новых сетей.

Оптоволоконные средства передачи данных. Главная особенность оптоволоконных систем передачи данных состоит в том, что физической средой передачи данных служит сверхтонкое стеклянное волокно, называемое *оптическим волокном*, а аналогом сообщения являются *световые сигналы*, при этом наличие светового импульса соответствует логической единице, а отсутствие — логическому нулю.

К одному концу оптического волокна подключено устройство, преобразующее электрические сигналы в световые импульсы, а к другому — приемник, который выполняет обратное преобразование светового потока разной интенсивности в электрические сигналы.

Принцип передачи светового луча по оптоволокну базируется на использовании эффекта преломления (рефракции) при его прохождении через границу двух разнородных сред, например стекло — воздух. Как показано на рис. 5.5, луч света падает под углом α_1, а выходит под углом β_1. Соотношение углов падения α и отражения β зависит от свойств смежных сред. Если угол падения луча света превосходит некоторую критическую величину, то луч полностью отражается обратно в стекло, не попадая в воздух (случай α_3, β_3 на рис. 5.5).

Распространение света в волокне показано на рис. 5.6, из которого видно, что лучи света должны входить в оптоволокно относительно его оси под углом θ, не превышающем некоторого критического значения ($\theta < 18°$), т.е. должны попадать в воображаемый входной конус. В этом случае они окажутся запертыми внутри во-

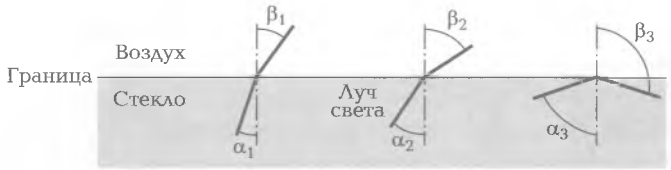


Рис. 5.5. Эффект преломления и отражения

локна и после многократного отражения могут быть переданы на большое расстояние. Каждый передаваемый луч ассоциируется с *модой*. Оптическое волокно, обладающее свойством передавать сразу несколько лучей, называется *многомодовым*. Если уменьшить диаметр волокна до нескольких длин световых волн, то свет начинает распространяться по прямой линии, без отражений от стенок волокна, т.е. остается только один луч. Такое волокно называется *одномодовым*.

В качестве источников света используются светоизлучающие диоды (Light Emitting Diode — LED) и полупроводниковые лазеры, или лазерные диоды, обладающие лучшими характеристиками. Приемниками световых сигналов служат фотодиоды, которые преобразуют световые импульсы в электрические. Время срабатывания фотодиода составляет порядок 1 нс, поэтому скорость передачи данных не превышает 1 Гбит/с.

В системах связи используются три диапазона длин волн (0,85, 1,30 и 1,55 мкм) с полосой пропускания от 25000 до 30000 ГГц каждый. Диапазон 0,85 мкм обладает более высоким ослаблением, однако его достоинством является то, что для этой длины волны лазеры и электронные компоненты изготовляются из одного и того же материала (арсенида галлия). Ослабление света в диапазоне 1,30 и 1,55 мкм составляет менее 5 % потерь на километр.

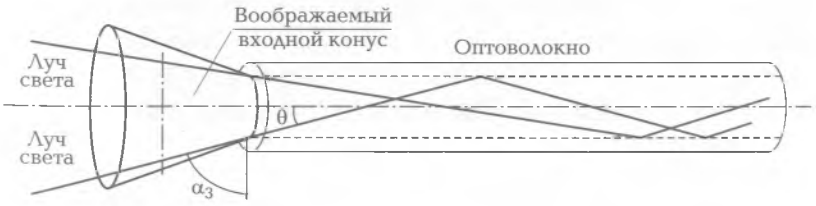


Рис. 5.6. Ввод света в оптоволокно

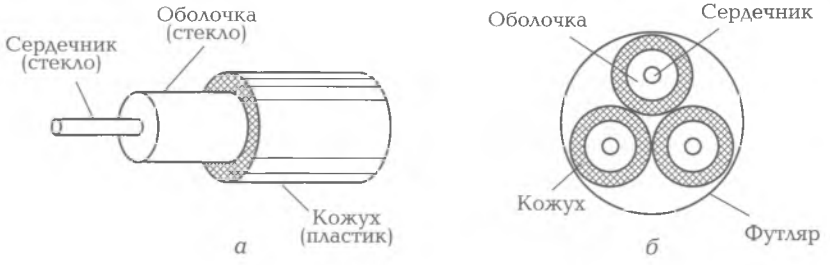


Рис. 5.7. Оптоволокно (*а*) и поперечное сечение трехжильного кабеля (*б*)

Оптоволоконный кабель состоит из отдельных волокон, каждое из которых содержит (рис. 5.7, *а*);

- выполненный из стекла *сердечник* для передачи световых сигналов. Диаметр сердечника составляет менее 50 мкм (тоньше человеческого волоса);
- стеклянную *оболочку* с более низким коэффициентом преломления, что предотвращает выход света за пределы сердечника;
- пластиковый кожух, выполняющий защитные функции.

На рис. 5.7, *б* показан трехжильный кабель.

В зависимости от распределения показателя преломления и диаметра сердечника различают кабели с много- и одномодовым волокном.

В многомодовом кабеле (Multi Mode Fiber — MMF) используются внутренние сердечники с *большим диаметром* (порядка 50 мкм), которые легче изготовить технологически. Они имеют *ступенчатое* и *градиентное* (плавное) изменение коэффициента преломления (рис. 5.8, *а*, *б*). В сердечнике одновременно существует несколько световых лучей, отражающихся от оболочки под разными углами. Возникающая при этом интерференция приводит к искажениям выходных импульсов (уменьшается амплитуда, изменяется форма). Кабель с градиентным профилем показателя преломления обеспечивает меньшие искажения выходных импульсов (см. рис. 5.8, *б*). Излучателями светового потока для многомодовых кабелей служат светодиоды. Многомодовые кабели используются для передачи данных на небольшие расстояния (до 300...2 000 м) на скоростях не более 1 Гбит/с.

Одномодовый кабель (Single Mode Fiber — SMF) обеспечивает более качественную передачу сигналов (рис. 5.8, *в*). Изготовление сверхтонких качественных волокон диаметром до 5...10 мкм представляет собой сложный технологический процесс,

значительно удорожающий стоимость одномодового кабеля. Кроме того, в волокно такого малого диаметра достаточно сложно направить пучок света, не потеряв при этом значительную часть его энергии, поэтому для одномодовых кабелей применяются только лазерные диоды, имеющие весьма узкую диаграмму направленности излучения. Одномодовые кабели используются для передачи данных на расстояния до нескольких десятков и даже сотен километров (дальняя связь) со сверхвысокими скоростями (от десятков гигабит в секунду до нескольких терабит в секунду).

Соединение отдельных отрезков кабеля осуществляется тремя способами:

- *сплавлением*, обеспечивающим минимальные потери силы света;
- *механическим сращиванием с использованием специальной муфты*. Улучшение прохождения света достигается выравниванием концов кабеля. Потери силы света составляют около 10 %;

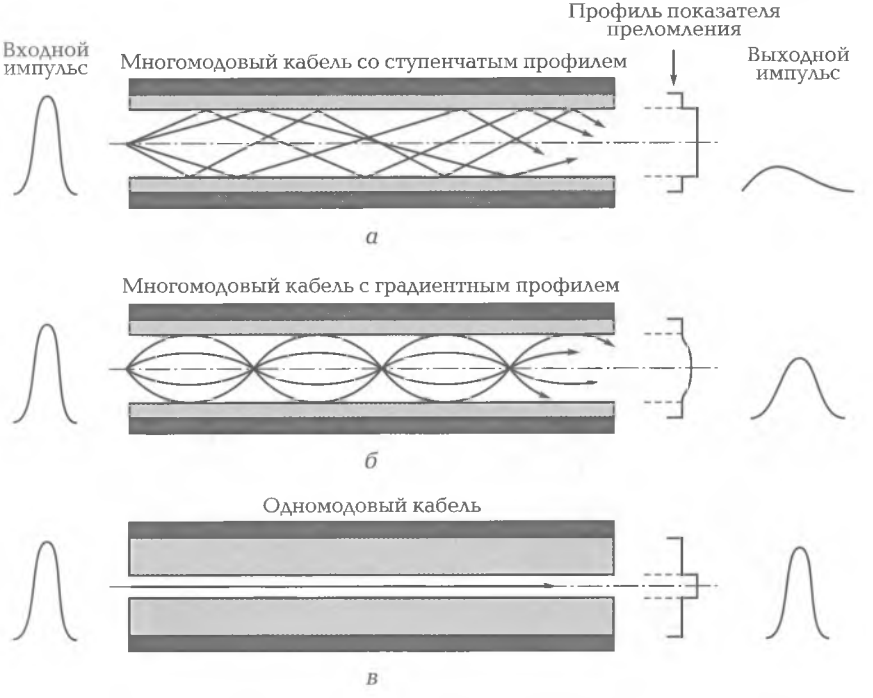


Рис. 5.8. Распространение волн в многомодовом (*а*, *б*) и одномодовом кабелях (*в*)

- *соединением с помощью специального разъема* и *оптической розетки*. Потери силы света составляют 10...20 %, однако можно легко изменять конфигурацию системы.

При построении локальных оптоволоконных сетей используется соединение оптических кабелей в кольцо, которое можно рассматривать как совокупность соединений *точка—точка* (рис. 5.9, *а*). Интерфейс каждого компьютера представляет собой Т-образное соединение, которое позволяет принимать и передавать световые сообщения самому компьютеру или пропускать принятый свет дальше по кольцу. Применяются два типа интерфейсов: пассивный и активный.

Пассивный интерфейс состоит из двух ответвлений, вплавленных в основной кабель. С одной стороны ответвления устанавливается принимающий фотодиод, с другой — светодиод (или лазерный диод) для передачи. Достоинство интерфейса — высокая надежность, поскольку выход из строя диодов не приводит к разрыву кольца, отключенным от сети окажется только один компьютер.

Активный интерфейс с повторителем (рис. 5.9, *б*) представляет собой набор их трех компонентов (приемника, регенератора и передатчика), включенных между двумя отрезками оптоволокна (см. рис. 5.9, *а*). Принимаемый световой импульс преобразуется (фотодиодом) в электрический сигнал, усиливается при необходимости в регенераторе сигнала до требуемого уровня и снова пересылает-

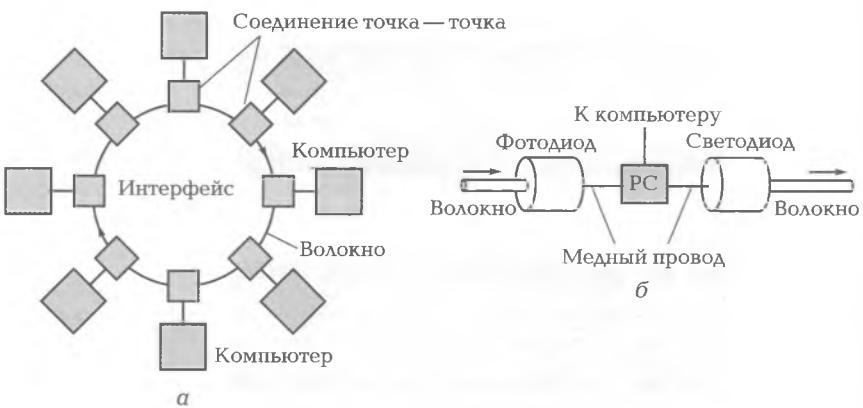


Рис. 5.9. Оптоволоконное кольцо (*а*) с регенераторами сигналов (*б*):
PC — регенератор сигнала; фотодиод — оптический приемник; светодиод — оптический передатчик; ⟶ — направление распространения света

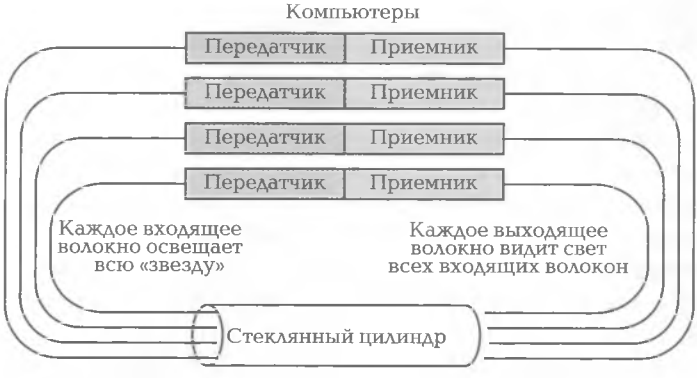


Рис. 5.10. Топология пассивной звезды

ся светодиодом в виде светового пучка. Компьютер через медный провод соединен с регенератором сигнала. Достоинством активного интерфейса является возможность значительного увеличения протяженности кольца, поскольку сигнал регенерируется каждым интерфейсом, а недостатком — разрыв кольца и прекращение работы сети при поломке повторителя.

Пример локальной сети с топологией *пассивной звезды*, в которой используется стеклянный цилиндр, приведен на рис. 5.10. При этом с одним торцом цилиндра соединены входные оптоволокна, идущие от передатчиков, а с другим — выходные оптоволокна, идущие к приемникам.

Свет, поступающий по оптоволокну от любого передатчика, видят сразу все приемники. Поскольку энергия светового пучка разделяется в цилиндре между выходными оптоволокнами, число узлов (компьютеров) в подобной сети ограничивается чувствительностью фотодиодов. В этой сети можно организовать широковещание.

Наряду с такими достоинствами оптоволоконных кабелей, как более высокие скорость передачи и пропускная способность, малое затухание, хорошая защищенность от внешних электромагнитных помех и возмущений, а также от коррозии, низкие затраты на прокладку кабеля, им присущи следующие недостатки: оптическая передача данных является строго однонаправленной, поэтому для двухсторонней связи требуются либо два кабеля, либо две частотные полосы в одном кабеле; кабель хрупкий и ломается в местах сильных изгибов; высока стоимость интерфейсных средств.

5.3. БЕСПРОВОДНАЯ СРЕДА

Развитие телекоммуникационных сетей идет в направлении внедрения и дальнейшего расширения беспроводной связи, которая позволяет объединять в сети мобильные устройства, поэтому рассмотрим наиболее важные вопросы использования беспроводной среды в качестве коммуникационного канала.

Свободное пространство как среда передачи данных. Следует выделить два главных средства для беспроводной передачи сообщений:

1) *гармонические электромагнитные колебания*, используемые в качестве несущих колебаний, т. е. непосредственного транспортного средства для доставки информационного сигнала, вложенного в несущее колебание. Диапазон волн используемых электромагнитных колебаний простирается от 10^8 до 10^{-7} м;

2) *свободное пространство*, которое служит естественной средой, позволяющей с максимальной скоростью и минимальным затуханием в широком диапазоне частот пересылать электромагнитные колебания из одной точки пространства в другую.

Формируемые в радиопередающем устройстве электрические колебания преобразуются антенной в электромагнитные колебания, которые после изучения распространяются в свободном пространстве со скоростью света. На распространение радиоволн сильное влияние оказывают *ионосфера* и *тропосфера* (рис. 5.11). *Метровые* и более короткие волны (колебания с частотой выше 30... 40 МГц) пронизывают ионосферу и проникают в космическое пространство. В диапазоне *коротких волн* (10... 100 м) ионосфера отражает радиоизлучения. *Гектометровые волны* (100... 1 000 м) поглощаются ионосферой, что приводит к заметному затуханию и ослаблению результирующей мощности сигнала. Причем, чем ниже частота радиосигнала, тем больше поглощение, поэтому радиоволны диапазона *средних* и *длинных волн* практически от ионосферы не отражаются, а затухают в ней. С увеличением длины волны начинают проявляться эффекты искривления траектории (рефракция) радиоволн и огибания встречающихся на пути препятствий (дифракция). Наоборот, *очень короткие волны* (сантиметрового диапазона) распространяются в пределах прямой видимости (см. рис. 5.11, $A \rightarrow B$). Поверхность Земли также оказывает существенное влияние на распространение радиоволн.

Рассмотрим два способа организации радиосвязи: через базовую станцию и с помощью спутников.

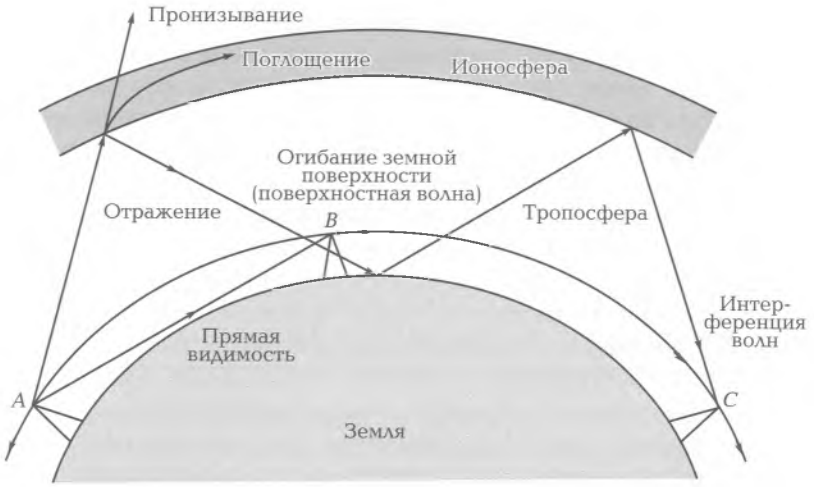


Рис. 5.11. Распространение радиоволн

Связь через базовую станцию (Base Station — BS). Базовая станция является *точкой доступа* (Access Point — AP) для ее пользователей. Точка доступа включает в себя оборудование передачи данных, необходимое для образования линии связи, и выполняет функции коммутатора сетей. Базовую станцию обслуживает оператор связи. Существует два способа доступа к базовой станции: фиксированный и мобильный.

При *фиксированном доступе* в микроволновом диапазоне используется высокая башня для прямой видимости с антеннами приемных устройств, расположенными на крышах зданий. На башне устанавливается несколько направленных антенн, обеспечивающих связь в пределах полного сектора в 360°. Информация от одного пользователя (абонента) по линии доступа поступает на базовую станцию, которая транзитом передает ее другому пользователю. Базовая станция обычно соединена с проводной частью сети, обеспечивая взаимодействие с пользователями других базовых станций или пользователями проводных сетей.

Для *мобильного доступа* в большинстве случаев используется сотовая организация сети. Каждая *сота* (ячейка) представляет собой небольшую по площади территорию, которая обслуживается одной базовой станцией при использовании выделенного для нее

набора частот. Разбиение области охвата всей сети на небольшие соты осуществляется по принципу *многократного* использования частоты. Для пояснения его сути на рис. 5.12 показано два варианта организации сот при наличии трех и семи наборов частот, выделенных для всей сети. Соты имеют форму окружности, площадь которой определяет зону действия передатчика. Цифра в центре круга соответствует порядковому номеру набора частот. Как видно из рисунков, ни одна из двух соседних сот не использует один и тот же набор частот. Кроме того, чем больше выделено наборов частот, тем дальше разнесены соты, использующие одинаковые наборы. Принцип многократного использования частоты позволяет экономно расходовать выделенный частотный диапазон без взаимных мешающих влияний базовых станций друг на друга.

Спутниковая связь. Искусственные спутники Земли используются как ретрансляторы для организации высокоскоростных протяженных линий микроволнового диапазона. Они усиливают сигналы и преобразуют их на новую частоту, чтобы прямой и отраженный сигналы не накладывались друг на друга, а также выполняют функции узла первичной сети, телефонного коммутатора и коммутатора (маршрутизатора) компьютерной сети. Установленная на спутнике аппаратура взаимодействует как с наземными станциями, так и между собой, создавая прямые космические беспроводные каналы связи. Для спутниковой связи выделено несколько диапазонов частот.

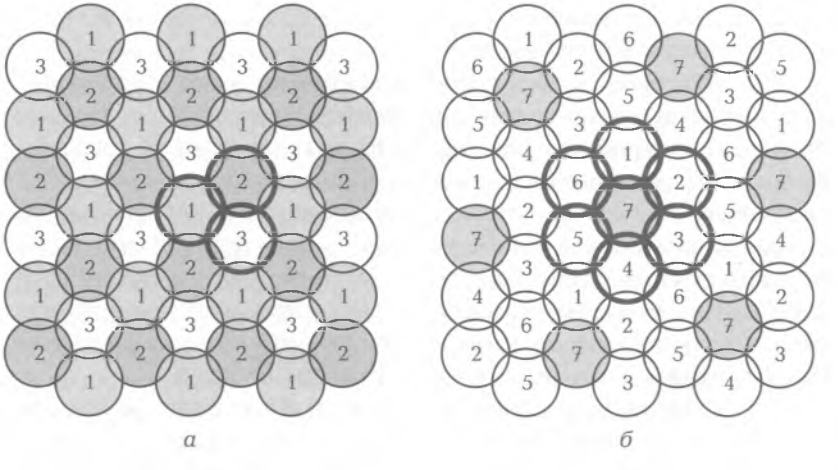


Рис. 5.12. Организация сотовой связи с использованием трех (*а*) и семи (*б*) повторяемых частот

Искусственные спутники вращаются вокруг Земли по эллиптическим орбитам. Используются три группы орбит, отличающихся высотой над Землей:

1) геостационарная (Geostationary Orbit — GEO) — 35 863 км;

2) средневысотная (Medium Earth Orbit — MEO) — 5 000... 15 000 км;

3) маловысотная (Low Earth Orbit — LEO) — 100... 1 000 км.

5.4. ИСПОЛЬЗОВАНИЕ МОСТОВ ДЛЯ ЛОГИЧЕСКОЙ СТРУКТУРИЗАЦИИ СЕТИ

Логическая структуризация сетей предназначена для сохранения и поддержки высокой производительности сети при увеличении числа узлов. Она состоит в разбиении общей среды на логические *сегменты*, которые представляют собой самостоятельные разделяемые среды с небольшим количеством узлов.

Взаимодействие между логическими сегментами можно осуществить с помощью коммутирующих устройств канального уровня — *мостов* и *коммутаторов*, которые передают кадры с одного своего порта на другой, анализируя находящийся в них адрес назначения. По функциональному назначению мост и коммутатор близки друг к другу. Основное отличие коммутатора от моста состоит в том, что коммутатор обрабатывает кадры параллельно, а мост — последовательно.

Так как логический сегмент представляет собой единую разделяемую среду, деление сети на отдельные сегменты уменьшает нагрузку на каждый вновь образованный сегмент, которая оказывается значительно меньше нагрузки исходной сети. Как следует из рис. 5.13, на котором изображены два соединенных мостом сегмента, для связи компьютеров внутри каждого сегмента используется концентратор (повторитель), а для связи компьютеров разных сегментов — мост. Теперь допустим, что вместо моста используется третий концентратор, который соединяет все компьютеры обоих сегментов. В этом случае возрастет вероятность возможных коллизий, из-за чего замедлится доступ к общей сети и производительность снизится.

Таким образом, повышение производительности достигается благодаря разделению трафика на внешний и внутренний. Производительность зависит от того, как сеть разбита на логические подсети. В общем случае деление сети на логические сегменты, или *сегментация*, повышает производительность сети (за счет раз-

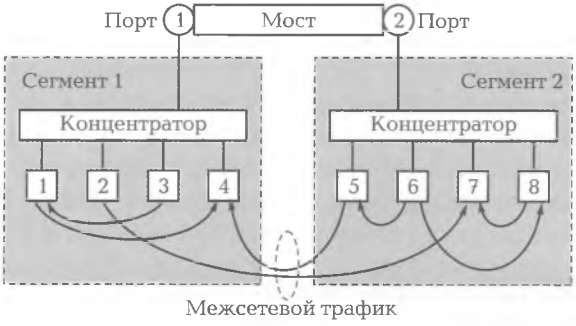


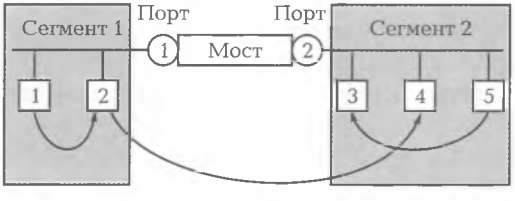
Рис. 5.13. Распределение нагрузки в сегментированной сети

грузки сегментов), обеспечивает гибкость построения сети, увеличивает степень защиты данных и облегчает управление сетью.

Для ознакомления с принципами работы мостов рассмотрим один из алгоритмов их работы.

Алгоритм прозрачного моста (Transparent Bridge). Для выявления направления передачи кадров многопортовый мост строит специальную адресную таблицу на основании пассивного наблюдения за трафиком, циркулирующим в подключенных к его портам сегментах. Прежде всего мост выявляет, нужно или нет передавать поступившие на его порт кадры данных в какой-либо другой сегмент. Для этого он анализирует их адреса, по которым определяет принадлежность этого узла тому или иному сегменту сети. По результатам анализа строится таблица адресов моста.

Рассмотрим процесс построения и использования адресной таблицы на примере простой сети (рис. 5.14, *а*), в которой мост объединяет два логических сегмента, подключенных к портам 1 и 2. При этом сегмент 1 содержит компьютеры 1, 2, а сегмент 2 — ком-



а

MAC-адрес	Порт
1	1
2	1
3	2
4	2
5	2

б

Рис. 5.14. Алгоритм прозрачного моста:
а — сеть; *б* — адресная таблица

пьютеры 3, 4, 5. Каждый порт моста по сути является оконечным узлом своего сегмента. Все поступающие на порт пакеты запоминаются в его буферной памяти, поэтому адрес порта мосту не нужен и порты мостов в отличие от других оконечных узлов (компьютеров) не имеют собственного аппаратного MAC-адреса. В этом режиме мост следит за трафиком и использует проходящие через него данные для изучения состава сети.

Пусть *в исходном состоянии* мост не располагает MAC-адресами компьютеров, подключенных к каждому из его портов. В этом случае *после начала передачи* любой кадр, поступивший в буфер одного из портов моста, транслируется на все его другие порты. Поскольку в рассматриваемом примере мост имеет два порта, кадры могут передаваться из порта 1 в порт 2, или наоборот. Если повторитель пересылает данные побитно, то мост, используя буферизацию, передает сразу полный кадр. Благодаря буферизации разрывается логика работы всех сегментов как единой разделяемой среды. В отличие от повторителя мост в процессе передачи кадра, например с сегмента 1 на сегмент 2, *снова попытается* получить доступ к сегменту 2 (новой среде) как оконечный узел.

При *трансляции* кадра мост изучает адрес его отправителя и делает соответствующую запись в своей адресной таблице, которую также называют таблицей фильтрации или маршрутизации. Например, получив на порт 1 кадр от компьютера 1, мост делает первую запись в своей адресной таблице: MAC-адрес — 1; порт — 1. После того как все компьютеры сети пошлют друг другу кадры, мост построит полную адресную таблицу сети, состоящую из пяти записей (рис. 5.14, *б*). Создание адресной таблицы называется *процессом самообучения* моста.

Мост не ждет, когда адресная таблица заполнится полностью, а сразу приступает к работе. Как только в таблице появляется первый адрес, мост пытается его использовать, проверяя совпадение с ним адресов назначения всех поступающих кадров. Кадр, посылаемый любым компьютером, всегда попадает в порт своего сегмента.

Работу моста проиллюстрируем на конкретном примере, когда компьютер 2 направляет кадр компьютеру 4, который находится в другом сегменте. В этом случае кадр поступает в буфер порта 1 и мост начинает просматривать адресную таблицу в целях выявления записи с адресом компьютера-получателя 4. При этом возможны две ситуации.

1. Мост обнаруживает запись «MAC-адрес — 4; Порт — 2». Тогда выявляется адрес отправителя (компьютера 2 — MAC-адрес 2).

Так как компьютеры 2 и 4 находятся в разных сегментах, мост выполняет операцию *продвижения* (Forwarding) кадра: сначала получает доступ к сегменту 2, затем передает кадр в порт 2. Если бы компьютеры принадлежали одному сегменту, то кадр был бы просто удален из буфера. Такая операция называется *фильтрацией* (Filtering).

2. Запись адреса компьютера 4 в таблице отсутствует. В этом случае мост передает кадр в порт 2 и выявляет адрес, как описано выше.

Используются два вида записей: динамические и статические.

Динамические записи создаются в процессе самообучения моста. При создании или обновлении записи в адресной таблице с ней связывается отметка времени. Если по истечении *тайм-аута* (определенного срока) мост не принял ни одного кадра с адресом, указанном в поле адреса источника (отправителя), запись помечается как недействительная. Механизм динамических записей позволяет автоматически контролировать состояние компьютера:

а) можно обнаружить перемещения компьютера из сегмента в сегмент, поскольку при отключении компьютера от старого сегмента запись о его принадлежности к сегменту через некоторое время вычеркивается из адресной таблицы;

б) после включения компьютера в работу в другом сегменте его кадры начнут попадать в буфер моста через другой порт и в адресной таблице появится новая запись, соответствующая текущему состоянию сети.

Статические записи создаются администратором. Они не имеют срока жизни, что дает возможность при необходимости корректировать работу моста.

Данные, доставляемые всем узлам сети, называются *широковещательным сообщением* (Broadcast). Мосты не препятствуют распространению кадров с (известными и неизвестными) широковещательными MAC-адресами по всем сегментам сети, сохраняя при этом ее прозрачность. Такой режим распространения кадров называется *затоплением сети* (Flood) и допускается при нормальном функционировании сети. При программных или аппаратных сбоях протокол верхнего уровня или сетевой адаптер компьютера может постоянно генерировать кадры с широковещательным адресом в течение длительного промежутка времени. В этом случае мост будет передавать эти кадры во все сегменты, затапливая сеть ошибочным трафиком. Такой режим называется *широковещательным штормом* (Broadcast Storm). Мосты самостоятельно не способны защитить сети от широковещательного шторма, как это делают марш-

рутизаторы. Единственная возможность борьбы с широковещательным штормом — установка предельно допустимой интенсивности генерации кадров с широковещательным адресом администратором для каждого узла. Однако для этого нужно точно знать количественную оценку интенсивности, что весьма затруднительно.

Недостатки мостов. Один из недостатков моста проявляется в слабой защите сети от широковещательного шторма, осуществляемой администратором. Другой недостаток — ограничение топологии структурированной сети древовидной структурой, что вытекает из самого принципа построения адресной таблицы мостом. В простых сетях можно поддерживать существование одного пути между двумя сегментами. Но с увеличением количества соединений сеть становится сложной и вероятность непреднамеренного образования петли оказывается высокой.

Наличие в топологии сети петель может привести:

- к появлению нескольких копий, или размножению, кадра;
- бесконечной циркуляции обеих копий кадра по петле в противоположных направлениях, а значит, засорению сети ненужным трафиком;
- постоянной модификации мостами своих адресных таблиц, так как кадр с адресом отправителя может появляться то на одном порту, то на другом.

5.5. КОММУТАТОРЫ ЛОКАЛЬНЫХ СЕТЕЙ И ИХ ФУНКЦИИ

Коммутатор EtherSwitch. Особенности коммутаторов рассмотрим на примере технического решения, предложенного фирмой *Kalpana* для удовлетворения потребности в повышении пропускной способности связей высокопроизводительных серверов с сегментами рабочих станций (компьютеров) в сетях Ethernet [12].

В состав коммутатора входят (рис. 5.15):

- восемь *процессоров* для обслуживания пакетов Ethernet (Ethernet Packet Processor — EPP), подключенных к восьми портам 10Base-T;
- *коммутационная матрица*, предназначенная для передачи кадров между портами. Она работает по принципу коммутации каналов и способна для восьми портов обеспечить восемь одновременных внутренних каналов при полудуплексном режиме работы портов и 16 — при полнодуплексном;

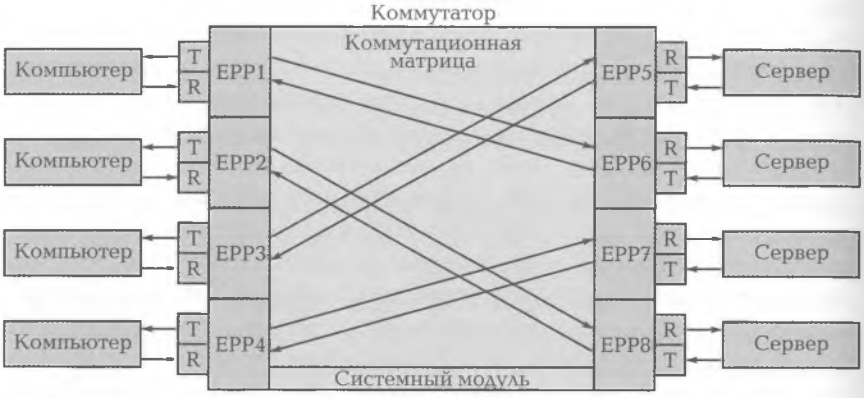


Рис. 5.15. Коммутатор фирмы *Kolpana*

- *системный модуль*, используемый для координации работы всех процессоров EPP. Он ведет общую адресную таблицу и обеспечивает управление коммутатором. Модуль работает в многозадачном режиме, параллельно обслуживая запросы всех процессоров EPP.

При поступлении кадра в какой-либо порт выполняется такая последовательность действий.

1. Процессор EPP буферизует несколько первых байтов кадра, чтобы прочитать адрес назначения.

2. Получив адрес назначения, процессор, не дожидаясь прихода остальных байтов кадра, сразу же начинает просматривать свою адресную таблицу для принятия решения о передаче пакета. При этом:

а) если нужный адрес находится в таблице, то строка с адресом поступает на хранение в буфер для последующего использования;

б) если процессор не находит в таблице нужного адреса, то обращается к системному модулю, который производит просмотр общей адресной таблицы. Найденная там строка с адресом также поступает на хранение в буфер процессора для последующего использования.

3. Во время просмотра адресных таблиц процессор EPP продолжает буферизацию поступающих в порт байтов кадра. После анализа найденного адреса назначения возможны следующие действия с поступающим кадром:

- если кадр нужно отфильтровать, то процессор просто прекращает записывать в буфер байты кадра, очищает буфер и ждет поступления нового кадра;

- если кадр требуется передать на другой порт, то процессор обращается к коммутационной матрице и устанавливает в ней путь, связывающий входной порт с портом, через который идет маршрут к адресу назначения;
- если порт назначения занят, то матрица отказывает в соединении. В этом случае процессор входного порта помещает весь кадр в буфер и ожидает освобождения выходного порта для создания коммутационной матрицей нужного пути.

4. По созданному пути буферизованные байты кадра передаются в выходной порт. После того как процессор выходного порта получит доступ (по алгоритму CSMA/CD) к подключенному к нему сегменту Ethernet, байты кадра начнут передаваться в сеть. Обычно процессор входного порта хранит несколько байтов принимаемого кадра в своем буфере, что позволяет ему независимо и асинхронно принимать и передавать байты кадра.

Для повышения производительности сети используется конвейерная обработка поступающих данных. На рис. 5.15 показана идеальная ситуация, когда в передаче задействованы все восемь портов.

Коммутационная матрица. Рассмотрим особенности коммутационной матрицы, построенной на основе коммутаторов 2×2, имеющих четыре зажима, при этом любой из зажимов *A* или *B* может быть соединен с любым зажимом *X*, *Y* (рис. 5.16, *а*). На рис. 5.16, *в* представлена *трехступенчатая* матрица, связывающая восемь входных портов с восемью выходными портами при использовании 12 коммутаторов. Структура сети внутри матрицы получается путем чередования сигналов, подаваемых на входы коммутаторов. На верхние входы каждого коммутатора подаются сигналы из верхней половины всех входных сигналов, на нижние входы — из нижней половины.

Принцип работы матрицы поясним на конкретном примере, полагая, что формат сообщения содержит (рис. 5.16, *б*):

- поле *Направление передачи* — задает два направления передачи сообщения: входной порт → выходной порт или выходной порт → входной порт;
- поле *Адрес назначения* — определяет адрес получателя;
- поле *Номер порта* — это код требуемого порта. Каждый разряд кода определяет выходной зажим коммутатора: 0 — зажим *X* или *A* в зависимости от направления передачи; 1 — зажим *Y* или *B*.

При поступлении сообщения по адресу назначения в зависимости от направления определяется номер выходного (входного)

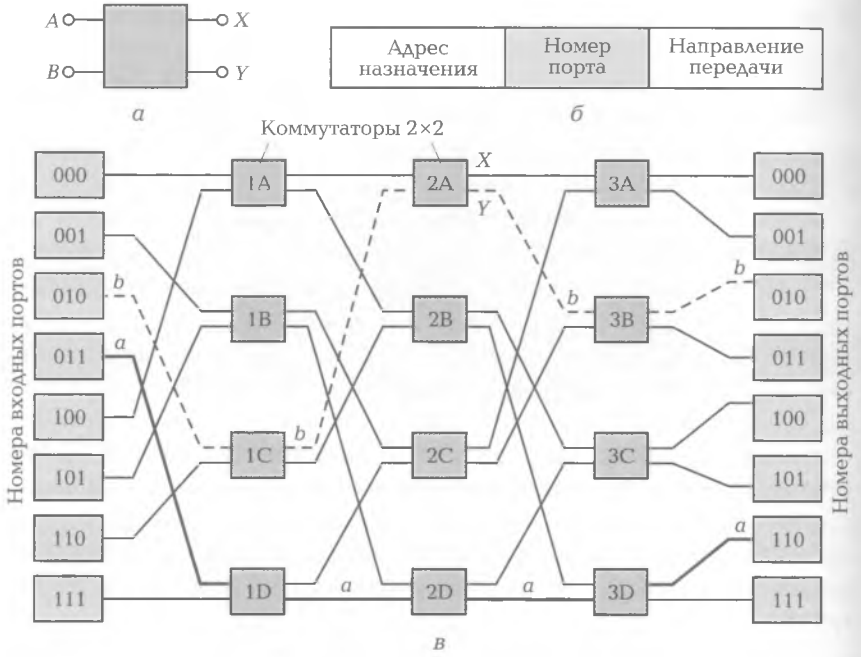


Рис. 5.16. Коммутатор 2 × 2 (*а*), формат сообщения (*б*) и структура матрицы (*в*)

порта. Предположим, что нужно передать сообщение из входного порта 011 в выходной порт 110, т. е. задано направление входной порт → выходной порт и номер выходного порта 110. Его разряды указывают на то, что путь пролегает через нижние выходы *Y* коммутаторов 1D (**1**), 2D (**1**) и верхний выход *X* коммутатора 3D (**0**). Маршрут для этого случая показан на рис. 5.16, *в* толстой сплошной линией и обозначен буквой *a*. В это же самое время через матрицу может передаваться сообщение в обратном направлении из выходного порта 010 во входной порт 010 (толстая пунктирная линия с буквой *b*). Однако попытка передачи сообщения входной порт 111 ↔ выходной порт 000 (в любую сторону) удовлетворена не будет, придется подождать, пока освободятся требуемые для прокладки маршрута коммутаторы. Таким образом, коммутаторы с такой матрицей являются *блокируемыми коммутаторами*. Не всякий набор запросов может быть удовлетворен одновременно.

Наличие процессорных модулей в коммутаторе позволяет помимо выполнения основной функции — передачи кадров с порта на порт по алгоритму моста — нагрузить его некоторыми допол-

нительными функциями, полезными при построении надежных и гибких сетей.

Поддержка алгоритма покрывающего дерева. Рассмотренный ранее алгоритм прозрачного моста используется только в ЛС с древовидной (без петель) топологией, имеющих *низкую* надежность, поскольку при выходе из строя любой линии связи или коммутатора сеть распадается на два или более изолированных сегмента.

Появление коммутаторов с расширенными функциональными возможностями позволило использовать алгоритмы управления маршрутизацией в сетях со сложной топологией. Одним из таких алгоритмов является *алгоритм покрывающего дерева* (Spanning Tree Algorithm — STA), позволяющий коммутаторам автоматически определять древовидную конфигурацию связей в сети при произвольном соединении портов между собой. Коммутаторы находят (формируют) покрывающее дерево с помощью обмена служебными пакетами. Благодаря алгоритму STA, который обеспечивает избыточные связи, появилась возможность на основе коммутаторов (без маршрутизаторов) строить крупные ЛС, обладающие *высокой* надежностью.

Для пояснения алгоритма покрывающего дерева воспользуемся рис. 5.17, на котором изображены:

- *корневой коммутатор* 1, или *корень* дерева, от которого начинает строиться дерево;
- *назначенные коммутаторы* 2 и 5, которые совместно с корнем дерева образуют активную конфигурацию сети. Назначенным коммутатором сегмента объявляется коммутатор, которому принадлежит назначенный порт данного сегмента;
- *резервные коммутаторы* 3 и 4, в которых отсутствуют порты, передающие кадры данных;
- *корневые порты* 1 коммутаторов 2—5, которые имеют кратчайшее расстояние до одного из портов корневого коммутатора. Отметим, что в коммутаторе 3 в качестве корневого порта можно было выбрать порт 2;
- *назначенные порты*: порт 1 для сегмента 1; порт 2 для сегментов 2, 3 и 4; порт 3 для сегмента 5. Назначенный порт должен иметь минимальное расстояние до корневого коммутатора среди *всех* портов *всех* коммутаторов данного сегмента сети;
- *заблокированные порты* 2 коммутаторов 3 и 4.

При автоматическом конфигурировании все коммутаторы сети после их инициализации начинают периодически обмениваться

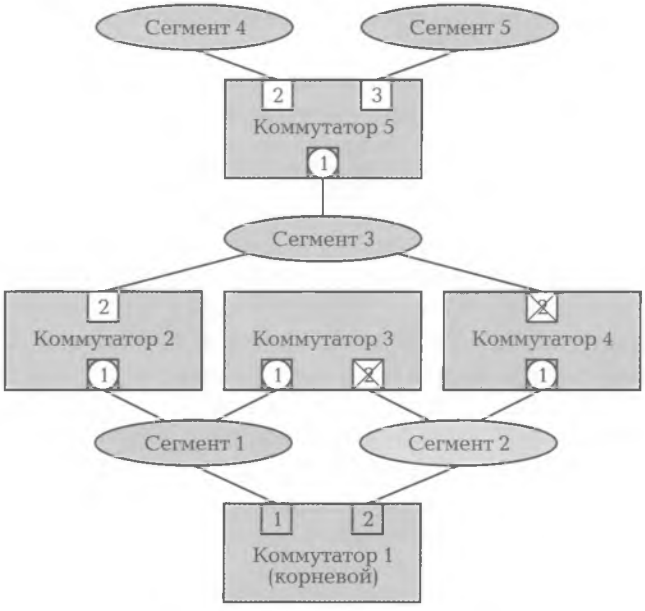


Рис. 5.17. Иллюстрация алгоритма покрывающего дерева:
◯ — корневой порт; □ — назначенный порт; ⊠ — заблокированный порт

протокольными блоками данных (Bridge Protocol Data Unit — BPDU). Пакеты BPDU содержат поля, которые используются в процессе конфигурации: *тип* пакета BPDU; *идентификаторы* версии протокола STA, корневого коммутатора и порта; расстояние до корневого протокола; время жизни сообщения и др.

Активная конфигурация сети формируется в такой последовательности:

1) определяется *корневой коммутатор* (Root Switch), от которого строится дерево. При автоматической конфигурировании корневым становится коммутатор с меньшим значением MAC-адреса его блока управления, при ручном назначается администратором. Корневым коммутатором выбран коммутатор 1;

2) для каждого коммутатора определяется *корневой порт* (Root Port), который имеет по сети кратчайшее расстояние до любого из портов корневого коммутатора;

3) для каждого сегмента сети выбирается *назначенный порт* (Designated Port), имеющий кратчайшее расстояние от данного сегмента до корневого коммутатора;

4) на последнем этапе конфигурирования каждый коммутатор блокирует собственные порты, которые не являются корневыми и назначенными.

При таком выборе активных портов в сети исключаются петли и оставшиеся связи образуют *покрывающее дерево* (если оно принципиально может быть построено при существующих связях в сети). Активная структура сети, полученная по завершении конфигурирования, показана на рис. 5.17.

Отметим, что понятие расстояния, которое определяется как суммарное время на передачу одного бита данных от порта данного коммутатора до порта корневого коммутатора, играет важную роль в построении покрывающего дерева. По этому критерию выбирают единственный порт, соединяющий каждый *коммутатор* (или *сегмент сети*) с корневым коммутатором. В приведенном примере предполагалось, что все сегменты работают на одной скорости и поэтому имеют одинаковые условные расстояния.

Достоинство алгоритма покрывающего дерева состоит в том, что решение о реконфигурировании сети принимается с учетом связей как соседних, так и отдаленных сегментов сети, недостаток — в сетях с большим числом коммутаторов время формирования новой активной конфигурации может оказаться слишком большим.

Трансляция протоколов канального уровня. Все конечные узлы имеют уникальные адреса одного и того же формата независимо от поддерживаемого протокола, поэтому адрес сетевого адаптера Ethernet понятен сетевому адаптеру FDDI и коммутаторы при согласовании протоколов ЛС не строят таблиц соответствия адресов узлов, а переносят адреса назначения и источника из кадра одного протокола в кадр другого. Трансляция протокола Ethernet в протоколы FDDI (или Token Ring) включает в себя выполнение таких операций, как *вычисление длины* поля данных кадра; *заполнение полей статуса кадра* при передаче кадров из сети FDDI в сеть Ethernet; *отбрасывание кадров*, передаваемых из FDDI в Ethernet с размером поля данных большим, чем 1 500 байт, и др.

Фильтрация трафика. Она предназначена для создания дополнительных барьеров на пути кадров, которые ограничивают доступ определенных групп пользователей к определенным службам сети. Наиболее простым способом фильтрации является фильтрация на основе MAC-адресов, когда пользователю, работающему на компьютере с данным MAC-адресом, полностью запрещается доступ к ресурсам другого сегмента сети. Многие коммутаторы

(наряду со стандартными условиями фильтрации) позволяют администраторам задавать дополнительные условия фильтрации кадров в соответствии с информацией адресной таблицы. Например, можно запретить некоторому пользователю печатать свои документы на определенном сервере печати чужого сегмента, а остальные ресурсы этого сегмента сделать доступными.

Приоритетная обработка кадров. Обычно для каждого входного и выходного порта коммутатор ведет несколько очередей, каждая из которых имеет свой приоритет обработки. Коммутатор может быть сконфигурирован так, чтобы на несколько высокоприоритетных пакетов передавать только один низкоприоритетный пакет. Приоритетная обработка возможна благодаря наличию буферной памяти и применяется для приложений, предъявляющих различные требования к допустимым задержкам кадров и к пропускной способности сети для потока кадров.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что представляет собой линия связи? Как классифицируют линии связи? Какие особенности имеют проводные и беспроводные среды передачи данных?
2. Что такое амплитудно-частотная характеристика, фазочастотная характеристика, полоса пропускания, пропускная способность, помехоустойчивость и затухание линий связи?
3. Какие виды кабельных сред применяют для передачи данных? Дайте их краткую характеристику и сравнительную оценку.
4. Какие особенности имеют одно- и многомодовый оптоволоконный кабель? Какие интерфейсы применяют в оптоволоконных сетях и в чем состоят их особенности?
5. Чем характеризуются беспроводные каналы связи? Поясните принцип передачи данных.
6. В чем заключается сущность способов организации радиосвязи через базовую станцию и с помощью спутников? Какие способы доступа к базовой станции используются в беспроводной среде и как они реализуются?
7. Для каких целей используют логическую структуризацию сети и с помощью каких средств она реализуется?
8. В чем состоит отличие коммутатора от моста? Какова сущность алгоритма прозрачного моста? Проиллюстрируйте работу прозрачного моста на примере. Как работает мост в широковещательных режимах? Каковы недостатки мостов?
9. Из каких блоков состоит коммутатор EtherSwitch? Поясните алгоритм работы коммутатора.

10. Каковы схемные особенности коммутационной матрицы? Поясните принцип работы матрицы на конкретном примере.
11. Для чего предназначен алгоритм покрывающего дерева? Поясните принцип действия алгоритма покрывающего дерева. В какой последовательности формируется активная конфигурация сети? Каковы достоинства алгоритма покрывающего дерева?
12. Поясните следующие функции коммутаторов: трансляция протоколов канального уровня, фильтрация трафика, приоритетная обработка кадров.

Глава 6

ЛОКАЛЬНЫЕ СЕТИ

6.1. СЕТИ ETHERNET

Архитектура Ethernet разработана в 1960-х гг., а в 1980 г. закреплена стандартом института IEEE 802.3. На основании этого стандарта можно выделить следующие характерные признаки сетевой архитектуры Ethernet:

- *физическая топология сетей* — шина или «звезда»;
- *метод доступа к сети* — множественный доступ с контролем несущей частоты и обнаружением конфликтов (Carrier Sense Multiple Access Collision Detect — CSMA/CD);
- *пакетная передача немодулированных сигналов* — по коаксиальным кабелям, витым парам или оптоволокну с использованием временно́го принципа разделения каналов.

Основными факторами, способствующими широкой популярности и долголетию Ethernet, являются высокая надежность, низкая стоимость сетевого оборудования, простота обслуживания сети, простая возможность взаимодействия с Internet с помощью протокола без установления соединения (TCP/IP) и др. [12]. Благодаря использованию современного сетевого оборудования Ethernet догнал и перегнал по скорости работы глобальные сети (FDDI, ATM), не растеряв при этом всех своих старых достоинств ЛС.

Рассмотрим разновидности архитектуры Ethernet. Их изучение позволит проследить историю развития ЛС с момента зарождения до настоящего времени.

Сети 10Base-5. Эта сеть — оригинальный (первый) полный вариант спецификации Ethernet.

Состав сети. Фрагмент сети из *нагруженного* и *ненагруженного* сегментов приведен на рис. 6.1. На концах каждого сегмента устанавливаются терминаторы. Компьютеры К (или рабочие станции) через интерфейс подключаемых устройств (Attachment Unit

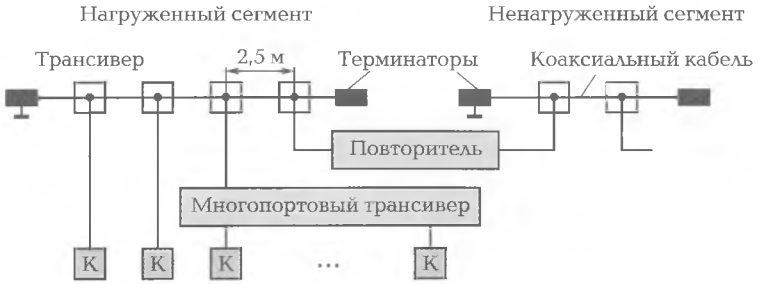


Рис. 6.1. Фрагмент сети 10Base-5:
К — компьютер

Interface — AUI) соединены с нагруженным сегментом. В ненагруженных сегментах компьютеры отсутствуют. Сеть имеет *шинную топологию*.

В сетях 10Base-5 используется толстый (диаметром 0,5 дюйма) *коаксиальный кабель* RG-8 с посеребренной центральной жилой, двойной экранирующей оплеткой, волновым сопротивлением 50 Ом и малым затуханием, который служит общей линией связи для всех компьютеров сети. Т-образные ответвления кабеля не допускаются. Максимальная длина кабельного сегмента составляет 500 м.

Сопротивление согласующих *терминаторов* на концах сегментов выбирается равным волновому сопротивлению кабеля (50 Ом). В этом случае терминаторы поглощают распространившиеся по кабелю сигналы и препятствуют возникновению отраженных сигналов. При отсутствии терминаторов в кабеле возникают стоячие волны. Это может привести к тому, что одни компьютеры получат мощные сигналы, а другие — настолько слабые, что их прием станет невозможным.

В состав интерфейса подключаемых устройств AUI входят одно- и многопортовый трансиверы, повторитель и трансиверный кабель, а также сетевой адаптер компьютера.

Термин «трансивер» происходит от двух английских слов: *trans*mitter (передатчик) + rece*iver* (приемник) = *transiver* (приемопередатчик). По функциональному назначению трансивер можно считать частью сетевого адаптера компьютера. Однако он устанавливается непосредственно на кабеле (см. рис. 6.1). Через трансивер осуществляется доступ к среде передачи данных.

Структура *однопортового трансивера* приведена на рис. 6.2. В его состав входят следующие узлы:

- *передатчик* и *приемник*, которые присоединяются к одной точке кабеля с помощью специальной схемы, позволяющей организовать одновременную передачу и прием сигналов;
- *детектор коллизий*, обеспечивающий доступ компьютера к среде передачи данных. Он определяет наличие коллизии в коаксиальном кабеле по повышенному уровню постоянной составляющей сигналов. Если постоянная составляющая более 1,5 В, значит, на кабель работает более одного передатчика;
- *узел локального управления*, предназначенный для контроля длительности транслируемых трансивером сообщений. При неисправностях в адаптере может возникнуть ситуация, когда в кабель будет непрерывно выдаваться последовательность случайных сигналов. Так как кабель является общей средой для всех компьютеров, работа сети может быть заблокирована одним неисправным адаптером. Чтобы этого не случилось, узел локального управления проверяет время передачи кадра. Если время передачи пакета превышает 4 мс, то выход передатчика отсоединяется от кабеля;
- *развязывающие элементы* (РЭ), которые обеспечивают высоковольтную (1...5 кВ) гальваническую развязку трансивера от остальной части сетевого адаптера и тем самым защищают адаптер и компьютер от значительных перепадов напряжения, возникающих на кабеле при его повреждении;
- *светодиодные индикаторы*, фиксирующие наличие питания, режимы передачи и приема, контроля детектора коллизий и коллизии.

Рис. 6.2. Схема трансивера

Трансивер устанавливается либо между концевыми разъемами отрезков кабеля в виде вставки через Т-коннектор, или с прокалыванием кабеля («зуб вампира»).

К одному сегменту допускается подключение не более 100 трансиверов на расстоянии не менее 2,5 м друг от друга. На кабеле через каждые 2,5 м нанесены метки, обозначающие точки подключения трансиверов. Подсоединение компьютеров в соответствии с разметкой сводит к минимуму влияние стоячих волн в кабеле на сетевые адаптеры.

Многопортовые трансиверы (см. рис. 6.1) предназначены для увеличения числа подключаемых к сети 10Base-5 адаптеров (компьютеров). Они обычно имеют восемь портов и допускают одноуровневое каскадирование, поэтому к одному установленному на кабеле трансиверу можно подключать до 64 компьютеров. Многопортовые трансиверы обеспечивают коллективный доступ к среде всем подключенным к ним адаптерам.

Повторители представляют собой активные устройства, предназначенные для увеличения общей длины сети путем объединения нескольких сегментов кабеля. Повторитель (см. рис. 6.1) подключается к трансиверам разных сегментов, поэтому принимает сигналы из одного сегмента кабеля и побитно синхронно повторяет их в другом сегменте, улучшая форму и повышая мощность импульсов.

Трансивер соединяется с сетевым адаптером или многопортовым трансивером с помощью *трансиверного кабеля* длиной до 50 м, который также имеет названия *интерфейсный кабель* или *кабель-спуск* (Drop Cable). Он включает в себя четыре витые экранированные пары и 15-штырьковые разъемы D-типа с защелками (Slide): розетка — к трансиверу, вилка — к AUI-разъему адаптера. По кабелю передаются сигналы передачи, приема, детектора коллизий, а также питание (12 В) цепей трансивера (см. рис. 6.2).

Топологические ограничения. Соединение отдельных сегментов в сеть подчинено правилу «5-4-3»: пять сегментов, четыре повторителя, три нагруженных сегмента (рис. 6.3). Между нагруженными сегментами должны быть включены ненагруженные сегменты.

Максимальная конфигурация сети представляет собой один центральный и два крайних нагруженных сегмента, которые соединены между собой двумя ненагруженными сегментами.

Ограниченное число повторителей обусловлено дополнительными задержками распространения сигнала, которые они вносят. Каждый повторитель подключается к сегменту одним своим трансси-

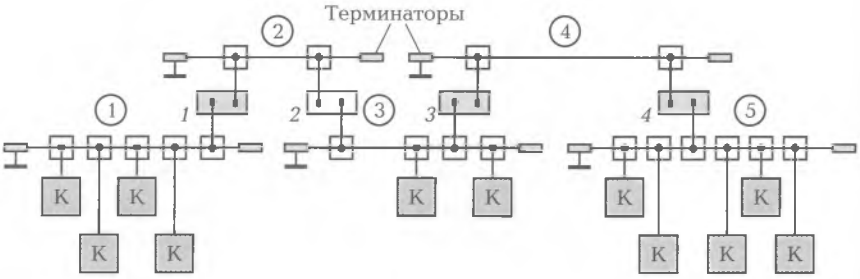


Рис. 6.3. Соединение сегментов по правилу «5-4-3»:

К — компьютер; *1—4* — повторители; ①, ③, ⑤ — нагруженные сегменты; ②, ④ — ненагруженные сегменты

вером, поэтому к нагруженным сегментам можно подключить не более 99 компьютеров. Максимальное число компьютеров (оконечных узлов) в последовательной цепи с тремя нагруженными сегментами составляет $99 \cdot 3 = 297$.

Применение многопортовых повторителей позволяет соединять по схеме звезды или дерева большее число кабельных сегментов, однако на любом пути не должно быть более пяти сегментов.

Сети 10Base-2. Основные особенности сети 10Base-2 состоят в том, что:

- используется *тонкий* коаксиальный кабель RG-58 с волновым сопротивлением 50 Ом. Максимальная длина кабельного сегмента составляет 185 м;
- адаптеры имеют встроенный трансивер, оканчивающийся BNC-разъемом (Bayonet Nut Connector — шипообразный, или штыкообразный, разъем), который гальванически отсоединен от схем адаптера. К кабелю адаптеры подключаются с помощью Т-коннекторов. Минимальное расстояние между точками подключения составляет 0,5 или 1 м.

Архитектура 10Base-2 хорошо подходит для небольших временных сетей. По электрическим сигналам, передаваемым по коаксиальному кабелю, сети 10Base-2 и 10Base-5 совместимы. Возможно построение комбинированных сегментов, состоящих из тонкого и толстого кабелей.

Подключение адаптера 10Base-5 к тонкому кабелю осуществляется через AUI-интерфейс с помощью внешнего трансивера. Тонкий кабель сети 10Base-2 дешевле, чем толстый кабель, используемый в 10Base-5, однако тонкий кабель более восприимчив к поме-

хам, чем толстый. Общим недостатком сетей 10Base-5 и 10Base-2 является отсутствие оперативной информации о состоянии сети. Повреждение кабеля обнаруживается сразу же (сеть перестает работать), но для поиска отказавшего отрезка кабеля необходим кабельный тестер.

Основные показатели сетей 10Base-2 и 10Base-2 приведены в табл. 6.1.

Сети 10Base-T. Главное отличие сетей 10Base-T от рассмотренных выше сетей Ethernet состоит в том, что вместо коаксиального кабеля используются две *неэкранированные витые пары* (Twisted-Pair) с волновым сопротивлением 85...150 Ом. Минимальная длина кабельного сегмента составляет 2,5 м, максимальная — 100 м. Кабель может вносить затухание до 11,5 дБ в диапазоне частот 5...10 МГц и задержку сигнала в сегменте порядка 1 мкс. Оконечные узлы (компьютеры) соединяются по двухточечной схеме с многопортовыми повторителями, которые обычно называют *концентраторами*, или *хабами*. Пример сети с использованием 4-портового концентратора показан на рис. 6.4. Приемник Rx концентратора принимает сигналы от одного из компьютеров и синхронно передают их на передатчики Tx всех своих остальных портов,

Таблица 6.1

Показатель	10Base-5	10Base-2
Вид сообщения	Немодулированный сигнал	
Метод доступа	CSMA/CD	
Коаксиальный кабель	Толстый	Тонкий
Ответвления кабеля	Не допустимы	
Длина кабельного сегмента, м	До 500	До 185
Максимальная длина трансиверного кабеля, м	50	—
Подключение трансиверов, м	Через 2,5	Не менее 0,5
Максимальное число точек подключения	100	30
Применение повторителей	По правилу «5-4-3»	
Максимальное число узлов	1 024	
Допустимое напряжение гальванической развязки трансивера и адаптера	1...5 кВ	100...150 В

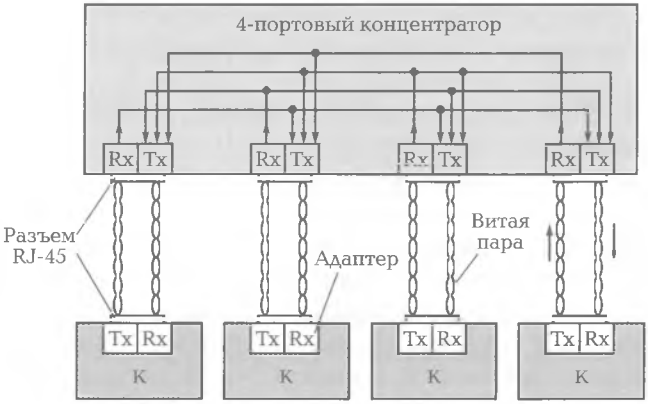


Рис. 6.4. Сеть 10Base-T с концентратором

кроме того, с которого поступили сигналы. Один из компьютеров принимает адресованные ему сигналы.

Основные особенности сетей 10Base-T связаны с тем, что:

а) *физической топологией* сети является «звезда», в центре которой находится концентратор;

б) поскольку концентратор выполняет функции повторителя сигналов по всем своим портам, образуется единая среда передачи данных — *логическая общая шина*;

в) благодаря схеме соединений приемников Rx с передатчиками Tx концентратор позволяет *обнаружить коллизию* в сети. При одновременном приеме сигналов по нескольким своим Rx-входам, получаемых от компьютеров, концентратор посылает ответный сигнал об обнаружении коллизии на все свои Tx-выходы (Transmit Mode Collision Detection);

г) поскольку к каждому компьютеру подходит только один гибкий кабель, его повреждение приведет к отказу соединения только одного компьютера, или узла сети;

д) имеется простая возможность контроля состояния каждой линии связи. В сетях 10Base-T для проверки целостности линии один раз в 16 мс узлы обмениваются специальными импульсными посылками. Отсутствие этих импульсов в течение определенного времени рассматривается как обрыв линии.

В качестве соединителей используются 8-позиционные модульные разъемы типа RJ-45 (вилки на концах кабеля и гнезда на адаптерах). Различают два типа портов: *типа MDI* (Media Dependent

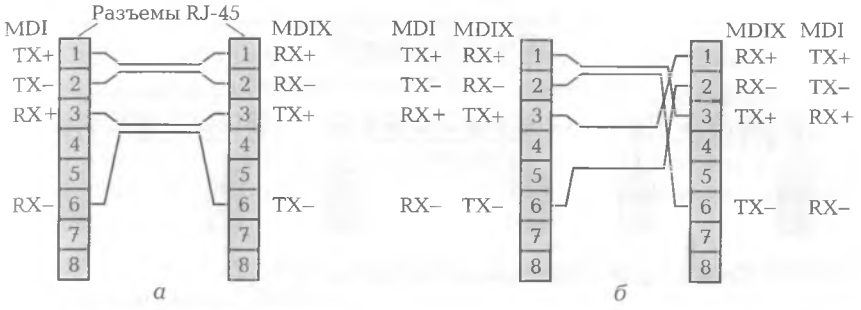


Рис. 6.5. Схемы соединения портов MDI и MDIX:
а — прямой кабель; *б* — перекрестный кабель

Interface — интерфейс, зависящий от среды передачи), соответствует для компьютеров гнездам адаптеров, а для концентраторов — гнездам, предназначенным для каскадирования; *типа MDIX* (Media Dependent Interface Xovier-Crossover — перевернутый MDI), соответствует гнездам концентраторов, предназначенным для подключения абонентов.

Схемы соединений, используемые в сетях 10Base-T, приведены на рис. 6.5. Порты MDI ↔ MDIX соединяются по схеме *прямого кабеля* (см. рис. 6.5, *а*). Соединение портов MDI ↔ MDI и MDIX ↔ ↔ MDIX осуществляется по схеме *перекрестного кабеля* (см. рис. 6.5, *б*). Эти схемы соединений используются при построении сетей со сложной топологией. При этом следует учитывать, что для надежного распознавания коллизий компьютерами сети максимальное число концентраторов между ними не должно превышать 4. Это условие носит название *правила четырех концентраторов*, или *хабов*. Для иллюстрации принципов построения сетей 10Base-T на рис. 6.6 изображена структура сети с использованием четырех концентраторов.

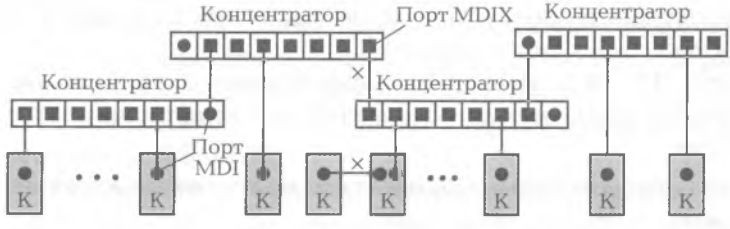


Рис. 6.6. Принцип соединения концентраторов:
К — компьютер; × — соединения по схеме перекрестного кабеля

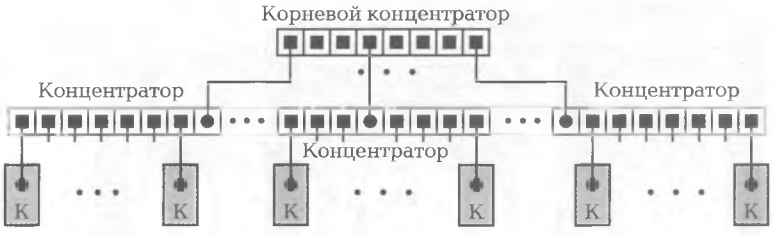


Рис. 6.7. Сеть с двумя уровнями концентраторов

Для построения сети 10Base-T с большим числом компьютеров концентраторы можно соединять друг с другом иерархическим способом, образуя древовидную структуру. Сеть с двумя уровнями концентраторов, в которой между любыми двумя компьютерами располагается только три концентратора, приведена на рис. 6.7. Общее число компьютеров в сети 10Base-T не должно превышать 1 024.

К достоинствам сетей 10Base-T следует отнести сравнительно низкую стоимость оборудования, простоту построения и модернизации, возможность контроля работоспособности и тестирования сети, к недостаткам — низкие скоростные качества и ограниченный радиус действия.

Оптоволоконные сети. Для построения оптоволоконных сетей разработаны стандарты FOIRL и 10Base-F с протоколами 10Base-FL, 10Base-FB и 10Base-FP. Сети включают в себя сетевые адаптеры, концентраторы, или многопортовые повторители, и кабель. Для соединения адаптера компьютера с портом концентратора используется достаточно дешевое многомодовое волокно на волне 850 нм, обладающее полосой пропускания 500...800 МГц при длине кабеля 1 км, реже — одномодовое (1310 нм). Смешанное соединение портов в сетях недопустимо. Более широкое распространение получили сети FOIRL10 и 10Base-FL, оборудование для которых выпускает широкий круг производителей. Протокол FOIRL10 полностью совместим с 10Base-FL.

Сеть FOIRL (Fiber Optic Inter-Repeater Link — волоконно-оптический канал между повторителями) имеет следующие особенности:

- длина оптоволоконной линии связи между повторителями — до 1 км;
- максимальное число повторителей между любыми узлами сети — 4;

- максимальный диаметр сети — 2,5 км, однако недопустимы отрезки кабеля предельного размера (1 км) между четырьмя повторителями, а также между повторителями и оконечными узлами сети;
- используются трансиверы, у которых с одной стороны имеется AUI-интерфейс (вилка DB-15P), с другой — два оптических коннектора ST.

Сеть 10Base-FL (Fiber Link) представляет собой улучшенный вариант сети FOIRL:

- максимальное расстояние между компьютером (узлом) и концентратором составляет 2000 м благодаря увеличению мощности передатчиков;
- при использовании одномодового волокна дальность связи составляет 5 км в полудуплексе и 10 км в дуплексе;
- совместима с сетью FOIRL при ограничении по дальности для многомодового волокна в 1 км;
- обеспечивается возможность подключения к пассивному разветвителю 10Base-FP;
- одномодовые порты позволяют использовать многомодовый кабель с ограничением на дальность связи до 2 км.

Сеть 10Base-FB (Fiber Backbone) предназначена для организации синхронных передач на дальние расстояния, т.е. представляет собой синхронный Ethernet. Она используется только для соединения концентраторов (повторителей), при этом оконечные узлы (компьютеры) не могут быть присоединены к портам концентратора. Вследствие этого с протоколами 10Base-FL или FOIRL совместимости нет. Синхронность позволяет увеличить число повторителей в цепочке до 12...15. Длина цепочки ограничена временем распространения сигнала между дальними узлами (25,6 мкс). Сеть также обеспечивает удаленную сигнализацию отказа линии путем оповещения концентраторов о разрыве волокна.

Сеть 10Base-FP (Fiber Passive) представляет собой сеть со звездообразной топологией с использованием пассивного разветвителя, который может объединять до 33 компьютеров, удаленных от него до 500 м (затухание 16...20 дБ). Подключаемые узлы должны иметь порты 10Base-FL.

Сети Fast Ethernet. Варианты сетей Fast Ethernet (Fast — быстрый) со скоростью передачи данных 100 Мбит/с описываются стандартом IEEE 802.3u, принятым в 1995 г. Сети Fast Ethernet сохранили характерные черты сетей 10Base-T и 10Base-F. Они осно-

ваны на том же *методе доступа* CSMA/CD к разделяемой среде, также используют *звездообразную* топологию с активным устройством в центре и оставляют такими же все соотношения, измеренные в битовых интервалах. Сокращение в 10 раз длительности битового интервала и максимально допустимого времени прохождения между двумя узлами до 2,6 мкс привело к более жестким топологическим ограничениям. Однако это обстоятельство не препятствует построению крупных сетей. Использование коммутаторов снимает ограничения на общую длину сети, остаются только ограничения на длину физических сегментов, соединяющих соседние устройства.

Стандартом установлено три основных вида сетей.

Сети 100Base-FX. В оптоволоконном варианте сетей Fast Ethernet со скоростью передачи 100 Мбит/с используется одно- и многомодовое волокно с длиной волны 1300 нм. В полудуплексном режиме дальность связи составляет 412 м, а в дуплексном — до 2 км для многомодового и до 32 км для одномодового волокна. В сетях 100Base-FX используется метод логического кодирования 4B/5B, в котором каждые 4 бит исходных данных (символов) представляются 5 бит. Избыточный бит позволяет получить 16 дополнительных комбинаций, с помощью которых можно распознать и отбраковывать ошибочные символы, повысив тем самым устойчивость работы сети, либо использовать для других целей. В сетях 100Base-FX/TX запрещенная комбинация 11111 используется в качестве символа простоя источника — *Idle*. Повторяющаяся передача символа *Idle* свидетельствует о том, что среда свободна. Для отделения кадра Ethernet от символов простоя *Idle* используются две других запрещенных комбинации из символов *J* (11000) и *K* (10001) в качестве 16-разрядного кода начального ограничителя кадра, а после завершения кадра перед первым символом простоя источника вставляется символ *T* (01101). Такое оформление кадра, показанное на рис. 6.8, позволяет приемнику всегда находиться в синхронизме с передатчиком.

На физическом уровне 5-битные комбинации представляют в виде потенциального кода с возвратом к нулю без инверсии (NRZI).

Преамбула *Idle*	*JK*	Преамбула	SFD	DA	SA	L	Данные	CRC	*T*	Преамбула *Idle*

Рис. 6.8. Формат кадра в сетях 100Base-FX/TX

Отметим, что для случая, когда не требуется преодоления больших расстояний, разработана новая версия оптоволоконной сети 100Base-SX как дешевая альтернатива дорогой сети 100Base-FX. Сеть строится на многомодовом волокне с использованием коротковолновых (830 нм) светодиодных передатчиков. Дальность связи составляет всего 300 м. Однако она поддерживает совместимость с сетью 10Base-FL и автоматическое согласование скорости передачи 10/100 Мбит/с (802.3u).

Сеть 100Base-TX. Эта сеть имеет следующие характерные особенности:

- средой передачи данных являются витые пары UTP категории 5 или STP типа 1;
- логическое кодирование осуществляется по методу 4B/5B: 4 бит исходной информации преобразуются в 5-битный символ. Избыточность используется для повышения достоверности и служебных целей;
- реализуются полудуплексный и полнодуплексный режимы работы;
- по используемым разъемам полностью соответствует сети 10Base-T;
- определено пять различных режимов автопереговоров (Autonegotiation): режим 10Base-T, дуплексные режимы 10Base-T и 100Base-TX, режимы 100Base-TX и 100Base-T4. Переговорный процесс может быть инициирован в любой момент модулем управления устройства. Устройство, начавшее процесс автопереговоров, посылает своему партнеру специальный сигнал. Узел-партнер, имеющий функцию автопереговоров, может принять или отклонить запрос, а также предложить режим с более высоким уровнем приоритета. Режим 10Base-T имеет самый низкий приоритет, а дуплексный режим 100Base-T4 — самый высокий.

Сеть 100Base-T4. Такие сети используют четыре неэкранируемых витых пары категории 3, 4 или 5. При этом кадр передается параллельно по трем парам. Передача ведется со скоростью 33,3 Мбит/с. Каждые 8 бит, передаваемые по конкретной паре, кодируются шестью троичными цифрами по методу 8B/6T, что соответствует скорости изменения сигналов в линии $33{,}3 \cdot 6/8 = 25$ Мбод, т.е. 25 Мбит за 1 такт. Эти меры позволяют уменьшить необходимую для передачи полосу пропускания кабеля до требований категории 3 (16 МГц). Четвертая пара служит для прослушивания сигнала от противоположного передатчика: по его появлению определяется факт коллизии.

Для подключения оконечных узлов к портам активного оборудования используется рассмотренная выше схема *прямого кабеля*, для непосредственного соединения оконечных узлов или соединения двух коммуникационных устройств — схема *перекрестного кабеля*.

Для сетей 100Base-T4 также предусмотрена функция автопереговоров.

Коаксиальный кабель в сетях Fast Ethernet не находит применения, так как на *небольших расстояниях* используется витая пара категории 5, которая позволяет передавать данные с той же скоростью, что и коаксиальный кабель, при этом сеть получается более дешевой и удобной в эксплуатации, а на *больших расстояниях* используется оптическое волокно, обладающее более широкой полосой пропускания при незначительном превышении затрат по сравнению с коаксиальным кабелем.

Особенности построения сетей. При построении сетей Fast Ethernet необходимо выдержать ряд ограничений. Максимальные значения *длины сегментов* для случаев, когда сетевой адаптер непосредственно соединяется с портом моста (коммутатора) или маршрутизатора, или когда порты мостов, коммутаторов и маршрутизаторов соединяются между собой, приведены в табл. 6.2. Ограничений на общую длину сети нет.

В сетях Fast Ethernet используются два класса повторителей.

Повторители класса I поддерживают два способа кодирования данных: 4B/5B и 8B/6T. Это *транслирующий повторитель* (Translational Repeater). Из-за необходимости трансляции различных систем кодирования такой повторитель вносит большую задержку (70 битовых интервалов), поэтому в одном домене коллизий допускается наличие только одного повторителя класса I. Каждый из них может быть оборудован портами всех трех сетей 100Base-FX, 100Base-TX и 100Base-T4.

Повторители класса II поддерживают только какой-либо один из способов кодирования либо 4B/5B, либо 8B/6T. Их

Таблица 6.2

Сеть	Тип кабеля	Максимальная длина сегмента
100Base-FX	Многомодовое оптоволокно 62,5/125 мкм	412 м (полудуплекс), 2 км (дуплекс)
100Base-TX	Категория 5 UTP	100 м
100Base-T4	Категория 3, 4 или 5 UTP	100 м

называют *прозрачными повторителями* (Transparent Repeater). Повторители класса II при передаче сигналов вносят меньшую задержку, поэтому в домене коллизий может быть использовано два повторителя. Так как в сетях 100Base-TX и 100Base-FX используется логический код 4B/5B, повторитель класса II может быть оборудован портами для работы в обеих сетях. В сети 100Base-T4 должны использоваться повторители, поддерживающие логический код 8B/6T.

Таким образом, при построении сети Fast Ethernet необходимо придерживаться *правила одного* или *двух хабов* в зависимости от класса хаба.

Параметры сетей на основе повторителей класса I приведены в табл. 6.3.

Гигабитные сети. Главная задача, которую ставили перед собой разработчики стандарта Gigabit Ethernet, состояла в достижении битовой скорости в 1 Гбит/с при сохранении обратной совместимости со старыми сетями Ethernet. В результате появились две версии стандарта Gigabit Ethernet [2]: *802.3z* для оптоволоконных сетей 1000Base-SX, 1000Base-LX и 1000Base-CX, принятая в 1998 г., и *802.3ab* для сети 1000Base-T на витой паре, принятая в 1999 г.

В стандарте Gigabit Ethernet:

- осталась *неизменной* 48-битная схема адресации и сохранен формат кадра Ethernet, включая нижние и верхние ограничения его размера;
- по-прежнему поддерживается *полудуплексный режим работы* в сетях на основе разделяемой среды с методом доступа CSMA/CD. В полудуплексном режиме работы компьютеры в сети Gigabit Ethernet соединены через концентратор (повторитель), который связывает все линии в общую среду передачи. В связи

Таблица 6.3

Тип кабеля	Максимальный диаметр сети, м	Максимальная длина сегмента, м
Только витая пара (TX)	200	100
Только оптоволокно (FX)	272	136
Несколько сегментов на витой паре и один на оптоволокне	260	100 (TX) 160 (FX)
Несколько сегментов на витой паре и несколько на оптоволокне	272	100 (TX) 136 (FX)

с этим из-за возможных коллизий применяется метод доступа CSMA/CD. Поскольку кадр минимального размера (64 байт) должен передаваться в 100 раз быстрее, чем в классической сети Ethernet, максимальная длина сегмента уменьшается в 100 раз и составляет 25 м. При таком расстоянии между компьютерами шумовой всплеск, обусловленный коллизией, гарантированно достигнет отправителя сообщения до окончания его передачи и будет зафиксирована коллизия;

- используются основные виды кабелей — волоконно-оптический и витая пара.

Повышение скорости до 1 Гбит/с при сохранении показателей предыдущих технологий потребовало от разработчиков стандарта внесения изменений не только в физический уровень, как это было в случае Fast Ethernet, но и в уровень управления доступом к среде передачи (MAC).

Увеличение максимальной длины сегмента до 100 м (или диаметра сети до 200 м) и более достигнуто:

- введением в формат кадра дополнительного поля — поля расширения, которое сетевой адаптер компьютера заполнял нулями. Благодаря этому увеличивались размер кадра до 512 байт (4 096 бит) и продолжительность его передачи. Поскольку поле расширения вставляется отправителем после поля FCS (Frame Check Sequence — последовательность контроля кадра) и изымается получателем, оно является прозрачным для программного обеспечения и не нарушает нормальной работы сети;
- использованием *пакетной* передачи кадров (Frame Bursting), когда вместо единичного кадра посылается пакет, объединяющий в себе много кадров. Кадры пакета могут адресоваться разным получателям. Если полная длина пакета окажется меньше 512 байт, то вставляется поле расширения с фиктивными данными, как в предыдущем случае.

Использование в качестве кабеля витой пары. Решение такой задачи для 100-мегабитных сетей было сопряжено с известными трудностями. Для гигабитной сети эти трудности многократно возрастают в связи с тем, что:

а) современная сеть должна поддерживать одновременный двухсторонний обмен данными, или *полнодуплексный* режим;

б) каждая витая пара кабеля категории *5e* имеет гарантированную полосу пропускания только до 125 МГц [2], поэтому даже одновременное использование всех четырех пар без принятия дополнительных мер лишает сеть возможности работы в дуплексном

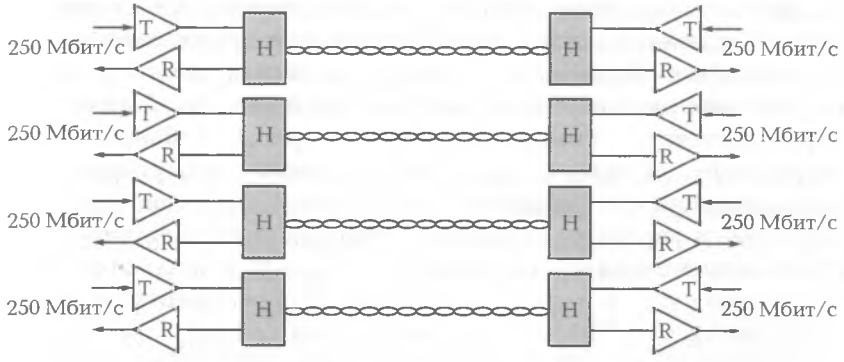


Рис. 6.9. Схема двунаправленной передачи по четырем витым парам неэкранированного кабеля категории *5e*

режиме, поскольку не остается свободных пар для одновременной передачи данных в двух направлениях.

Рассмотрим, как была решена задача использования кабеля категории *5e* (с четырьмя витыми парами) в гигабитной сети. Для передачи данных использовались следующие средства:

- 4-канальная схема с одновременной передачей в двух направлениях по всем четырем парам кабеля со скоростью 250 Мбит/с (рис. 6.9);
- 5-уровневый код (–2, –1, 0, +1, +2), обеспечивающий за один такт по одной паре передачу $\log_2 5 = 2{,}322$ бит информации. Это позволило снизить тактовую частоту до 125 МГц (с запасом, так как $250/2{,}322 < 125$) и удовлетворить требованиям по полосе пропускания для кабеля категории *5e*. Использование четырех витых пар дает возможность параллельно передавать четыре символа. Каждый символ кодируется одним из пяти уровней напряжения, поэтому для кодирования четырех разных символов достаточно двух битов, например 00 (соответствует уровню –2), 01 (–1), 10 (0) и 11 (+1). Так как на одну витую пару приходится 2 бит данных, за один временной интервал по четырем витым парам передается 8 биттов, что при тактовой частоте 125 МГц соответствует скорости $8 \cdot 125 = 1\,000$ Мбит/с = 1 Гбит/с. Пятый уровень напряжения (+2) добавлен для специальных целей — кадрирования и управления.

Полнодуплексный режим. Для его реализации используются коммутаторы, которые обладают способностью буферизировать (накапливать и сохранять) поступающие сигналы, что по-

зволяет в любое время без помех осуществлять двусторонний обмен, не прибегая к протоколу CSMA/CD, а также специальным средствам для организации полнодуплексного режима. Так как два передатчика работают навстречу друг другу, в каждой из четырех пар присутствует суммарный сигнал (см. рис. 6.9). Выделение передаваемого сигнала на другом конце линии осуществляется путем вычитания из суммарного сигнала известного приемнику сигнала своего передатчика. Схема H гибридной развязки позволяет приемнику и передатчику одного и того же узла использовать одновременно витую пару и для приема, и для передачи (так же, как и в трансиверах Ethernet на коаксиальном кабеле). Эта операция выполняется с помощью цифрового сигнального процессора (Digital Signal Processor — DSP).

Таким образом, связи в гигабитных сетях строятся по принципу точка—точка с использованием концентраторов-повторителей для организации полудуплексного режима и коммутаторов для организации полнодуплексного режима.

Метод кодирования. В сетях на смену манчестерскому кодированию пришел метод 8B/10B, позволяющий получить 1 024 кодовых комбинаций вместо 256. Данный метод предоставляет некоторую свободу выбора кодовых слов. При кодировании данных стремятся к тому, чтобы:

- ни одно кодовое слово не имело более четырех одинаковых битов подряд. Большое количество нулей может привести к сбою синхронизации;
- ни в одном кодовом слове не было более шести нулей или шести единиц. Количество нулей и единиц стараются выровнять. Это позволит уменьшить постоянную составляющую сигнала и облегчить требования к гальванической развязке цепей.

Средства контроля потока. Для контроля потока одна из сторон посылает служебный кадр, сообщающий о том, что второй стороне необходимо приостановиться на некоторое время. Служебным является обычный кадр, в поле *Type* которого записан код 1000 1000 0000 1000. Первые два байта поля данных — командные, а последующие, по необходимости, содержат параметры команды. Для контроля потока используются кадры типа PAUSE, причем в качестве параметра указывается продолжительность паузы в единицах времени передачи минимального кадра. Для гигабитного Ethernet такая единица равна 512 нс, а паузы могут длиться до 33,6 мс.

Виды сетей. Стандартом закреплены следующие виды сетей:

- 1000Base-SX (Short Wavelength), которая использует оптический интерфейс с коротковолновыми (850 нм) лазерными передатчиками для связи по многомодовому волокну (50 и 62,5 мкм) на небольшие расстояния. Длина магистрального кабеля (сегмента) — 500 м;
- 1000Base-LX (Long Wavelength), которая использует интерфейс с длинноволновыми (1310 нм) лазерными передатчиками для связи по одномодовому (10 мкм) и многомодовому (50 и 62,5 мкм) волокну на большие расстояния (порядка 5 км);
- 1000Base-CX с электрическим интерфейсом для связи на короткие расстояния (до 25 м). В качестве среды передачи данных в спецификации 1000-CX определен экранированный сбалансированный медный кабель с волновым сопротивлением 150 Ом, например двухосевой (Twinaxial) кабель или скрученные четверки проводов (Quad Cable). Подходит для соединения оборудования, расположенного в одной комнате;
- 1000Base-T на витой паре (четыре пары проводов) категории 5e (и даже 5) при ограничении на длину линии в 100 м. Используется 5-уровневое физическое кодирование. Сигнал передается одновременно по четырем парам проводов в обоих направлениях. Сигнал противоположного передатчика выделяется из смеси оконечными цепями.

Стандарт IEEE 802.3ae для локальных сетей 10G Ethernet. Отличие этого стандарта от своих прародителей существенно: он не поддерживает разделяемую среду и определяет только полнодуплексный режим, т.е. используется исключительно в коммутируемых ЛС. Стандарт описывает *семь* новых спецификаций физического уровня, которые взаимодействуют с уровнем MAC с помощью нового подуровня согласования [9]. Этот подуровень обеспечивает для всех вариантов физического уровня 10G Ethernet единый расширенный интерфейс независимого доступа к гигабитной среде (eXtended Gigabit Medium Independent Interface — XGMII). Интерфейс XGMII предусматривает параллельный обмен четырьмя байтами, образующими четыре потока данных. Существуют три группы физических интерфейсов стандарта 10G Ethernet: 10GBase-X, 10GBase-R и 10GBase-W. Они используют оптическую среду для передачи данных в диапазоне волн 850, 1310 и 1550 нм и отличаются способом кодирования данных: в варианте 10GBase-X используется код 8B/10B, а в остальных двух — 64B/66B. Группа 10GBase-X состоит из одного интерфейса 10GBase-LX4. Информация передается в каждом направлении одновременно с

помощью четырех волн длиной 1 310 нм, которые мультиплексируются на основе технологии уплотнения с разделением по длине волны (WDM). Каждый из четырех потоков передается со скоростью 2,5 Гбит/с.

Максимальное расстояние между передатчиком и приемником стандарта 10GBase-LX4 на многомодовом волокне равно 200...300 м (в зависимости от полосы пропускания волокна), а на одномодовом — 10 км. Физические интерфейсы обеспечивают передачу данных на расстояния до 40 км.

6.2. ОСОБЕННОСТИ СЕТЕЙ TOKEN RING, APPLETALK И ARCNET

Сети Token Ring. Архитектура сетей Token Ring (маркерное кольцо), появившаяся в конце 1970-х гг., была задумана и разработана компанией *IBM* как надежная сетевая архитектура на основе метода управления доступом с передачей маркера. Стандарты Token Ring определяются спецификациями IEEE 802.5, принятыми в 1985 г. В настоящее время компания *IBM* использует Token Ring в качестве своей основной сетевой технологии, производя около 60 % сетевых адаптеров.

Архитектура Token Ring имеет следующие особенности:

а) *разделяемая среда* передачи данных из *отрезков* экранированной или неэкранированной витой пары, соединяющих все компьютеры (или станции) сети в *логическое кольцо*;

б) *кольцевая логическая* топология, реализованная на основе *физической звезды*, в центре которой находится концентратор, называемый многостанционным устройством доступа (Multi-Station Access Unit — MSAU);

в) *детерминированный* метод доступа к разделяемому кольцу с помощью *маркера*, или *токена* (Token);

г) *немодулированные* цифровые сигналы, которые регенерируются сетевыми адаптерами при движении по кольцу.

Архитектура и технологии сетей обеспечивают:

- сохранение целостности кольца при выключении одного или нескольких компьютеров;
- передачу данных с двумя битовыми скоростями — 4 и 16 Мбит/с;
- максимальное расстояние от станции до MSAU — 100 м для экранированной витой пары и 45 м — для неэкранированной;

- максимальное число компьютеров в кольце с экранированной витой парой — 260, с неэкранированной — 72;
- максимальную длину кольца — 4 км;
- контроль работы сети. Обнаруженные ошибки устраняются автоматически (например, потерянный маркер восстанавливается) или только фиксируются (в этом случае устраняются вручную обслуживающим персоналом);
- возможность построения сетей произвольной конфигурации на основе нескольких колец, разделенных мостами;
- совместимость с другими технологиями локальных сетей (Ethernet, FDDI, 100VG, ARCnet), поскольку охватываются физический и канальный уровни (с реализацией логической связи через LLC-мосты).

Сети AppleTalk. Архитектура AppleTalk разработана компанией *Apple Computers* для объединения компьютеров Macintosh в целях совместного использования (разделения) файлов, принтеров и других ресурсов рабочей группы. Она включает в себя пакет протоколов AppleShare, в который входят встроенные в ОС Macintosh: *файловый сервер* AppleShare, предоставляющий пользователям доступ к ресурсам компьютера, и *принтерный сервер* AppleShare, позволяющий совместно использовать принтеры.

Сеть AppleTalk (как Ethernet) использует метод доступа CSMA/CA, поддерживает динамическую адресацию, пересылает данные со скоростью 230 Кбит/с по экранированной витой паре и позволяет подключать до 32 устройств. Сеть можно разделить на *зоны*, играющие роль, аналогичную рабочим группам в больших сетях. Пользователи имеют доступ только к разделяемым ресурсам своей зоны. Для связи между зонами используется протокол ZIP (Zone Information Protocol).

Сети ARCnet. Сетевая архитектура ARCnet (Attached Resources Computer network — компьютерная сеть соединенных ресурсов) с разделяемой средой и широковещательной передачей разработана корпорацией *DataPoint* в 1977 г. Ее особенностями являются [2]:

- логическая топология — шина; физическая топология — шина, «звезда» или смешанная; петлевые соединения недопустимы;
- метод доступа — маркерный (Token Passing);
- скорость передачи данных в канале — 2,5 Мбит/с;
- среда передачи — коаксиальный кабель, витая пара;
- максимальное число узлов в сети — 255.

Допустимые затухание сигнала между парой узлов (не более 11 дБ на частоте 5 МГц) и задержка распространения сигнала (до 31 мкс между любой парой узлов) ограничивают максимальные значения общей длины кабеля (порядка 6 000 м), длины кабеля между узлами (от 100 до 600 м в зависимости типа кабеля) и максимальное число сегментов в цепочке (3).

6.3. ПЕРСОНАЛЬНАЯ РАДИОСЕТЬ BLUETOOTH

Сеть Bluetooth предназначена для беспроводной ближней радиосвязи и позволяет объединять устройства разных типов для передачи речи и данных. Стандарт IEEE 802.15 определяет работу на частоте 2,4 ГГц, со скоростями передачи 722...784 Кбит/с и расстояниями до 10 м. Основу Bluetooth составляет пикосеть (Piconet), представляющая собой централизованную систему с временны́м уплотнением. В сеть может входить до 255 узлов (устройств), один из которых является *главным* (Master — M), остальные — *подчиненными* (Slave — S). Главным узлом может быть компьютер, подчиненным — радионаушник. Связь существует только между подчиненным и главным узлами, при этом только восемь из них могут быть одновременно *активными* и обмениваться данными. Прямой связи между активными подчиненными узлами нет.

Главный узел обеспечивает доступ к разделяемой среде пикосети на частотах диапазона 2,4 ГГц, контролирует временны́е интервалы и распределяет очередность передачи данных каждым из восьми подчиненных узлов. Кроме того, он может переводить в режим пониженного энергопотребления все остальные узлы сети, благодаря чему продлевается ресурс их источников питания. В этом режиме так называемые *отдыхающие узлы* могут принять сигнал главного узла для перехода в активное состояние.

Подключение к пикосети новых устройств (узлов) происходит динамически в такой последовательности:

1) главное устройство (узел) пикосети путем опроса собирает информацию об устройствах, попадающих в зону его действия;

2) обнаружив новое устройство, проводит с ним переговоры;

3) при получении согласия на подключение осуществляется проверка аутентичности;

4) при положительном исходе проверки подчиненное устройство присоединяется к сети.

Несколько объединенных вместе с помощью специального узла-моста пикосетей образуют *рассредоточенную сеть* (Scatter-

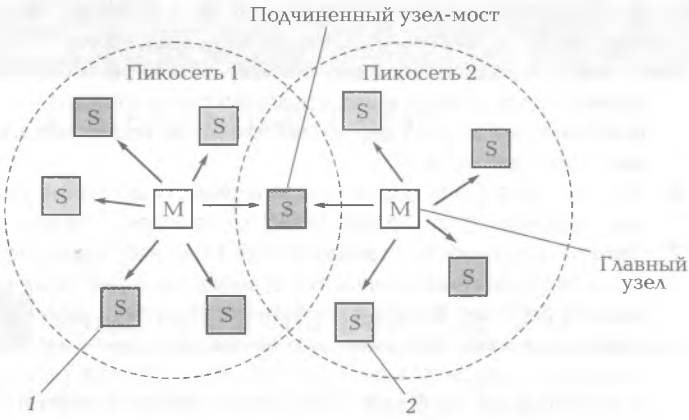


Рис. 6.10. Рассредоточенная сеть из двух пикосетей:
1 — активный подчиненный узел; *2* — отдыхающий подчиненный узел

net), при этом узел-мост в одной сети может выполнять функции главного узла, в другой сети — подчиненного. Рассредоточенная сеть, составленная из двух пикосетей, приведена на рис. 6.10. Чтобы в рассредоточенной сети исключить влияние (обусловленное интерференцией сигналов) пикосетей, друг на друга, радиопередатчик во время передачи сигнала псевдослучайным образом переходит с одной рабочей частоты на другую.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. В чем состоит смысл следующих терминов: «терминатор», «трансивер», «концентратор», «хаб», «коллизия», «маркер», «токен», «пикосеть»?
2. Каковы характерные признаки сетевой архитектуры Ethernet и основные факторы, способствующие широкой популярности и долголетию сетей Ethernet?
3. На примере стандарта 10Base-5 (см. рис. 6.1, 6.3) поясните общие принципы построения сетей Ethernet. Для чего на концах каждого сегмента устанавливаются терминаторы? Какие функции выполняют трансивер, повторитель и многопортовый трансивер? Чем обусловлены топологические ограничения сети?
4. Какова структура трансивера? Для чего предназначены детектор коллизий, узел локального управлении и развязывающие элементы?

5. В чем заключаются особенности сети 10Base-5? Почему стандарты 10Base-T и 10Base-FL/FB вытеснили стандарты Ethernet на коаксиальном кабеле? Каковы их особенности? Какие схемы соединений используются в сетях и каковы их особенности? С чем связано ограничение, известное как «правило четырех хабов»?
6. За счет чего была увеличена максимальная длина сегмента при переходе от стандарта FOIRL к стандарту 10Base-FL?
7. Каковы особенности стандарта Fast Ethernet? Какие основные виды сетей установлены этим стандартом? Дайте их краткую характеристику. Каковы особенности используемых в сетях повторителей? Чем отличаются повторители Fast Ethernet класса I и класса II? Почему в сети Fast Ethernet разрешается использование не более одного повторителя класса I?
8. Какую задачу ставили перед собой разработчики стандарта Gigabit Ethernet? Дайте краткую его характеристику. Благодаря чему достигнуто увеличение длины сегмента до 100 м и более? Какие меры были предприняты для обеспечения передачи данных со скоростью 1 000 Мбит/с по витой паре? Какие средства использованы для реализации полнодуплексного режима? Какой метод кодирования используется в сетях Gigabit Ethernet? Как организован контроль потока? Какие виды сетей закреплены стандартом?
9. Каковы особенности стандарта IEEE 802.3ae для локальных сетей 10G Ethernet? Дайте его краткую характеристику.
10. В чем проявляются особенности архитектуры Token Ring и какие возможности она обеспечивает?
11. Чем характеризуются локальные сети AppleTalk и ARCnet?
12. В чем состоит сущность основных принципов организации персональной радиосети Bluetooth? Как подключаются к пикосети новые устройства? Как на основе пикосетей построить рассредоточенную радиосеть?

Глава 7

ГЛОБАЛЬНЫЕ СЕТИ

7.1. ВВЕДЕНИЕ В ГЛОБАЛЬНЫЕ СЕТИ

Структура и состав глобальной сети. С появлением и широким распространением Internet понятие *глобальная сеть* утратило свой первоначальный смысл, поскольку любой компьютер (не говоря о ЛС), имеющий доступ к Internet, формально принадлежит этой сети. На первый план выдвигаются вопросы организации двухточечных соединений.

Глобальную сеть (рис. 7.1) можно представить как совокупность коммутаторов S (Switch), связанных друг с другом с помощью аналоговых или цифровых выделенных линий (магистралей). Коммутаторы устанавливаются в тех местах, где требуется ответвление или слияние потоков данных конечных абонентов или магистральных каналов, переносящих данные многих абонентов. Абоненты

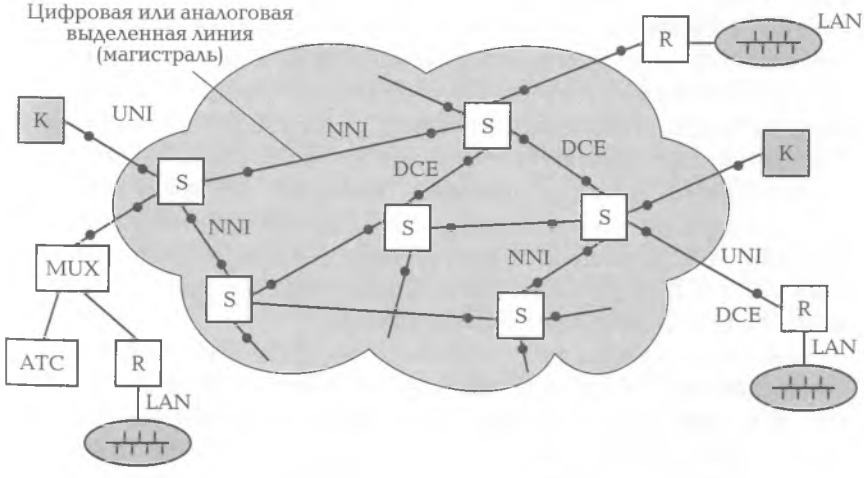


Рис. 7.1. Фрагмент глобальной сети

сети могут подключаться к коммутаторам с помощью выделенных каналов или коммутируемых телефонных линий связи. Магистральные линии связи, объединяющие коммутаторы, имеют более высокую пропускную способность, чем абонентские.

Глобальные сети содержат следующее оконечное оборудование данных (Data Terminal Equipment — DTE): компьютеры K, локальные сети (LAN), маршрутизаторы R (Router) и мультиплексоры MUX (Multiplexor). Локальная сеть подсоединяется к глобальной сети через маршрутизатор R (см. рис. 7.1) или удаленные мосты (Remote Bridges).

Передача данных через глобальную сеть происходит следующим образом:

- *маршрутизаторы* принимают решение об их отправлении следующему маршрутизатору на основании номера сети пакета какого-либо протокола сетевого уровня (например, IP или IPX). Затем упаковывают пакет в кадр этой сети, снабжают соответствующим аппаратным адресом следующего маршрутизатора и отправляют в глобальную сеть;
- *удаленные мосты* строят таблицу MAC-адресов на основании проходящего через них трафика и по данным этой таблицы принимают решение — передавать или не передавать кадры в удаленную сеть.

Для передачи в одной территориальной сети компьютерного и голосового трафиков используют *мультиплексоры* «голос — данные», которые упаковывают голосовую информацию в кадры или пакеты и передают их ближайшему коммутатору точно так же, как и любой конечный узел глобальной сети (мост или маршрутизатор). Чтобы коммутаторы обрабатывали и продвигали в первую очередь кадры голосового трафика, мультиплексор присваивает им наивысший приоритет. На приемном узле также должен быть мультиплексор «голос — данные», который сортирует поступившие данные по своим выходам: голосовые данные направляет офисной АТС, а компьютерные данные — через маршрутизатор в LAN или ЛС (см. рис. 7.1). Часто модуль мультиплексора «голос — данные» встраивается в маршрутизатор.

Для обеспечения совместимости передаваемых двоичных данных с магистральным каналом связи каждое устройство DTE и коммутатор S оснащается устройством типа DCE (Data Circuit terminating Equipment), представляющим собой аппаратуру передачи (канала) данных или коммуникационное оборудование. Для связи с каналами глобальных сетей используются:

- *модемы* для работы в выделенных и коммутируемых аналоговых каналах;
- *специальные канальные и цифровые устройства обслуживания* (DSU/CSU) для работы в цифровых выделенных каналах сетей с временны́м мультиплексированием (Time-Division Multiplexing — TDM);
- *терминальные адаптеры* (Terminal Adapter — TA) для работы в каналах цифровых сетей с интеграцией обслуживания (ISDN).

Для абонентов глобальной сети имеется стандартизованный интерфейс *пользователь — сеть* (User-to-Network Interface — UNI), в котором определены правила взаимодействия между оборудованием пользователя телекоммуникационного сервиса и сетью, предоставляющей этот сервис. Например, интерфейс BRI (Basic Rate Interface) цифровой сети ISDN в случае обычной абонентской телефонной линии позволяет одновременно передавать данные, голос, графическую и видеоинформацию со скоростью 128 Кбит/с. Для взаимодействия коммутаторов внутри глобальной сети предусмотрен интерфейс *сеть — сеть* (Network-to-Network Interface — NNI).

Стандартные интерфейсы DTE-DCE. Для подключения устройств DCE к DTE существуют стандартные интерфейсы физического уровня, позволяющие организовать передачу данных со скоростями до нескольких мегабит в секунду на небольшие расстояния (15...20 м), достаточные для удобного размещения маршрутизатора или модема.

Интерфейс RS-232C/V.24 [9] поддерживает последовательные порты (например, COM-порты) и обеспечивает асинхронную (обычно) и синхронную передачу данных со скоростями до 230 400 бит/с. Он позволяет подключить к компьютеру не только коммуникационное устройство (такое, как модем), но и другие периферийные устройства (мышь, графопостроитель). Интерфейс использует 25-контактный разъем (рис. 7.2) или в упрощенном варианте — 9-контактный разъем.

Высокоскоростной последовательный интерфейс HSSI (High-Speed Serial Interface) для синхронной связи оборудования DTE с DCE на скоростях до 52 Мбит/с может служить другим примером.

Основные типы глобальных сетей. Наиболее подходящим способом организации глобальной сети для компьютерного трафика является способ коммутации пакетов. Сеть с территориально распределенными коммутаторами пакетов обеспечивает высокую производительность при минимальной стоимости услуг.

Рис. 7.2. Сигналы интерфейса RS-232/V.24

Однако такая глобальная сеть часто оказывается недоступной для пользователя в том или ином географическом регионе. Более распространенными и доступными являются телефонные, а также первичные сети, поддерживающие услуги выделенных каналов. В связи с этим при построении глобальной (корпоративной) сети недостающие средства и компоненты можно дополнить услугами и оборудованием, арендуемыми у владельцев первичной или телефонной сети.

В зависимости от арендуемых средств различают глобальные сети, построенные с использованием выделенных каналов, коммутации каналов и коммутации пакетов [9, 13].

Выделенные каналы (Leased Channel). Такие каналы можно получить у телекоммуникационных компаний. Следует указать на две возможности использования арендуемых каналов:

1) *построение территориальной сети* (например, с использованием технологии Frame Relay), в которой выделенные линии служат для соединения промежуточных, территориально распределенных коммутаторов пакетов;

2) *соединение объединяемых ЛС* (или отдельных абонентов) с помощью выделенных линий без использования транзитных коммутаторов пакетов, работающих по технологии глобальной сети. Этот более простой способ получил название *услуги выделенных каналов*, он требует использования маршрутизаторов или удаленных мостов в объединяемых ЛС и не использует протоколы глобальных сетей (таких, как X.25 или Frame Relay). По выделенным каналам передаются те же пакеты сетевого или канального уровня, что и в ЛС. При этом гарантируется заданная пропускная способность канала между ЛС.

Существует большой выбор выделенных каналов — от аналоговых каналов тональной частоты с полосой пропускания 3,1 кГц до цифровых каналов технологии синхронной цифровой иерархии (SDH) с пропускной способностью 155, 622 Мбит/с и более.

Глобальные сети с коммутацией каналов. Для глобальных связей в корпоративной сети используют:

- традиционные аналоговые *телефонные сети* с коммутацией каналов, достоинством которых является их широкая распространенность. К недостаткам таких сетей следует отнести: низкое качество (наличие шумов и помех) составного канала, которое объясняется использованием телефонных коммутаторов устаревших моделей, работающих по принципу частотного уплотнения каналов (FDM-технологии), и большое время установления соединения, особенно при импульсном способе набора номера, характерного для нашей страны;
- *цифровые сети* с интеграцией услуг ISDN и цифровые абонентские линии DSL, полностью построенные на цифровых коммутаторах. Они свободны от многих недостатков традиционных аналоговых телефонных сетей и предоставляют пользователям высококачественные линии связи. Технологии ISDN и DSL рассмотрены в подразд. 7.7 и 7.9.

Для организации корпоративных глобальных связей сети с коммутацией каналов могут оказаться экономически неэффективными. Однако в ряде случаев телефонная сеть является единственным доступным видом связи.

Первичные сети. В первичных сетях также применяется технология коммутации каналов. Этот вид сетей широко используется для организации каналов точка—точка и отличается высокой пропускной способностью.

Выделяют три поколения технологий первичных сетей [9]:

1) плезиохронная цифровая иерархия (PDH);

2) синхронная цифровая иерархия (SDH или SONET);

3) волновое мультиплексирование (WDM).

Технологии PDH и SDH передают данные в цифровой форме и для разделения высокоскоростного канала используют *временно́е мультиплексирование*. Каждая из них поддерживает иерархию скоростей, и пользователь может выбрать подходящую скорость для канала, с помощью которого он будет строить свою *вторичную*, или *наложенную*, *сеть*. Название «наложенная сеть» говорит о том, что компьютерная или телефонная сеть пользователя как бы накладывается на первичную сеть.

Технология WDM использует разделение каналов по частоте (или длине волны) оптического излучения, предоставляя для передачи информации выделенную часть оптического диапазона, которую пользователь может задействовать по своему усмотрению, выбрав соответствующий способ кодирования или модуляции. На протяженных магистралях технология WDM вытесняет технологию SDH на периферию сети, превращая SDH в технологию сетей доступа.

Первичные сети рассматриваются в подразд. 7.2—7.4.

Глобальные сети с коммутацией пакетов. Для организации глобальных связей можно воспользоваться технологиями X.25, Frame Relay и ATM, специально разработанными для глобальных компьютерных сетей, а также услугами территориальных сетей TCP/IP, доступными в виде недорогого и очень распространенного Internet. Сведения о сетях X.25, Frame Relay и ATM приведены в подразд. 7.5, 7.6, 7.8.

Магистральные сети и сети доступа. В глобальной сети можно выделить две категории сетей: магистральные сети и сети доступа.

Магистральные сети (Backbone Wide Area Networks) используются для образования одноранговых связей (точка—точка) между крупными ЛС, которые принадлежат большим подразделениям предприятия или непосредственно связаны с коммутатором глобальной сети (см. рис. 7.1). Так как по магистральным сетям передается интенсивный трафик, они должны обеспечивать высокую пропускную способность и быть постоянно доступны.

В качестве магистральных сетей можно использовать цифровые выделенные каналы, по которым передается трафик протоколов IP, IPX или архитектуры SNA компании *IBM*, и первичные сети, а также сети с коммутацией пакетов Frame Relay, ATM, X.25 или Internet (TCP/IP).

Сети доступа представляют собой территориальные сети, предназначенные для организации удаленного доступа сотрудников предприятия (отдельных удаленных компьютеров) или для связи ЛС с магистральной сетью. В качестве отдельных удаленных

узлов могут также выступать банкоматы или кассовые аппараты, требующие доступа к центральной базе данных для получения информации о легальных клиентах банка, пластиковые карточки которых необходимо авторизовать на месте.

7.2. СЕТИ ПЛЕЗИОХРОННОЙ ЦИФРОВОЙ ИЕРАРХИИ

Сети плезиохронной цифровой иерархии (Plesiochronous Digital Hierarchy — PDH) появились в США как альтернатива телефонным линиям связи с частотным уплотнением (FDM), которые исчерпали свои возможности по организации высокоскоростной многоканальной связи по одному кабелю. Появлению PDH сопутствовала разработка мультиплексора T-1. В его функции входило оцифровывание речевого сообщения с частотой 8 000 Гц и кодирование по способу импульсно-кодовой модуляции. Мультиплексор позволял в цифровом виде объединять, передавать и коммутировать речевой трафик 24 абонентов. При этом каждый абонентский канал представлял собой цифровой поток данных 64 Кбит/с, а групповой первичный канал, объединяющий 24 абонентских канала, имел скорость передачи 1,544 Мбит/с. Для более гибкого соединения телефонных станций использовалась *иерархия скоростей*, основанная на объединении первичных каналов. В Европе первичный канал PDH объединял 30 абонентских каналов и имел скорость передачи 2 048 Кбит/с. В результате появились несовместимые американская и европейская версии стандарта PDH (табл. 7.1). Для иерархии скоростей принято использовать общее обозначение DS-N (Digital Signal N). Отметим, что несовпадение приведенных в табл. 7.1 значений скоростей ($64 \cdot 24 \neq 1\,544$ или $64 \cdot 30 \neq 2\,048$) обусловлено наличием дополнительных служебных битов. Например, канал E1 со скоростью передачи 2,048 Мбит/с состоит из 30 каналов DS-0 и двух дополнительных каналов 64 Кбит/с, несущих управляющую информацию.

На практике в основном используются каналы T1/E1 и T3/E3.

Системы T-каналов позволяют передавать не только речевые сообщения, но и любые цифровые данные. С середины 1970-х гг. выделенные каналы стали сдаваться телефонными компаниями в аренду на коммерческих условиях, перестав быть их внутренней технологией.

Один из недостатков технологии PDH обусловлен необходимостью выполнения операций полного демультиплексирования и

Таблица 7.1

Общее обозначение	Америка			Европа		
	Обозначение и число каналов		Скорость, Мбит/с	Обозначение и число каналов		Скорость, Мбит/с
DS-0	—	1	64 Кбит/с	—	1	64 Кбит/с
DS-1	T1	1 · 24 = 24	1,544	E1	1 · 30 = 30	2,048
DS-2	T2	24 · 4 = 96	6,312	E2	30 · 4 = 120	8,488
DS-3	T3	96 · 7 = 672	44,736	E3	120 · 4 = 480	34,368
DS-4	T4	672 · 6 = 4 032	274,176	E4	480 · 4 = 1 920	139,264

мультиплексирования группового канала при выделении требуемого абонентского канала. Например, чтобы выделить один E1 из канала E4, нужно выполнить полное демультиплексирование: E4 разобрать на четыре E3, далее из одного E3 извлечь E2 и, наконец, требуемый E1 извлечь из одного E2, а затем все остальное собрать обратно (рис. 7.3).

К другим недостаткам PDH следует отнести низкие по современным меркам скорости передачи данных, ограниченные для европейского стандарта 139 Мбит/с (см. табл. 7.1), и то, что в технологии PDH не предусмотрены встроенные средства обеспечения отказоустойчивости и администрирования сети. Для устранения указанных недостатков были разработаны синхронные сети.

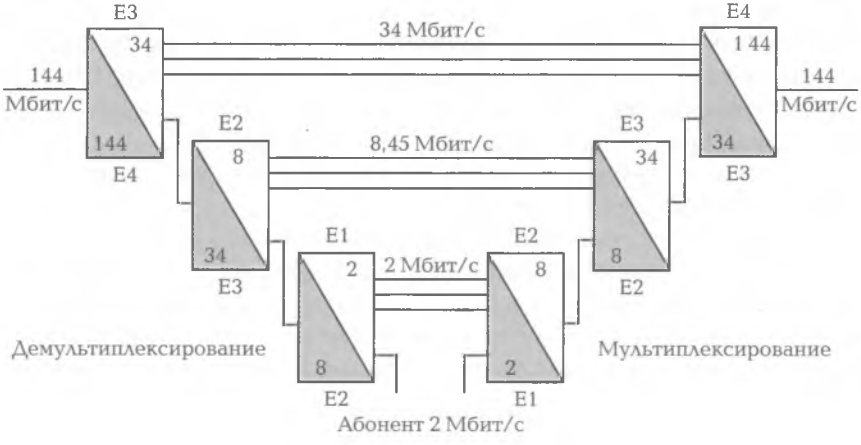


Рис. 7.3. Выделение одного канала E1 из E4

7.3. СИНХРОННЫЕ СЕТИ SONET/SDH

Особенности сетей. Основные цели, которые ставили разработчики синхронных оптических сетей, — создание технологии, способной передавать трафик всех существующих цифровых каналов уровня PDH (как европейских E1—E4, так и американских T1—T3) по высокоскоростной магистральной сети на базе волоконно-оптических кабелей, продолжив иерархию скоростей, заложенную в технологии PDH, до скорости в несколько гигабит в секунду.

Результатом работы явились две разновидности синхронных сетей с иерархией скоростей каналов (табл. 7.2).

1. *Синхронные оптические сети* (Synchronous Optical NET — SONET), стандартизованные ANSI. В сетях SONET *оптические каналы* обозначаются OC-N (Optical Carier level N — оптоволоконная линия связи уровня *N*), а *электрические* — STS-N (Synchronous Transport Signal level N — синхронный транспортный сигнал уровня *N*). Здесь *N* — кратность базовой скорости, которая для SONET составляет 51,84 Мбит/с.

2. *Сети синхронной цифровой иерархии* (Synchronous Digital Hierarchy — SDH), определенные спецификациями ITU-T G.707-G.709. В SDH каналы обозначаются как STM-N (Synchronous Transport Module level N — синхронный транспортный модуль уровня *N*). Здесь *N* — кратность базовой скорости, которая для SDH составляет 155,52 Мбит/с.

Сети SDH и SONET совместимы и могут мультиплексировать входные потоки как европейского (SDH), так и американского (SONET) стандартов.

Аппаратные средства. Основными устройствами в сетях SONET/SDH являются мультиплексоры (Multiplexer). Каждый мультиплексор оснащен двумя типами портов: портами *ввода-вывода* и *линейными* (агрегатными) портами, соединяющими мультиплексоры с магистралью. В зависимости от расположения в сети различают мультиплексоры:

- *терминальные* (Terminal Multiplexers — TM), включенные на концах магистрали. Они принимают данные от терминальных устройств и мультиплексируют потоки кадров разных скоростей STS-n в кадры более высокой иерархии STS-m, а также выполняют обратные операции. Каждый терминальный мультиплексор оснащен одним линейным портом и большим числом портов ввода-вывода;

Таблица 7.2

SDH	SONET	Скорость
—	STS-1, OC-1	51,84 Мбит/с
STM-1	STS-3, OC-3	155,520 Мбит/с
STM-3	OC-9	466,560 Мбит/с
STM-4	OC-12	622,080 Мбит/с
STM-6	OC-18	933,120 Мбит/с
STM-8	OC-24	1,244 Гбит/с
STM-12	OC-36	1,866 Гбит/с
STM-16	OC-48	2,488 Гбит/с
STM-64	OC-192	9,953 Гбит/с
STM-256	OC-768	39,81 Гбит/с

- *ввода-вывода* (Add-Drop Multiplexers — ADM), которые могут принимать и передавать транзитом поток со скоростью STS-N, а также выводить (без полного демультиплексирования) или вводить на ходу пользовательские данные низкоскоростных портов ввода-вывода.

Мультиплексор может содержать несколько портов ввода-вывода SDH и PDH. Для приема (передачи) пользовательских данных от низкоскоростных каналов технологии PDH (E1/T1, E3/T3) и преобразования их в кадры STS-N используются терминальные устройства (Terminal — T) или сервисные адаптеры (Service Adapter — SA).

Топология сетей. Базовыми топологиями сетей SDH являются кольцевая топология и линейная цепь.

Сеть с кольцевой топологией (рис. 7.4, *а*) строится на основе мультиплексоров ввода-вывода, имеющих по два линейных порта, и кабеля с двумя или четырьмя (для повышения надежности и пропускной способности) оптическими волокнами. Пользовательские потоки данных вводятся в кольцо и выводятся из кольца через порты ввода-вывода, образуя двухточечные соединения (на рис. 7.4, *а* показаны два таких соединения).

Линейная цепь (рис. 7.4, *б*) состоит из мультиплексоров обоих типов, при этом два оконечных мультиплексора являются терми-

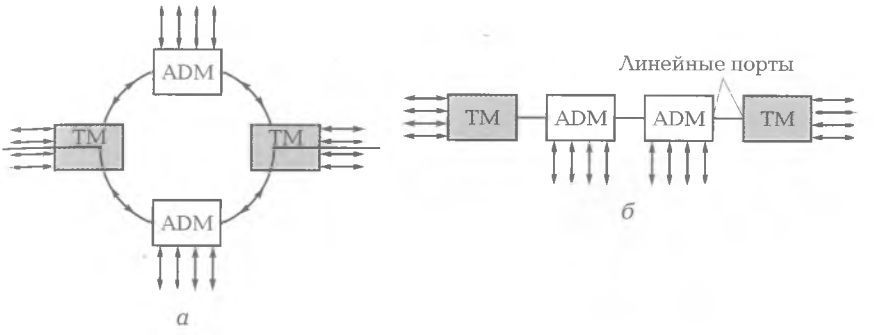


Рис. 7.4. Базовые топологии:
а — кольцевая цепь; *б* — линейная цепь

нальными (TM), а остальные — мультиплексорами ввода-вывода (ADM).

На основе базовых топологий строятся сложные разветвленные сети SDH с ячеистой, радиально-кольцевой топологией, кольцо — кольцо и др. При ячеистой топологии мультиплексоры соединяются друг с другом большим количеством связей, благодаря чему повышается производительность и надежность сети.

Формат кадра STM-1. Кадры STM-N позволяют объединять (агрегировать) потоки синхронной (SDH) и плезиохронной (PDH) цифровой иерархии в общий магистральный поток, а также выполнять операции ввода-вывода без полного демультиплексирования магистрального потока. Они имеют достаточно сложную

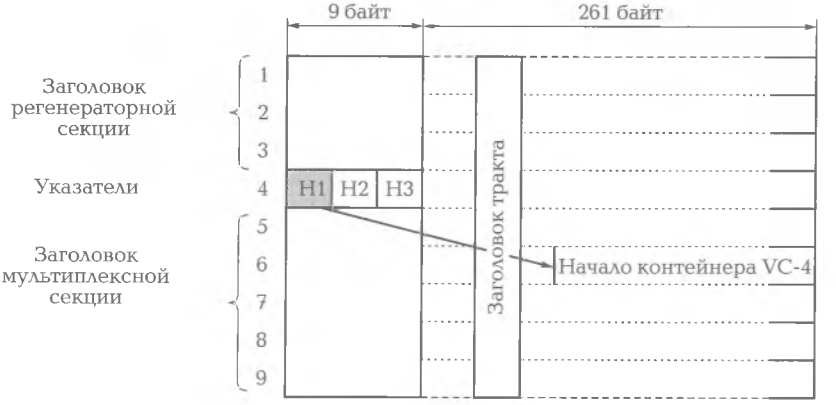


Рис. 7.5. Формат кадра STM-1

структуру, которую представляют в виде матрицы. Рассмотрим формат кадр STM-1, который можно представить в виде матрицы 270 × 9 байт. В каждой строке матрицы (рис. 7.5):

- первые 9 байт отводятся под служебные данные заголовков;
- 260 байт занимает полезная нагрузка (данные таких структур, как AUG, AU, TUG, TU и VC);
- один байт предназначен для заголовка тракта, который используется для указания местоположения виртуальных контейнеров внутри кадра, если кадр переносит низкоскоростные данные пользовательских каналов типа E1/T1.

Строки 1—3 служебных данных являются *заголовком регенераторной секции* RSOH (Regenerator Start Of Header), включающим в себя синхробайты, байты контроля ошибок и другие данные, необходимые для контроля и реконфигурации секции. Строки 5—9 отведены под *заголовок мультиплексной секции* MSOH (Multiplex Start Of Header), который используется для реконфигурации, контроля и управления линией. В заголовке MSOH содержатся байты контроля ошибок для мультиплексной секции, два байта для автоматической защиты трафика, обеспечивающего живучесть сети; байт передачи сообщений статуса системы синхронизации и др. В строке 4 помещены 3-байтные *указатели* H1, H2, H3 (Pointers), которые задают положение начала виртуального контейнера VC-4 или трех виртуальных контейнеров VC-3. С помощью указателей обеспечивается синхронная передача байт кадров с асинхронным характером вставляемых и удаляемых пользовательских данных. Указатели позволяют задавать и изменять местоположение виртуальных контейнеров.

Мультиплексирование и ввод-вывод. Эти операции в сетях SDH выполняются с помощью виртуальных контейнеров. Существуют правила, по которым контейнеры объединяются в группы. Схема, иллюстрирующая принцип объединения контейнеров (или мультиплексирования) для получения кадра STM-N, приведена на рис. 7.6 [9]. Структурные единицы кадра SDH, содержащие указатели, заштрихованы. Связь между контейнерами и блоками, допускающая сдвиг данных по фазе, показана цветной стрелкой.

Как видно из рис. 7.6, виртуальные блоки (Virtual Container — VC-2, VC-3, VC-11, VC-12) помещаются в трибутарные блоки (Tributary Unit — TU-2, TU-3, TU-11, TU-12). При этом имеется возможность их сдвига в некоторых пределах. Затем строятся административные блоки (Administrative Unit — AU-3, AU-4). Группа из *N* административных блоков (Administrative Unit Group — AUG) об-

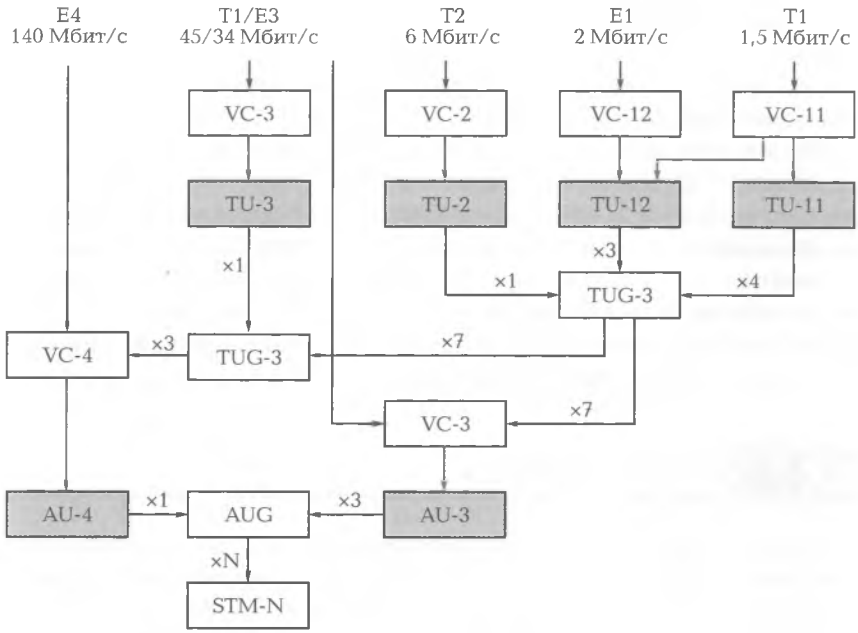


Рис. 7.6. Мультиплексирование данных SDH:

⟶ — связи, допускающие сдвиг данных; ▭ — узлы, содержащие указатели

разует полезную нагрузку (данные) кадра STM-N. На каждом шаге преобразования к предыдущим данным добавляется несколько служебных байтов, которые помогают распознать структуру блока или группы блоков и затем определить с помощью указателей начало пользовательских данных.

Схема мультиплексирования SDH предоставляет разнообразные возможности по объединению пользовательских потоков PDH. Например, для кадра STM-1 можно использовать один поток E4 или 63 потока E1 ($E1 \times 3 \times 7 \times 3$).

Отказоустойчивость сети. В архитектуру сетей SDH заложен разнообразный набор средств отказоустойчивости, позволяющий восстановить работоспособность сети в случае отказа линии связи, порта, мультиплексора или какого-либо другого ее элемента. Основным механизмом поддержки отказоустойчивости в сетях является автоматическое защитное переключение (Automatic Protection Switching — APS), при котором в случае отказа основного элемента автоматически осуществляется переход на резервный элемент. Сети, поддерживающие такой механизм, называют *само-*

восстанавливающимися. В сетях SDH используются три способа защиты:

1) защита 1 + 1, при которой резервный элемент выполняет те же функции, что и основной;

2) защита 1 : 1, когда защитный элемент начинает выполнять функции защищаемого элемента только в случае его отказа. В нормальном режиме он функции не выполняет, а переключается на них;

3) защита 1 : N, основанная на выделении одного защитного элемента на N защищаемых. В случае отказа одного из защищаемых элементов его функции начинает выполнять защитный, при этом остальные элементы остаются без защиты до тех пор, пока не будет заменен отказавший элемент.

7.4. СЕТИ DWDM

Общие сведения. Для организации магистральных каналов в оптоволоконных сетях нашел эффективное применение *принцип мультиплексирования с разделением частот* (Wave Division Multiplexing — WDM). В качестве средства доставки используются электромагнитные колебания инфракрасного диапазона частот от 196 до 350 ТГц (длины волн от 850 до 1 565 нм). В одном скоростном магистральном канале обычно мультиплексируется 16, 32, 40, 80 или 160 низкоскоростных каналов. Техника мультиплексирования с числом каналов 16 и более называется *уплотненным волновым мультиплексированием с разделением* (Dense Wave Division Multiplexing — DWDM). Название связано с тем, что технология использует существенно меньшее расстояние между частотами соседних несущих колебаний (волн), чем в WDM. Согласно рекомендациям G.692 определены два набора таких частот, или *частотных плана*: частотный план с разнесением частот между соседними каналами 100 ГГц ($\Delta\lambda \approx 0{,}8$ нм), в соответствии с которым для передачи данных применяется 41 волна в диапазоне от 196,1 ТГц (1 528,77 нм) до 192,1 ТГц (1 560,61 нм), и частотный план с шагом 50 ГГц ($\Delta\lambda \approx 0{,}4$ нм), позволяющий в этом же диапазоне передавать 81 длину волны (почти в два раза больше).

Разработано оборудование для *высокоуплотненного волнового мультиплексирования* (High-Dense WDM — HDWDM), способное работать с шагом 25 ГГц. В настоящее время ведутся работы по повышению скорости передачи информации на одной длине волны до 40...80 Гбит/с [9]. Современные устройства DWDM могут также коммутировать отдельные волны.

Главная особенность DWDM — очень высокая общая пропускная способность сети, достигающая нескольких терабит в секунду. Операции мультиплексирования и коммутации в сетях над световыми сигналами в отличие от других технологий (например, Gigabit Ethernet) выполняются без преобразования их в электрическую форму.

Аппаратные средства DWDM-сетей. В их число входят волоконно-оптические усилители, оптические мультиплексоры ввода-вывода и оптические кросс-коннекторы.

Волоконно-оптические усилители. Они непосредственно усиливают световые сигналы в диапазоне 1 550 нм, обеспечивая протяженность участка между ними 150 км и более, а длину мультиплексной секции — 600...3 000 км.

Оптические мультиплексоры ввода-вывода (Optical Add-Drop Multiplexers — OADM). При *вводе* мультиплексор OADM выполняет операцию сложения (смешения) нескольких сигналов разных частот (длин волн) для передачи по линии связи, при *выводе* выделяет сигнал с требуемой частотой. Для выделения волн могут использоваться разные оптические механизмы. При небольшом количестве сигналов применяются *тонкопленочные фильтры*, состоящие из пластин с многослойным покрытием. В качестве пластин используется торец оптического волокна, скошенный под углом 30...45°, с нанесенными на него слоями покрытий.

Оптические кросс-коннекторы (Optical Cross-Connect — OCC). В отличие от мультиплексоров крос-коннекторы не только добавляют волны в общий транзитный сигнал и выводят их оттуда, но и поддерживают произвольную коммутацию между оптическими сигналами, передаваемыми волнами разной длины. Такая способность кросс-коннекторов позволяет направить любую из волн входного сигнала каждого порта в любой из выходных портов. Микроэлектронная механическая система кросс-коммутации (Micro-Electro Mechanical Systems — MEMS), представляющая собой набор подвижных микрозеркал с диаметром менее 1 мм, приведена на рис. 7.7. За счет поворота микрозеркала на заданный угол исходный луч определенной волны направляется в соответствующее выходное волокно. Затем все лучи мультиплексируются в общий выходной сигнал.

Топология сетей. Впервые технология DWDM применена для построения сверхдальних высокоскоростных магистралей с *топологией двухточечной цепи*. В конечных точках такой магистрали устанавливались терминальные мультиплексоры DWDM, а в про-

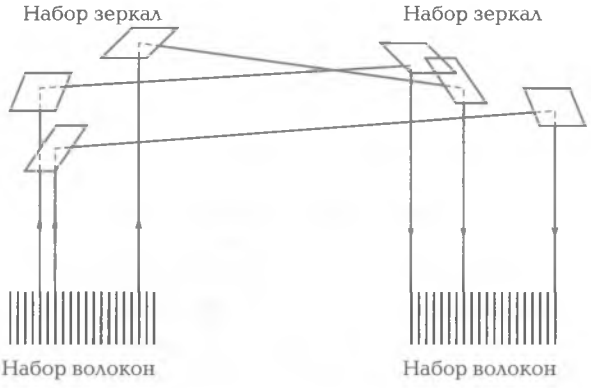


Рис. 7.7. Принцип кросс-коммутации

межуточных точках — оптические усилители. В схеме для дуплексного обмена между абонентами используется однонаправленная передача всего набора волн по двум волокнам (рис. 7.8). Возможен вариант работы магистрали DWDM с использованием одного волокна, когда одна половина волн частотного плана передает информацию в одном направлении, другая половина — в обратном.

Дальнейшим развитием двухточечной топологии является *цепь с использованием мультиплексоров* ввода-вывода OADM, которые позволяют соединиться с одним из абонентов (рис. 7.9). Для этого

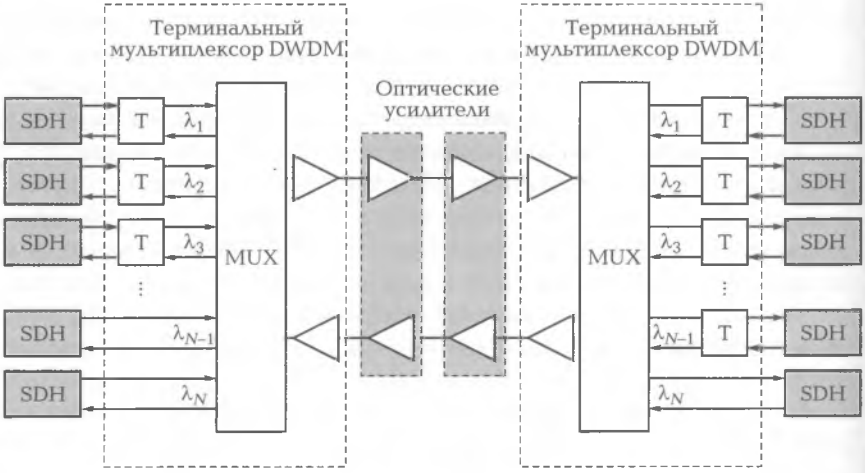


Рис. 7.8. Сверхдальняя DWDM-магистраль

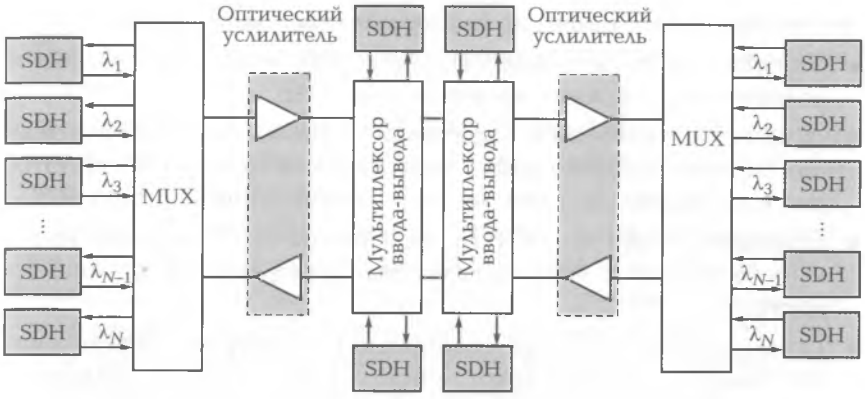


Рис. 7.9. Ввод-вывод в сети DWDM

из мультиплексора выводится сигнал с определенной длиной волны и вводится туда сигнал такой же длины волны.

При *кольцевой топологии* с использованием двух путей (основного и резервного) обеспечивается живучесть сети DWDM. В конечном узле мультиплексор сравнивает два сигнала и выбирает сигнал лучшего качества (или заданный по умолчанию). *Ячеистая топология* обеспечивает бóльшие гибкость, производительность и отказоустойчивость, чем остальные топологии. Для организации таких сетей используются оптические кросс-коннекторы, которые поддерживают произвольную коммутацию отдельных частотных каналов.

7.5. СЕТИ X25

Особенности сети. Появившаяся в 1970-е гг. сеть X.25 относится к одной из первых глобальных общественных сетей передачи данных. В то время для передачи данных можно было использовать только телефонную сеть. Соединение двух компьютеров устанавливалось с помощью телефонного звонка. Ему присваивался уникальный номер, по которому определялось место назначения передаваемых пакетов. В сети X.25 одновременно могло быть много соединений. Посылаемые пакеты содержали трехбайтный заголовок, после которого следовало поле данных размером до 128 байт. Заголовок состоял из 12-битного номера соединения, порядкового номера пакета, номера для подтверждения доставки и еще некоторой служебной информации.

Особенности сети X.25 состоят в том, что сеть:

- основана на коммутации пакетов между конечными узлами и реализует три нижних уровня модели OSI;
- гарантирует целостность доставки данных, при этом высокая надежность обеспечивается избыточными связями коммутаторов и возможностью динамического изменения маршрутов;
- стандартизована (с 1974 г.), протоколы X.25 поддерживают многие мосты и маршрутизаторы (контроллеры удаленного доступа);
- применяется для обмена сообщениями между пользователями, построения распределенных систем клиент-сервер, подключения терминальных узлов (кассовых аппаратов, банкоматов и др.), связи между собой локальных сетей и других задач.

Недостатком сетей являются значительные задержки передачи пакетов, не позволяющие использовать их для голосовой связи.

Структура и состав сети. В состав сети X.25 входят (рис. 7.10):

- *коммутаторы пакетов* (Packet Switching Exchange — PSE), соединенные высокоскоростными выделенными цифровыми или аналоговыми линиями, которые и образуют непосредственно глобальную сеть;

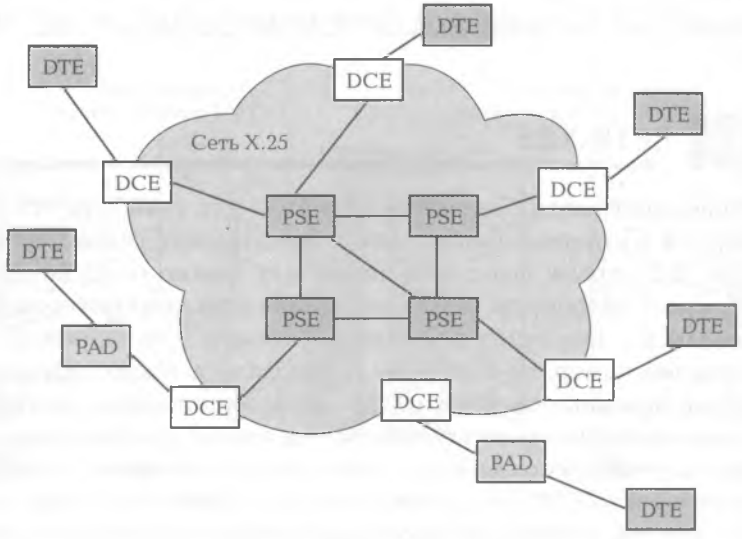


Рис. 7.10. Структура сети X.25

- *телекоммуникационное оборудование* (Data Circuit-terminating Equipment — DCE), например модемы, обеспечивающее доступ к сети;
- *аппаратура передачи данных* (Data Terminal Equipment — DTE), в том числе терминалы, компьютеры и другое оконечное оборудование пользователей;
- *сборщики-разборщики пакетов* (Packet Assembler/Disassembler — PAD), предназначенные для доступа абонентов в сеть с коммутацией пакетов. Используются для терминалов, не поддерживающих в полном объеме функциональности X.25. Их функции: перед отправкой разбивают потоки данных на пакеты, а при получении восстанавливают из пакетов потоки данных.

Адресация в сети. В автономной сети X.25 максимальная длина поля адреса в пакете составляет 16 байт. Администратор может назначать произвольные адреса в пределах поля адреса.

При обмене данными с другими сетями X.25 адресация узлов DTE осуществляется в соответствии с рекомендациями X.121, обеспечивающими единое адресное пространство в мировом масштабе. Используются три разновидности адресов:

1) *полный международный сетевой*, который начинается с префикса «0», за ним следует трехзначный код страны (250 — Россия), затем номер сети в стране (один знак) и номер узла (до 10 цифр);

2) *полный международный телефонный*, начинающийся с префикса 9, за которым следует трехзначный код страны, а затем телефонный номер в стране (до 11 цифр);

3) *внутренний сетевой*, состоящий из номера сети в стране и номера узла (до 10 цифр).

Стек протоколов сети. Стандарты сетей X.25 описывают три уровня протоколов: физический, канальный и сетевой.

На физическом уровне соответствующими протоколами определены интерфейсы оборудования передачи данных. Для линии связи протокол не оговорен, можно использовать разные стандарты.

На канальном уровне сеть X.25 обеспечивает гарантированную доставку, целостность данных и контроль потока. Обычно используется протокол сбалансированного доступа к линии связи (Link Access Protocol-Balanced — LAP-B), при котором оба участвующих в соединении узла равноправны. Протокол LAP-B ориентирован на соединение и для надежной передачи кадров между двумя непосредственно соединенными устройствами использует *алгоритм скользящего окна*. Окно имеет фиксированный

- *телекоммуникационное оборудование* (Data Circuit-terminating Equipment — DCE), например модемы, обеспечивающее доступ к сети;
- *аппаратура передачи данных* (Data Terminal Equipment — DTE), в том числе терминалы, компьютеры и другое оконечное оборудование пользователей;
- *сборщики-разборщики пакетов* (Packet Assembler/Disassembler — PAD), предназначенные для доступа абонентов в сеть с коммутацией пакетов. Используются для терминалов, не поддерживающих в полном объеме функциональности X.25. Их функции: перед отправкой разбивают потоки данных на пакеты, а при получении восстанавливают из пакетов потоки данных.

Адресация в сети. В автономной сети X.25 максимальная длина поля адреса в пакете составляет 16 байт. Администратор может назначать произвольные адреса в пределах поля адреса.

При обмене данными с другими сетями X.25 адресация узлов DTE осуществляется в соответствии с рекомендациями X.121, обеспечивающими единое адресное пространство в мировом масштабе. Используются три разновидности адресов:

1) *полный международный сетевой*, который начинается с префикса «0», за ним следует трехзначный код страны (250 — Россия), затем номер сети в стране (один знак) и номер узла (до 10 цифр);

2) *полный международный телефонный*, начинающийся с префикса 9, за которым следует трехзначный код страны, а затем телефонный номер в стране (до 11 цифр);

3) *внутренний сетевой*, состоящий из номера сети в стране и номера узла (до 10 цифр).

Стек протоколов сети. Стандарты сетей X.25 описывают три уровня протоколов: физический, канальный и сетевой.

На физическом уровне соответствующими протоколами определены интерфейсы оборудования передачи данных. Для линии связи протокол не оговорен, можно использовать разные стандарты.

На канальном уровне сеть X.25 обеспечивает гарантированную доставку, целостность данных и контроль потока. Обычно используется протокол сбалансированного доступа к линии связи (Link Access Protocol-Balanced — LAP-B), при котором оба участвующих в соединении узла равноправны. Протокол LAP-B ориентирован на соединение и для надежной передачи кадров между двумя непосредственно соединенными устройствами использует *алгоритм скользящего окна*. Окно имеет фиксированный

размер в 8 или 128 кадров и не может изменяться динамически. Согласно протоколу нумеруются не байты, а кадры. По протоколу LAP-B также обычно устанавливаются соединения на канальном уровне между непосредственно связанными коммутаторами сети.

Сетевой уровень реализуется пакетным протоколом (Packet-Layer Protocol — PLP), который управляет обменом кадрами через виртуальные цепи и определяет следующие режимы:

- *установление соединения* (Call Setup), используемый для организации коммутируемой виртуальной цепи между аппаратурой передачи данных DTE. Для постоянных виртуальных цепей режим не используется;
- *передача данных* (Data-Transfer Mode), в котором выполняются сегментация, заполнение недостающих битов (Padding), контроль ошибок и управление потоком. Режим используется при обмене данными для всех виртуальных цепей (PVC и SVC);
- *пауза* (Idle Mode), используемый в коммутируемых виртуальных цепях после установления соединений до начала обмена данными;
- *сброс соединения* (Call-Clearing Mode), предназначенный для разрыва конкретной коммутируемой виртуальной сети SVC при завершении сеанса;
- *рестарт* (Restarting Mode), используемый для синхронизации передачи между аппаратурой передачи данных DTE и локальным DCE. В этом режиме все устройства передачи данных DTE, подключенные к данному телекоммуникационному оборудованию DCE, должны установить виртуальные цепи.

Отличием технологии X.25 от рассматриваемых далее технологий Frame Relay и ATM является то, что после установления виртуального канала данные передаются протоколом сетевого, а не канального уровня.

7.6. СЕТИ FRAME RELAY

Общие сведения. В 1980-е гг. на смену X.25 пришла технология ретрансляции кадров (Frame Relay), на основе которой была построена сеть без контроля ошибок и передачи, с ориентацией на установление соединения, сохраняющего последовательность доставки пакетов. Эти свойства сделали Frame Relay похожей на *глобальную* по охвату и *локальную* по принципу действия сеть.

Основные особенности сетей Frame Relay заключаются в следующем:

а) сеть является упрощенным вариантом сетей с *коммутацией пакетов*, ориентированным на использование цифровых линий связи со скоростью до 2 Мбит/с;

б) технология Frame Relay охватывает два нижних уровня модели OSI — *физический* и *канальный*;

в) сеть имеет *интерфейс пользователя* UNI (User-to-Network Interface) — синхронный порт со скоростью 9,6...64 Кбит/с (и выше), а также *межсетевой интерфейс* NNI (Network-to-Net-work Interface), использующий высокопроизводительные цифровые каналы;

г) сеть позволяет передавать пакеты в пункты назначения, определяемые адресным полем. Список возможных путей пересылки формируется провайдером услуг сети. Согласно этому списку до начала работы осуществляется конфигурирование линий;

д) сеть *обеспечивает* установление постоянных виртуальных цепей PVC (Permanent Virtual Circuit) или же коммутируемых соединений SVC (Switched Virtual Circuit);

е) сеть *не обеспечивает* гарантированной доставки, целостности данных и контроля потока (пакеты в сети могут искажаться и теряться), что обусловлено отсутствием промежуточной буферизации;

ж) Frame Relay относят к технологии *канального уровня*, поскольку основное внимание уделяется процедурам передачи пользовательских данных, а не процедурам установления виртуального канала, которые выполняются с привлечением протокола *сетевого уровня*;

з) сети Frame Relay гораздо лучше подходят для передачи *пульсирующего трафика* ЛС по сравнению с сетями X.25 (при использовании волоконно-оптических кабелей);

и) технология Frame Relay обеспечивает гарантированную поддержку основных показателей качества транспортного обслуживания (QoS) локальных сетей — средней скорости передачи данных по виртуальному каналу при допустимых пульсациях трафика.

Технология Frame Relay в основном применяется для маршрутизации протоколов ЛС (IPX и TCP/IP) через общие (Public) коммуникационные сети при создании виртуальных каналов. Она может использоваться для передачи асинхронного трафика и даже голоса. Главная привлекательность — низкая цена.

Протоколы. Стандарты Frame Relay определяют два типа виртуальных каналов: *постоянные* (PVC), по которым трафик передает-

ся почти всегда, и *коммутируемые* (SVC), которые нужны для кратковременной работы (на несколько часов в месяц).

На физическом уровне сеть Frame Relay может использовать линии связи асинхронной и синхронной цифровой иерархии PDH/SDH или ISDN.

Протокол канального уровня LAP-F определяет в сетях Frame Relay два режима работы. В *основном режиме* кадры передаются без преобразования и контроля (не передаются квитанции подтверждения между коммутаторами на каждый пользовательский кадр), благодаря чему сети обладают весьма высокой производительностью. В *управляющем режиме* осуществляется контроль доставки кадров и управления потоком. Оба режима обеспечивают передачу кадров между двумя соседними коммутаторами.

Формат кадра. Кадр протокола LAP-F содержит два флага-разделителя начала и конца пакета, поле заголовка (адреса), поле данных длиной до 4 Кбайт и двухбайтное поле CRC контроля с помощью циклического избыточного кода (рис. 7.11, *а*). Мультиплексирование кадров осуществляется по двум-четырем байтам заголовка (рис. 7.11, *б*), следующего за флагом-разделителем начала пакета. Поля и биты кадра используются протоколом в качестве идентификатора соединения канала данных, для управления трафиком, для поддержания заданного качества обслуживания виртуального канала, индикации перегрузки сети и других целей.

Поддержка качества обслуживания. Технология Frame Relay обеспечивает качество транспортного обслуживания по наборам следующих параметров:

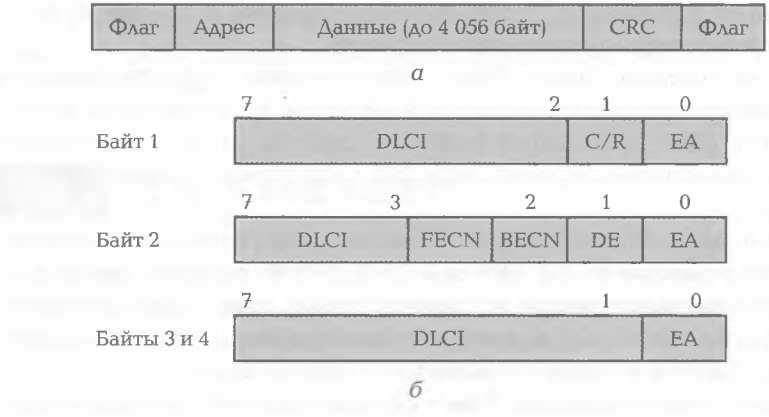


Рис. 7.11. Формат кадра LAP-F (*а*) и заголовка пакета Frame Relay (*б*)

- *согласованная скорость передачи данных* (Committed Information Rate — CIR), представляющая собой скорость, с которой сеть должна передавать данные пользователя;
- *согласованная величина пульсации* (Committed Burst Size — *Bc*), определяемая максимальным количеством байтов, которое передаст сеть от данного пользователя за интервал времени *T* с заданной согласованной скоростью CIR;
- *дополнительная величина пульсации* (Excess Burst Size — *Be*) определяемая максимальным количеством байтов, которое пытается передать сеть сверх установленного значения *Bc* за интервал времени *T*.

7.7. СЕТИ ISDN

Цифровая сеть связи с комплексными услугами (Integrated Services Digital Network — ISDN) является первым широкомасштабным проектом по созданию всемирной универсальной сети, предоставляющей все основные виды услуг телефонных сетей и сетей передачи данных.

Интерфейсы ISDN обеспечивают подключение оборудования различных классов: телефонов, факсов, аппаратуры видеоконференцсвязи, телекоммуникационных и других устройств. Услуги (сервисы) сетей выглядят как традиционные аналоговые, однако благодаря цифровому каналу обеспечивают более высокие качество и надежность, а также многие дополнительные возможности. Через линии ISDN могут соединяться учрежденческие мини-АТС, обеспечивая единую телефонную сеть организации, разбросанной по всему миру.

Большинство телефонных компаний предлагают услуги ISDN с двумя интерфейсами *доступа*.

1. *Базовый интерфейс* (Basic Rate Interface — BRI). Предназначен для индивидуальных пользователей и состоит из двух B-каналов (от *bearer* — однонаправленный) на 64 Кбит/с, переносящих данные, и одного управляющего канала (дельта-канала, или D-канала) на 16 Кбит/с. При объединении (2B + D) каналов можно одновременно передавать данные, голос, графическую и видеоинформацию со скоростью 128 Кбит/с. Интерфейс чаще всего устанавливается на обычных телефонных станциях, в небольших организациях.

2. *Первичный интерфейс* (Primary Rate Interface — PRI). Предназначен для пользователей с большими потребностями. Американ-

ский интерфейс состоит из 23 B-каналов на 64 Кбит/с и одного D-канала на 64 Кбит/с. При объединении (23 B + D) каналов суммарная пропускная способность составляет 64 · 23 + 64 = 1 536 Кбит/с. Для Европы (и России) PRI = 64 · 30 + 64 = 1 984 Кбит/с. Интерфейс используется для цифровой передачи голоса в частных телефонных станциях (Private Branch eXchange — PBX).

Абоненты сервиса BRI могут пользоваться следующими типами интерфейса:

- *U-интерфейс линейных окончаний* — обеспечивает полный дуплекс с помощью витой пары, проложенной от абонента к коммутатору. К U-интерфейсу может подключаться только одно устройство NT1 (Network Termination) — сетевое окончание;
- *двухточечный T-интерфейс* — служит для подключения к NT1 устройств, рассчитанных на монопольное использование абонентской линии ISDN;
- *шинный S-интерфейс* (или S/T) — служит для подключения ISDN-устройств TE1 (Terminal Equipment) разных типов (телефонов, факсов, мостов (маршрутизаторов), терминальных адаптеров и др.).

Пользователь от провайдера (или телефонной компании) получает один из интерфейсов [2], характеристики которых приведены в табл. 7.3.

Коммутатор ISDN имеет два типа интерфейсов (рис. 7.12):

1) *U-интерфейсы линейных окончаний* (Line Termination), обращенные к пользователям.

Таблица 7.3

Показатель	BRI U-интерфейс	BRI S-интерфейс	T1 PRI (США, Япония)	E1 PRI (Европа и Россия)
B-каналы, Кбит/с	2 × 64	2 × 64	23 × 64	30 × 64
D-каналы, Кбит/с	1 × 16	1 × 16	1 × 64	1 × 64
Синхронизация, Кбит/с	16	48	8	64
Суммарный поток, Кбит/с	160	192	1 544	2 048
Способ кодирования	2B1Q/4B3T	ASI (MAMI)	AMI/ B8ZS	HDB3

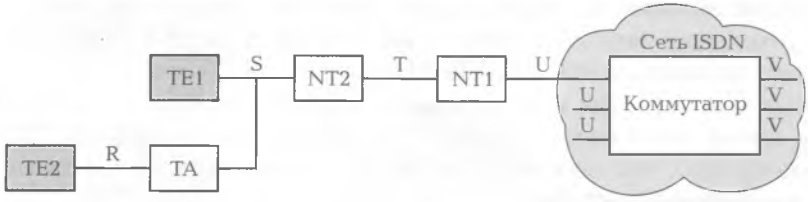


Рис. 7.12. Интерфейсы ISDN

2) *V-интерфейс для соединения с другими коммутаторами* (Exchange Termination). Этот интерфейс использует владелец сети (провайдер услуг) ISDN.

7.8. СЕТИ ATM

Общие сведения. Технология с асинхронным режимом передачи (Asynchronous Transfer Mode — ATM) должна была обеспечивать:

- передачу компьютерного и мультимедийного трафика (голос, видео, управление — в реальном времени) с высоким качеством обслуживания (QoS);
- скорость передачи данных от десятков мегабит до нескольких гигабит в секунду;
- возможность использования имеющихся линий связи и взаимодействия с протоколами локальных и глобальных сетей (IP, Ethernet, ISDN).

Бóльшая часть поставленных целей была достигнута, и с середины 1990-х гг. ATM нашла практическое применение в основном в глобальных и локальных *магистралях*.

Основные особенности ATM:

а) одним из главных свойств ATM, которое отличает ее от других технологий, является комплексная поддержка параметров качества обслуживания QoS для всех основных видов трафика;

б) сеть ATM имеет классическую иерархическую структуру крупной территориальной сети — оконечные устройства соединяются индивидуальными линиями связи с коммутаторами нижнего уровня, которые, в свою очередь, соединяются с коммутаторами более высоких уровней;

в) соединение пользователя с сетью ATM может быть прямым или по требованию. Соединение между двумя сетевыми компью-

терами называется *виртуальным каналом*. Существует два типа виртуальных каналов: *постоянный* PVC (Permanent Virtual Circuit) и *переключаемый* SVC (Switched Virtual Circuit). В отличие от Frame Relay или X.25, где виртуальные каналы устанавливаются только на время соединения, в сетях ATM используются предопределенные каналы, что служит одним из факторов высокого быстродействия технологии ATM;

г) данные разбиваются на части с фиксированной длиной по 53 байт, которые называются *ячейками*. Коммутацию ячеек выполняет оборудование ATM (в сетях Frame Relay — программное обеспечение). Для заголовка ATM, содержащего адресную формацию, используется 5 байт. Одновременно передавать по сети голос, данные и видео позволяет мультиплексирование сигналов. Стандартные скорости передачи ATM: 25, 155, 520 или 2,080 Мбит/с, а также 10 Гбит/с, но по более высокой цене [13];

д) определен межсетевой интерфейс частных сетей (Private Network to Network Interface — PNNI), с помощью которого коммутаторы могут автоматически строить таблицы маршрутизации с учетом требований инжиниринга трафика;

е) стандарт ATM не вводит своих спецификаций на реализацию физического уровня. Он основывается на технологии SDH/SONET, принимая ее иерархию скоростей.

Интерфейсы UNI и NNI. В сети ATM все узлы соединяются друг с другом двухточечными интерфейсами с помощью коммутаторов. При классификации интерфейсов используют два признака: назначение; принадлежность и территория установки коммутатора.

По назначению различают интерфейсы:

- *пользовательский* (User-to-Network Interface — UNI), используемый для подключения к коммутатору оконечных устройств;
- *межсетевой* (Network-to-Network Interface — NNI), предназначенный для соединений между коммутаторами.

По принадлежности и территории установки коммутатора выделяют *публичные* (Public) и *частные* (Private) интерфейсы. Публичный пользовательский интерфейс UNI используется для связи пользователя с коммутатором, принадлежащим оператору связи. Межсетевой публичный интерфейс NNI соединяет коммутаторы одной или нескольких публичных сетей. Частный интерфейс UNI используется для связи узла с собственным коммутатором заказчика, а частные NNI — для связи между его коммутаторами.

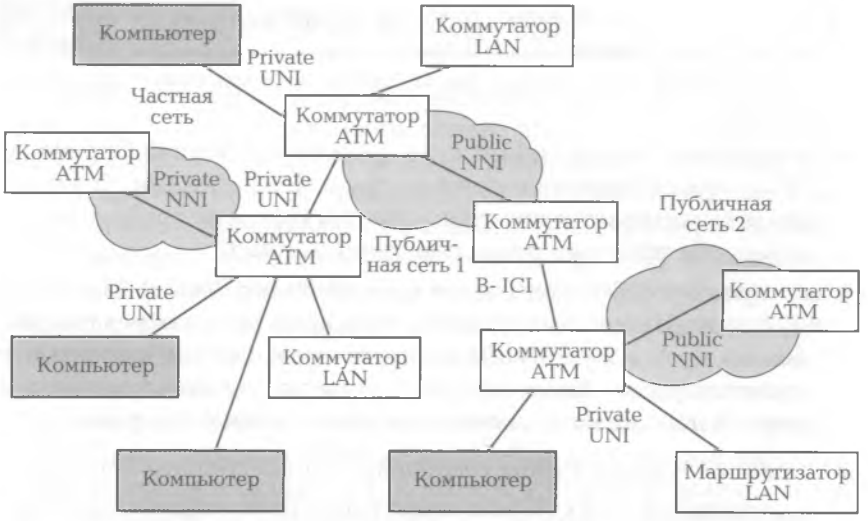


Рис. 7.13. Фрагмент сети с разными типами интерфейсов:

Public/Private NNI — связь коммутаторов одной публичной/частной сети; B-NNI — связь коммутаторов разных публичных сетей; Private UNI — частный пользовательский интерфейс

Пример сети с интерфейсами UNI и NNI приведен на рис. 7.13.

Оборудование ATM. Основным оборудованием сетей ATM являются сетевые адаптеры и коммутаторы. Различают *магистральные коммутаторы*, от которых требуется только коммутация ячеек с максимально возможной скоростью, и *пограничные*, к которым подключается оборудование не только ATM-сети (оконечные устройства, повторители, коммутаторы, маршрутизаторы), но и других сетей (Ethernet, Tokin Ring). По производительности пограничные коммутаторы обычно уступают магистральным. Коммутаторы ATM из-за высокой стоимости портов и других коммутирующих узлов имеют модульную конструкцию, что позволяет подбирать конфигурацию, наиболее близкую к решаемой задаче, и при необходимости наращивать число портов.

Соединения и цепи ATM. Сети ATM поддерживают соединение *точка — точка*, которое может быть как одно-, так и двунаправленным, и однонаправленное соединение *точка — множество точек*, при котором данные передаются от одного источника к множеству получателей, или от корневого узла (Root Node) к листьям (Leaves). Корневой узел является инициатором соединения. Соеди-

нение точка — множество точек используется для организации многоадресных групповых передач.

Существуют следующие типы цепей (соединений, сервисов) ATM [2]:

- *постоянные виртуальные цепи* (Permanent Virtual Circuits — PVC), обеспечивающие прямую связь между узлами. Соединение устанавливается вручную, оно статично и не требует дополнительных процедур перед передачей данных;
- *коммутируемые виртуальные цепи* (Switched Virtual Circuits — SVC), которые устанавливаются только на время передачи данных по протоколу сигнализации между конечными точками и коммутаторами. Выполнение протокола занимает некоторое время и порождает дополнительный служебный трафик;
- *сервис без установления соединения* (Connectionless Service).

Адресация. В сетях ATM с коммутируемыми виртуальными цепями используются три формата адресов (рис. 7.14):

1) DCC (Data Country Code — код страны) с идентификатором служб и форматов AFI=39 (Authority and Format Identifier) — позволяет адресовать пересылку данных в пределах страны;

2) ICD с идентификатором AFI=47 — использует для адресации код организации международного уровня (International Code Designator — ICD);

3) E.164 с идентификатором AFI=45 — использует адрес (аналогичный телефонной нумерации) улучшенной версии сети ISDN — BISDN (Broadband ISDN) в формате E.164.

Остальные поля имеют следующее назначение [2]:

- HO-DSP (High-Order Domain Specific Part) — старшая часть адреса;
- ESI (End System Identifier — идентификатор конечной системы) — представляет собой 48-битный MAC-адрес;
- SEL (Selector) — используется конечными станциями (для сети значения не имеет).

Формат DCC	AFI	DCC	HO-DSP	ESI	SEL
Формат ICD	AFI	ICD	HO-DSP	ESI	SEL
Формат E.164	AFI	E.164	HO-DSP	ESI	SEL

Рис. 7.14. Форматы адресов ATM

7.9. АБОНЕНТСКИЕ ЛИНИИ DSL

Общие сведения. Цифровая абонентская линия (Digital Subscriber Line — DSL) строится на основе абонентской линии обычной телефонной сети путем создания дополнительного цифрового канала, для чего на обоих концах (на АТС и у абонента) существующей линии устанавливаются разделительные фильтры (Splitter). Низкочастотная часть спектра сигнала (до 3,5 кГц) направляется на обычное телефонное оборудование (порт АТС и телефонный аппарат у абонента), а высокочастотная (свыше 4 кГц) используется для передачи данных с помощью DSL-модемов. Дополнительно высокочастотная часть спектра сигнала может разделяться между встречными потоками данных (полный дуплекс). Благодаря использованию широкого спектра (до 1 МГц) достижимые скорости передачи превысили предел в 56 Кбит/с обычных модемов. Услуги DSL предлагаются телефонными станциями дополнительно к обычной телефонной связи.

Технологии xDSL. При частотном разделении каналов часть спектра используется на передачу данных в одном направлении, часть — в другом. При этом можно организовать как симметричные, так и асимметричные (с разной пропускной способностью во встречных направлениях) каналы. Асимметрия полезна для пользователей Internet, которые передают в сеть короткие запросы и принимают оттуда длинные ответы. В связи с этим данные в направлении к пользователю могут передаваться со скоростью 1,5 Мбит/с, а в обратном направлении — со скоростью 384 Кбит/с и ниже. Эта наиболее распространенная технология называется ADSL (Asymmetric DSL — асимметричная DSL). Скорость к абоненту может достигать 6,1 Мбит/с, от абонента — 640 Кбит/с, в зависимости от длины и качества абонентской линии.

К другим технологиям xDSL относятся:

- UADSL (Universal ADSL) — улучшенный вариант ADSL с меньшими скоростями (при длине линии до 3,5 км скорости 1,5 Мбит/с и 384 Кбит/с в разных направлениях; при длине линии до 5,5 км — 640 и 196 Кбит/с);
- SDSL (Symmetric DSL — симметричная DSL) — поддерживает одинаковую пропускную способность в обоих направлениях со скоростью 1,536 или 2,048 Мбит/с на двухпроводной линии при длине до 3 км;
- HDSL (High Data-Rate DSL) — высокоскоростная технология, обеспечивающая скорости 1,536 или 2,048 Мбит/с в обоих на-

правлениях на четырехпроводной линии протяженностью до 3,7 км;

- VDSL (Very High Data Rate DSL) — DSL с очень высокой пропускной способностью (13...52 Мбит/с) на расстояние до 1,5 км. Технология весьма дорогая, рассчитанная на коллективное использование линий;
- IDSL — предоставление услуг DSL по линиям ISDN. Максимальная пропускная способность этой реализации может достигать 144 Кбит/с, однако она доступна в регионах, в которых другие реализации DSL не работают;
- RADSL (Rate Adaptive DSL) — технология с адаптивным изменением скорости передачи в зависимости от качества линии.

По сравнению с другими типами соединений в глобальной сети линии DSL обладают следующими преимуществами:

а) для их создания используются уже существующие телефонные линии;

б) одну и ту же телефонную линию можно одновременно и независимо использовать для передачи данных и для телефонных переговоров, чего не позволяют обычные модемы для коммутируемых линий;

в) пропускная способность DSL сравнима с пропускной способностью линий E1/T1 при значительно меньшей стоимости. Часто стоимость услуг DSL ниже, чем ISDN;

г) линия DSL подключена всегда. Для установки соединения нет необходимости набирать телефонный номер.

7.10. СЕТЬ INTERNET

Общие сведения. *Internet* — это глобальная компьютерная сеть (сеть сетей), использующая стандартные протоколы (TCP/IP) и объединяющая огромное количество сетей. Название происходит от *Inter*connected *net*works — связанные сети.

История Internet начинается с сети ARPANet (см. подразд. 1.1). Вплоть до начала 1990-х гг. Internet имел четыре основные сферы применения (электронная почта, конференции, удаленный доступ и передача файлов). Ситуация резко изменилась с появлением приложения WWW (World Wide Web — Всемирная паутина), которое сделало возможным размещение на сайте нескольких страниц информации, содержащей текст, изображения, звук и видео, со встроенными ссылками на другие страницы. К In-

ternet стали подключаться десятки миллионов новых пользователей в год, и Internet из закрытой сети превратился в услугу, подобную телефонной сети.

Главные особенности Internet состоят в том, что, во-первых, это *самая большая в мире сеть* по территории покрытия, числу пользователей и количеству оказываемых услуг, по суммарному объему передаваемого трафика, количеству входящих в ее состав сетей. Во-вторых, это *сеть без единого центра управления*, но работающая по единым правилам и предоставляющая всем своим пользователям единый набор услуг. Каждая входящая в Internet сеть управляется независимым оператором — поставщиком услуг Internet (Internet Service Provider — ISP). В-третьих, это сеть, располагающая огромным объемом *разнообразной информации*, отличающаяся простотой доступа к ней и сравнительно низкой стоимостью услуг.

Структура Internet. Internet обеспечивает обмен информацией между компьютерами и предоставляет в распоряжение своих пользователей всевозможные ресурсы. При этом тип компьютера и используемая им ОС не играют роли. Internet не только устанавливает связь между отдельными компьютерами, но и создает пути соединения для групп компьютеров, объединенных в глобальные и локальные компьютерные сети (ЛКС), как показано на рис. 7.15, *а*. Отдельные компьютеры, самостоятельно подключенные к Internet (рис. 7.15, *б*), называются *хост-компьютерами* (host — хозяин). Для каждого компьютера устанавливаются два адреса: *цифровой*

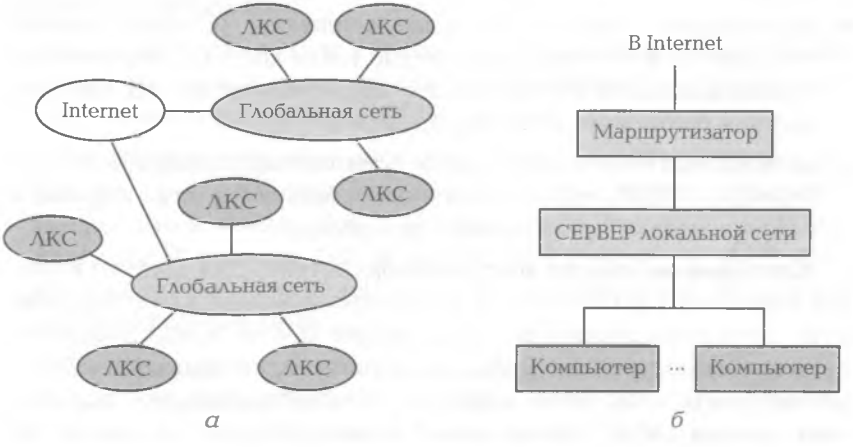


Рис. 7.15. Структура Internet (*а*) и схема подключения компьютеров (*б*)

IP-адрес длиной в 32 бит, содержащий полную информацию для идентификации (определения) компьютера, и *доменный адрес*, предназначенный для идентификации хост-компьютеров. Принципы адресации изложены в подразд. 4.3.

Организация Internet. Рассмотрим особенности организации Internet на территории США [13]. В инфраструктуре Internet используется гибридная ячеистая топология. Благодаря избыточности такой топологии при выходе из строя одной из связей пакеты могут проходить в пункт назначения альтернативными маршрутами. В настоящее время инфраструктура Internet на территории США состоит из коммерческой магистрали и высокоскоростной службы (Very high-speed Backbone Network Service — VBNS).

Коммерческая магистраль — это комплекс коммерческих сетей крупных компаний (*AT&T*, *Sprint*, *BBN Planet* и др.), к которым подключены поставщики услуг Interneta (Internet Service Provider — ISP), или *провайдеры*. Между провайдерами заключены равноправные соглашения по обслуживанию информационных потоков друг друга, в которых оговорена их взаимосвязь и обмен данными. Сети провайдеров подключены к линиям T1, T3 или OC-3. Существуют также:

- *поставщики Internet-контента* (Internet Content Provider — ICP), которые предоставляют содержимое (content) собственных информационно-справочных ресурсов в виде web-сайтов. Многие ISP являются одновременно и ICP;
- *поставщики услуг хостинга* (Hosting Service Provider — HSP), предоставляющие свои помещения, каналы связи и серверы для размещения контента, созданного другими предприятиями;
- *поставщики услуг по доставке контента* (Content Delivery Provider — CDP) в многочисленные точки доступа, максимально приближенные к пользователям так, чтобы повысить скорость доступа пользователей к информации;
- *поставщики услуг по поддержке приложений* (Application Service Provider — ASP), предоставляющие клиентам доступ к крупным универсальным программным продуктам.

Компоненты Internet и их взаимодействие. Для доступа в Internet компьютер должен иметь телефонный модем или соединение с ЛС, предоставляющей посреднические услуги. Когда модем компьютера подключен к телефонной линии, а программное обеспечение соответствующим образом сконфигурировано, пользователь должен набрать телефонный номер провайдера, ввести имя учетной записи и пароль.

Если соединение устанавливается с помощью провайдера услуг Internet, то компьютер становится удаленным клиентом его ЛС. Провайдеры имеют собственные линии или арендуют у телефонных компаний выделенные скоростные линии. Провайдеры, не имеющие непосредственного соединения с магистралью Internet, платят *региональным провайдерам* за соединение с региональной сетью, подключенной к национальной магистрали.

Провайдеры *доступа к магистрали* могут взаимодействовать между собой внутри географических регионов через точки доступа к сети (Network Access Point — NAP) и устанавливать равноправные отношения друг с другом.

Провайдеры *услуг* Internet соединены друг с другом в региональных пунктах обмена (Metropolitan Access Exchange — MAE). Существуют два пункта MAE первого уровня и пять пунктов MAE второго уровня. Самые большие национальные провайдеры услуг Internet, такие как *Sprint* и *Netcom*, подключены к MAE первых двух уровней. Региональные и меньшие провайдеры подключены к MAE второго уровня, где используются менее производительные маршрутизаторы.

Рассмотрим последовательность передачи сообщения по электронной почте:

1) данные разбиваются на пакеты;

2) сетевые протоколы добавляют к пакетам заголовки и трейлеры (trailer — запись с контрольной суммой в конце массива данных);

3) логические нули и единицы преобразуются в электрические или световые сигналы и поступают в линию. При этом возможны следующие варианты:

- если компьютер входит в состав ЛС, то данные проходят по ней к серверу или маршрутизатору, соединенному с телефонной или выделенной (арендованной) линией;
- если используется модемное соединение, то пакеты инкапсулируются протоколами канального уровня с непосредственным соединением точка—точка (Point-to Point Protocol — PPP) или передачи IP-пакетов (Serial Line Internet Protocol — SLIP) и модулированные электрические сигналы передаются по аналоговой телефонной линии;

4) сигналы поступают на принадлежащий провайдеру *сервер удаленного доступа* (Remote Access Server — RAS), настроенный для установки коммутируемого соединения. Возможен вариант передачи с использованием прямой выделенной линии с провай-

дером. При необходимости пользователь регистрируется на сервере, набрав свое имя и пароль;

5) компьютер становится удаленным узлом ЛС провайдера;

6) данные передаются из сервера провайдера в региональную сеть, к которой подключен провайдер (если провайдер входит в категорию крупнейших национальных провайдеров, то этот шаг отсутствует);

7) данные проходят через один из главных пунктов доступа к сети (Network Access Point — NAP) и передаются в коммерческую магистраль Internet;

8) на другом конце данные проходят через другой NAP, через другую региональную сеть и через провайдера на принимающем конце, который передает данные на принимающий компьютер;

9) и, наконец, данные передаются клиентской почтовой программе пользователя, подключенного к провайдеру. Возможно, что почтовый сервер провайдера на некоторое время сохраняет, а затем выгружает содержимое почтового ящика. В конфигурации почтового ящика должна быть заложена учетная запись принимающего пользователя.

Таким образом, посылаемый пакет проходит по различным физическим носителям через многочисленные серверы и маршрутизаторы, затрачивая лишь несколько минут на весь путь.

Службы Internet. Всемирная паутина WWW является одной из самых популярных информационных служб, благодаря возможности использования гипертекста. *Гипертекст* — это выделенный текст, содержащий связи с другими текстами графической, видео- и звуковой информацией. Указание на выделенную часть текста с помощью мыши позволяет перейти на другую часть этого документа, на другой документ этого же или другого компьютера, подключенного к Internet.

Все серверы WWW используют специальный язык разметки гипертекста (Hypertext Markup Language — HTML). HTML-документы представляют собой текстовые файлы, в которые встроены специальные команды. Отображенный на экране гипертекст представляет собой сочетание алфавитно-цифровой информации в различных форматах и стилях и некоторые графические изображения в виде картинок. С помощью программы *Lynx* WWW обеспечивается доступ к сети клиентам, требующим текстовый режим. Для работы в графическом режиме используется программа *Mosaic*.

Связь между гипертекстовыми документами осуществляется с помощью ключевых слов. Найдя ключевое слово, пользователь

может перейти в другой документ, чтобы получить дополнительную информацию. Новый документ также имеет гипертекстовые ссылки.

Сервис WWW обеспечивает взаимодействие с удаленным компьютером (Telnet), обмен файлами и программами по протоколу (File Transfer Protocol — FTP); выполняет прикладную программу.

Электронная почта (E-mail) — это сетевая служба, которая дает возможность пользователям посылать и получать электронные письма (сообщения). Кроме текста письмо может содержать вложенные файлы (программы, изображения, аудио и видео). Для этого существует многоцелевое расширение Internet — специальный стандарт MIME (Multipurpose Internet Mail Extension). Для работы с электронной почтой создано большое число программ (Microsoft Exchange, Microsoft Outlook, The Bat!). Адрес E-mail состоит из двух частей, разделенных символом @. Слева находится имя пользователя (имя почтового ящика), справа — имя домена.

Служба телеконференций (UseNet) состоит из множества тематических телеконференций — групп новостей (Newsgroup), поддерживаемых серверами новостей. *Сервер новостей* — это компьютер, который может содержать тысячи групп новостей самых разнообразных тематик. *Группа новостей* — это набор сообщений по определенной теме. Новости разделены по иерархически организованным тематическим группам, и имя каждой группы состоит из имен подуровней. Наряду с телеконференциями широкое распространение получили WWW-телеконференции, также называемые *форумами*. Отличие состоит в том, что они работают через web-интерфейс и размещаются на web-сайтах.

Списки рассылки (Maillists) — это сервис Internet, работающий через электронную почту. Существует адрес подписчиков списка рассылки. Вы посылаете письмо на этот адрес, и ваше сообщение получат все люди, подписанные на этот список рассылки.

Базовая сетевая услуга TelNet позволяет пользователю Internet дистанционно подключаться к другим удаленным компьютерам и работать с ними со своего компьютера, как если бы он был их удаленным терминалом.

Служба передачи файлов FTP (File Transfer Protocol) позволяет установить связь с одним из FTP-серверов Internet, на котором хранятся файлы, предназначенные для открытого доступа, просмотреть каталог FTP-сервера, осуществить поиск требуемых файлов и управлять их перемещением.

Интерактивная услуга ориентирована на удовлетворение информационных потребностей пользователей в диалоговом

режиме. Для пользования интерактивной услугой нужно зарегистрироваться на центральном сервере этой службы, получить персональный идентификационный номер и сообщить его партнеру. По известному номеру партнера можно через центральный сервер установить с ним соединение и обмениваться сообщениями.

Прослушивание звука в реальном времени осуществляется с помощью системы (RealAudio), состоящей из *сервера*, где хранятся звуковые файлы в гипертекстовом формате, и *проигрывателя*, встраиваемого в программу просмотра. Для прослушивания звуковых файлов разработано расширение языка HTML.

Компьютерная телефония позволяет географически удаленным пользователям устанавливать телефонную связь через Internet с оплатой значительно меньше, чем за связь по обычным телефонным линиям.

Видеоконференция — это интерактивный инструмент, который включает в себя аудио, видео, компьютерные и коммуникационные технологии для осуществления связи удаленных территориально собеседников «лицом к лицу» в реальном времени, а также разделения всех типов информации, в том числе данные, звук, изображение, документы и т. п.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. В чем состоит смысл следующих терминов: «глобальная сеть», «первичная сеть», «магистральная сеть», «сеть доступа», «сеть PDH», «сеть SONET/SDH», «сеть DWDM», «сеть X.25», «сеть Frame Relay», «сеть ISDN», «сеть ATM», «сеть Internet»?
2. Как можно представить современную глобальную сеть? Каковы ее структура и состав? Как происходит передача двоичных данных через глобальную сеть и обеспечивается их совместимость с магистральным каналом связи? Какие стандартные интерфейсы физического уровня используются в сетях? Перечислите основные типы глобальных сетей и дайте их краткую характеристику.
3. Чем вызвано появление сетей плезиохронной цифровой иерархии и каковы их особенности? В чем состоит недостаток этих сетей?
4. Какие основные цели ставили разработчики синхронных оптических сетей SONET/SDH? Какие аппаратные средства и базовые топологии используются в синхронных сетях? В чем состоят особенности формата кадра STM-1? Как в сетях SDH

выполняются операции мультиплексирования и ввода-вывода данных? Какие средства и способы отказоустойчивости используются в сетях SDH?

5. В чем состоит принцип мультиплексирования с разделением частот и с помощью каких аппаратных средств он реализуется? Какие топологии используют при построении сетей DWDM?
6. В чем заключаются особенности сети X.25? Какова структура и состав сети? Какие разновидности адресов используются в сетях X.25?
7. Каковы основные особенности сетей Frame Relay? Какие типы виртуальных каналов и режимов работы определены стандартом? Какие поля содержит формат кадра Frame Relay? По каким наборам параметров технология Frame Relay обеспечивает качество транспортного обслуживания?
8. Какова цель создания сетей ATM и в чем заключаются их основные особенности? Какие интерфейсы, коммутаторы, типы соединений и форматы адресов используются в сетях ATM?
9. В чем состоит основная особенность цифровой абонентской линии? Какие технологии включает в себя набор xDSL?
10. Каковы главные особенности Internet? Каковы структура, организация и компоненты Internet? Поясните последовательность передачи сообщения по электронной почте. Перечислите основные службы Internet и дайте их краткое описание.

Глава 8

АДМИНИСТРИРОВАНИЕ СЕТЕЙ

8.1. ЗАДАЧИ И ПРИНЦИПЫ УПРАВЛЕНИЯ СЕТЯМИ

Введение. Сеть состоит из многих сложных аппаратных средств (компьютеров, мостов, маршрутизаторов и других устройств, связанных линиями передачи), программного обеспечения, поставляемого его разработчиками и встроенного в ОС, а также различных протоколов для управления сетевыми устройствами. *Сетевое администрирование* включает в себя разработку, интеграцию и координацию аппаратуры, программного обеспечения и людей для мониторинга, тестирования, опроса, конфигурирования, анализа, оценки и контроля сети и ресурсов для обеспечения нормального функционирования, высокой производительности и качества обслуживания за приемлемую цену [4]. Выполнение задач поддержания сети в работоспособном состоянии возлагается на *администратора сети* (Network Administrator), которому придаются специальные средства, помогающие следить за состоянием сети и управлять ею. Излагаемый в этой главе материал можно рассматривать как введение в администрирование сетей.

Для управления сетью необходимо иметь ее план, содержащий информацию о кабельных трассах, схемах соединения кабелей, протяженности сети, о стандартах протоколов и оборудования. План должен отражать возможности расширения сети, т. е. учитывать появление новых средств, инструментов и технологий для управления сетью. Разработка такого плана и системы управления на его основе требует тщательного анализа технических и административных вопросов. Администратор должен ориентироваться в многообразии современных средств управления и технически грамотно использовать их для различных усовершенствований, направленных на повышение качества работы сети и облегчения своей работы. Администратор должен решать такие вопросы, как распространение программного обеспечения и контроль его версий, обнаружение и исправление ошибок, управление конфигура-

цией системы, контроль доступа и защиту данных. Для эффективного управления сетью администратору требуется знать, какое программное обеспечение установлено на каждой рабочей станции и как каждая из них сконфигурирована.

В связи с этим администратор сети должен обладать очень высокой квалификацией и творческим подходом при применении тех или иных средств для решения нестандартных ситуаций, возникающих в компьютерных сетях. Кроме того, он должен достаточно хорошо разбираться в конфигурациях сетей, их производительности, в вопросах учета и планирования, в защите данных и прикладных программах.

Задачи сетевого администрирования. Международная организация по стандартизации ISO разработала модель сетевого администрирования, в которой было определено пять групп задач.

1. *Управление конфигурацией сети* (Configuration Management). Включает в себя идентификацию и модификациию параметров конфигурации устройств сети. Выделяют следующие группы задач конфигурирования:

- *параметров элементов сети* (Network Element — NE), таких как маршрутизаторы, мультиплексоры и др. При этом определяются сетевые адреса, идентификаторы (имена), географическое положение и пр.;
- *сети в целом*, которое состоит в построении и поддержании карты сети. В карте отображаются реальные связи между элементами сети и вносятся изменения связей между ними, т. е. фиксируется образование новых физических или логических каналов, изменение таблиц коммутации и маршрутизации и т. п.

Конфигурирование сети определяет (задает), какие устройства входят в администрируемую сеть, а также аппаратную и программную конфигурацию этих устройств.

2. *Управление учетными записями* (Accounting Management). Это процесс сбора данных и координации индивидуального и группового доступа к различным сетевым ресурсам в целях предоставления соответствующих возможностей (в отношении пропускной способности и требований безопасности). Простейшими задачами этого вида управления являются создание и поддержка пользовательских бюджетов и групп, а также присвоение привилегий доступа пользователям и рабочим группам сети. Управление учетными записями позволяет сетевому администратору указать правила доступа пользователя или устройства к сетевым

ресурсам, регистрировать запросы доступа, а также контролировать доступ.

3. *Управление безопасностью* (Security Management). Подразумевает контроль доступа к ресурсам сети (данным и оборудованию) и сохранение целостности данных при их хранении и передаче через сеть; предусматривает составление и ведение списков доступа в маршрутизаторах, организацию парольной защиты для критических сетевых ресурсов, выявление и блокировку точек возможного проникновения злоумышленников.

4. *Обработка ошибок, неисправностей, сбоев* (Fault Management). Является наиболее важной задачей сетевого администрирования, которая состоит в выявлении и устранении сетевых проблем, т. е. в обнаружении неисправностей, их регистрации и принятии соответствующих ответных мер.

5. *Управление производительностью* (Performance Management). Предусматривает оценку пропускной способности сети, производительности компьютеров, числа одновременно поддерживаемых пользователей, времени реакции системы, накопление и анализ статистики использования ресурсов. На основании анализа выполняются необходимые действия по поддержанию определенного уровня производительности (например, пропускной способности) в различных сетевых компонентах, которыми могут быть конкретные устройства (маршрутизаторы, хосты) или абстракции (например, сетевые маршруты).

Следует отметить, что помимо разделения задач управления по функциональному признаку существует стандарт TMN (Telecommunication Management Network — сеть управления связью), разделяющий задачи на уровни в соответствии с иерархической организацией корпоративной сети, которая отражает иерархию самого предприятия и его задач. Нижний уровень сети составляют элементы сети — отдельные компьютеры, коммуникационные устройства, каналы передачи данных. Однако с повышением уровня управления технический характер собираемой о сети информации принимает более общий характер, приобретая производственный, финансовый и коммерческий оттенок. При этом на каждом уровне иерархии модели TMN решаются задачи рассмотренных выше пяти функциональных групп с учетом специфики каждом уровня.

Организация сетевого управления. Рассмотрим представленную на рис. 8.1 простейшую *систему управления сетью* (Network Management System — NMS), под которой обычно понимают совокупность средств мониторинга (текущего контроля) и управления

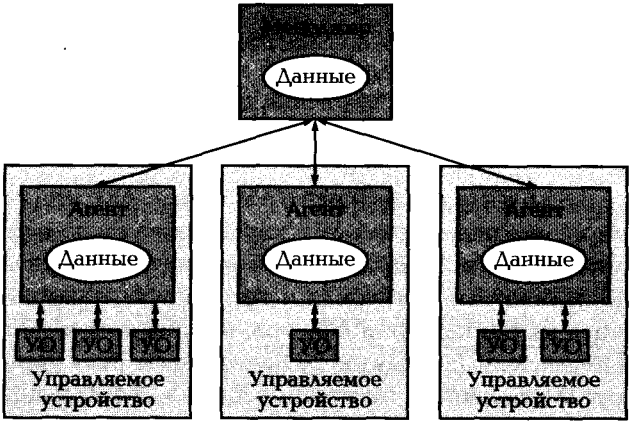


Рис. 8.1. Схема взаимодействия агента, менеджера и УО

коммуникационным оборудованием [9]. Ее основу составляет модель взаимодействия менеджер — агент — управляемый объект (УО).

Состав системы управления. *Менеджер* представляет собой управляющую программу, которая выполняет сбор, обработку, анализ и отображение данных. С ее помощью осуществляется взаимодействие администратора с сетевыми устройствами и управление ими.

Управляемое устройство является частью сетевого оборудования (хост, мост, хаб, принтер, модем) совместно с программным обеспечением. В управляемом устройстве может быть несколько *управляемых объектов* (УО), которые представляют его физические фрагменты (например, сетевую интерфейсную карту), а также наборы настраиваемых параметров для этих аппаратных и программных фрагментов (например, протокол внутренней маршрутизации RIP).

Агент является посредником между УО и менеджером и служит для наполнения УО текущими значениями параметров его модели, получения от ОУ требуемых данных о параметрах и выдачи ему управляющих сигналов. Агент обрабатывает описываемые моделью объекта параметры, представляет их в виде нормализованных данных и посылает менеджеру. На основе полученных данных менеджер принимает решения по управлению, а также выполняет дальнейшее их обобщение о состоянии управляемого ресурса. Таким образом, агент освобождает ме-

неджера от ненужной информации о деталях реализации ресурса. Агент может работать на отдельном компьютере, связанном с управляемым оборудованием, или встраиваться в управляемое устройство или ОС. Многообразие типов УО не позволяет стандартизовать способ взаимодействия агент — управляемый объект.

База управляющей информации. Для мониторинга и управления создаются *модели* УО, характеризуемые соответствующими показателями. Например, для маршрутизатора используются такие показатели, как число и тип портов, таблица маршрутизации, количество кадров и пакетов, прошедших через эти порты, и др. Показатели (значения) УО хранятся в *базе управляющей информации* (Management Information Base — MIB) и называются *MIB-объектами*.

Для спецификации (описания, определения) MIB-объектов используются правила SMI (Structure of Management Information — структура управляющей информации). Международной организацией по стандартизации ISO разработана древовидная структура идентификации MIB-объектов. Каждый узел дерева описывается последовательностью имен или чисел, определяющих путь от корня дерева к его узлу.

Менеджер через агента запрашивает значения показателей требуемого УО и на основе полученных данных принимает решения по его управлению. Менеджер может также обобщать данные о состоянии УО и передавать агенту информацию, на основе которой тот должен управлять объектом. Менеджер обычно работает на отдельном компьютере, взаимодействуя с несколькими агентами. Менеджер и агент взаимодействуют по *стандартному* протоколу сетевого управления. Этот протокол позволяет менеджеру запрашивать состояние УО и неявно (через агентов) предпринимать действия по управлению. Таким образом, базу MIB можно рассматривать как виртуальное хранилище УО, которые отражают текущее состояние сети.

Для маршрутизаторов, хостов и другого сетевого оборудования разработаны стандарты MIB-модулей, в которые входят основные идентификационные данные об определенном фрагменте аппаратуры, а также управляющая информация о сетевых интерфейсах и протоколах устройства.

Протоколы и стандарты. Рассмотренная общая модель сетевого управления применима ко многим стандартам сетевого управления. Существуют два семейства стандартов систем управления ЛС, особенности которых отражены в табл. 8.1 [6, 9].

Таблица 8.1

SNMP*	CMIP**
Стандарты протоколов	
Не является международным стандартом. Контролируется организацией *Internet Activities Board*. Специфицирует *минимум* аспектов и элементов системы управления	Является протоколом OSI. Контролируется Международной организацией по стандартизации ISO. Специфицирует *максимум* аспектов и элементов системы управления
Применение	
Широко используется для сетевого администрирования, ориентирован на управление конкретными устройствами	Предназначен для диагностики работоспособности различных ЛС. Лучше подходит для коммуникаций между двумя или несколькими системами управления ЛС. Используется в небольшом количестве сетевых устройств
Данные и способ их получения	
Извлекаются данные о конкретных устройствах по точной формулировке запроса об интересующем УО. Центральное устройство управления (станция) периодически опрашивает каждое устройство в сети для определения его статуса (состояния, режима)	Ориентирован на извлечение наборов данных. После общего запроса можно путем его уточнения вывести требуемые данные. Сетевые устройства с помощью отчетов информируют центральное управляющее устройство об изменениях в своем статусе
Способ обмена	
Для передачи запросов и ответов используются *дейтаграммы* и простые коммуникационные протоколы (например, UDP). При таком (ненадежном) способе обмена стороны должны предусматривать возможность неполучения данных адресатом. Поэтому отправитель должен повторить передачу несколько раз, прежде чем констатировать факт неработоспособности адресата	Используется *сеансовый* обмен информацией, что делает его более удобным при необходимости получения большого количества данных. Однако это может затруднить управление сетью при возникновении неполадок. Как только в результате сбоя в работе ЛС пропадает связь, обмен информацией становится невозможным

Окончание табл. 8.1

SNMP*	CMIP**
Особенности протоколов	
Протоколы SNMP основаны на концепциях, ориентированных на минимальную загрузку управляемых устройств: агент выполняет самые простые функции и работает в основном по инициативе менеджера; система управления состоит из одного менеджера, который периодически опрашивает всех агентов; протокол взаимодействия между агентом и менеджером SNMP опирается на простой (ненадежный) транспортный протокол UDP (для разгрузки управляемого устройства) и использует два основных типа команд — `get` для получения данных от агента и `set` для передачи управляющих воздействий агенту; агент может послать данные менеджеру по своей инициативе с помощью команды `trap`. Базы управляющей информации MIB состоят из дерева атрибутов, называемых объектами и группами объектов. Используются несколько спецификаций MIB. Более поздняя разработка RMON MIB была направлена на создание интеллектуальных агентов, контролирующих нижний уровень, — интерфейсы Ethernet и Token Ring. Имена объектов стандартных MIB Internet зарегистрированы в дереве регистрации имен стандартов ISO	Для представления управляемых устройств используется объектно-ориентированный подход. Определено несколько суперклассов обобщенных управляемых объектов, на основании которых путем наследования свойств должны создаваться более специфические классы объектов. Для описания управляемых объектов OSI разработаны правила GDMO, основанные на формах определенной структуры, заполняемых с помощью языка ASN.1. Для представления знаний об управляемых объектах, агентах и менеджерах системы управления OSI используются три древовидные базы данных: дерево наследования, которое описывает отношения наследования между классами объектов; дерево включения, которое описывает отношения соподчинения между конкретными элементами системы управления; дерево имен, которое определяет иерархические имена объектов в системе. Протокол CMIP является протоколом взаимодействия между агентами и менеджерами системы управления OSI, позволяет с помощью одной команды воздействовать сразу на группу агентов, применив такие опции, как обзор и фильтрация

* Simple Network Management Protocol — простой протокол управления сетью, входит в стек протоколов TCP/IP.

** Common Management Information Protocol — протокол передачи общей управляющей информации.

8.2. УПРАВЛЕНИЕ УЧЕТНЫМИ ЗАПИСЯМИ, РЕСУРСАМИ И АДРЕСАМИ

Управление сетевыми учетными записями. Используют три типа учетных записей: пользователя, группы пользователей и компьютеров.

Учетные записи пользователя. Каждая такая запись содержит:

- *имя пользователя и пароль*, информацию о пользователе (группу, к которой принадлежит пользователь, и его права доступа к данному ресурсу, т.е. разрешение на запись, чтение или удаление);
- *условия и ограничения пользователя* (компьютер, с которого пользователь может зарегистрироваться; разрешенные время и дата регистрации; разрешена ли удаленная регистрация и т.д.);
- *необязательную информацию* (полное имя, должность, служебный телефон и адрес электронной почты пользователя).

Имеются служебные программы, или *утилиты*, с помощью которых можно создавать учетные записи пользователей и добавлять в регистрационную базу данных новых пользователей.

Учетные записи группы пользователей. Для облегчения администрирования учетных записей целесообразно объединять пользователей в *группы*. Все пользователи, принадлежащие группе, имеют присвоенные ей права доступа. Пользователь может принадлежать нескольким группам одновременно. В некоторых ОС допускается *вложение* одних групп в другие. Поскольку в этих случаях возможны конфликты при доступе пользователей, принадлежащих разным группам, важной частью администрирования сетевых ОС являются анализ и разрешение этих конфликтов. Группы, которым присваиваются права доступа, называются *группами безопасности*; группа, созданная только для использования приложений (без права доступа), называется *группой распространения*.

В некоторых ОС группы делятся на категории в зависимости от области действия группы. Например, группа может быть локальной, если она закреплена за одним сервером, и глобальной, если отнесена ко всему домену. В системе Windows 2000/XP поддерживается также категория *универсальной группы*, область действия которой распространяется на все дерево, или лес, доменов. В сетях NetWare и UNIX локальные и глобальные группы не различаются.

В большинстве сетевых ОС при установке (конфигурировании) создается одна или несколько *групп по умолчанию*. Обычно одна из этих групп включает в себя учетные записи всех пользователей.

Учетные записи компьютеров. Для обеспечения более высокого уровня безопасности в сетях используются учетные записи не только пользователей, но и подключенных к сети компьютеров. Например, чтобы включить компьютер с ОС Windows NT/2000 в свою группу (домен), администратор должен создать для него учетную запись. Учетная запись компьютера используется сетевой ОС для проверки идентичности компьютера и для отслеживания (аудита) за использованием его учетной записи.

Система безопасности на уровне пользователей основана на создании отдельных учетных записей пользователей для каждого, кто получает доступ к ресурсам. Чаще всего безопасность с использованием учетных записей пользователя поддерживается на уровне сети. В сетях на основе Windows она называется *безопасностью на уровне доменов*.

Безопасность на уровне сети реализуется следующим образом:

- в процессе установки сетевой ОС создается специальная учетная запись пользователя, называемая *учетной записью администратора*. С ее помощью сетевой администратор может создавать учетные записи пользователей, которым нужен доступ к сетевым ресурсам;
- при регистрации в сети (рис. 8.2, *а*) пользователь вводит имя учетной записи пользователя и пароль. Вводимые данные сверяются с информацией, хранящейся в регистрационной базе данных, которая расположена на *сервере аутентификации*. Если введенная регистрационная информация признается правильной, пользователю выдается маркер доступа, с помощью которого его можно идентифицировать в группе;
- при попытке пользователя получить доступ к ресурсу (например, распечатать документ на принтере) *маркер доступа* проверяется по списку контроля доступа (рис. 8.2, *б*), который имеет каждый совместно используемый ресурс. Этот список содержит пользователей и группы пользователей, которым разрешен доступ к этому ресурсу, а также уровень доступа к ресурсу (разрешение на чтение, изменение или удаление ресурса). Если учетная запись пользователя или группы, к которой он принадлежит, присутствует в списке контроля доступа,

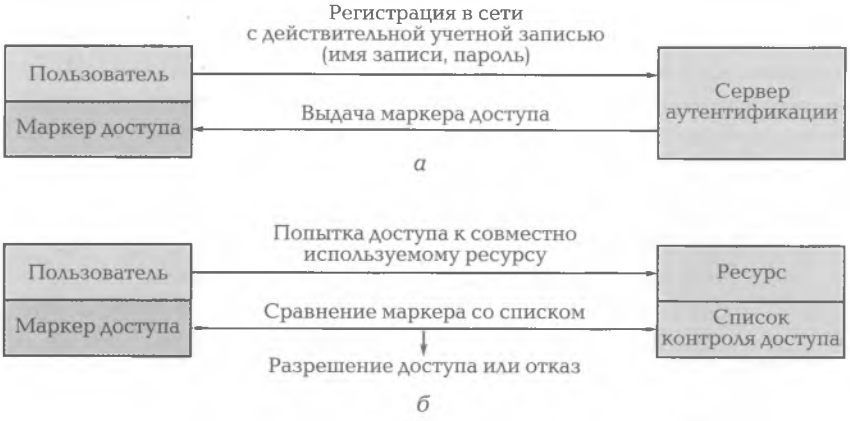


Рис. 8.2. Принцип управления учетными записями:
а — при регистрации в сети; *б* — при попытке доступа

пользователь получает доступ к ресурсу. Если пользователь не имеет соответствующего права доступа, то сервер отказывает ему в доступе.

Управление совместно используемыми ресурсами. Совместно использовать можно любые типы устройств, включая сканеры, факсы, внешние накопители и др. Управление ресурсами осуществляется в целях обеспечения доступа к ресурсам тем пользователям, которым эти ресурсы необходимы, и предотвращения несанкционированного доступа к ресурсам. Хотя эти цели противоречивы, однако обе они могут быть достигнуты путем использования *службы каталогов*, такой как Novell Directory Services (NDS) или Active Directory компании *Microsoft*.

К основным типам разделяемых ресурсов следует отнести:

- *разделяемые файлы и каталоги*. Общие документы, оформленные в виде файлов, целесообразно хранить на файловом сервере, поскольку администратор может обеспечить их регулярное резервное копирование, а каждый пользователь всегда получит последнюю копию требуемого документа. Достоинство сетевого разделения каталогов состоит в том, что каждому пользователю предоставляется безопасное место хранения документов, называемое *домашним каталогом*. Никто, кроме хозяина каталога, не может вносить в него изменения, при этом резервные копии домашних каталогов регулярно создаются сервером автоматически;

- *разделяемые принтеры*. В зависимости от ОС существует несколько способов подключения к удаленному разделяемому принтеру. Например, способ *захвата порта принтера* — позволяет перенаправить задачи принтера с порта локального принтера на сетевой принтер;
- *разделяемые приложения*. Пользователи сети могут выполнять все программы-приложения, хранящиеся на *сервере приложений*. Хотя производительность серверных приложений обычно ниже, чем приложений, выполняемых на локальных компьютерах, их использование уменьшает объем памяти жестких дисков на локальных компьютерах. Кроме того, можно чаще обновлять и модернизировать версии приложений;
- *разделяемые подключения*. Компьютеры, объединенные в сеть, могут подключаться к Internet с помощью одной линии и единственной учетной записи.

Управление сетевой адресацией. К функциям сетевого администрирования относятся поддержка набора адресов и внесение изменений в конфигурации рабочих станций (компьютеров).

Каждая станция должна иметь свой уникальный номер, который бы позволял передавать сообщения, предназначенные только для нее. Такой адрес, называемый *адресом управления доступом к среде* (Media Access Control — MAC) или *физическим адресом*, «прошит» в каждом сетевом адаптере производителем. Он состоит из 16 шестнадцатеричных цифр, первые восемь из которых определяют код производителя сетевого адаптера, а оставшиеся — номер адаптера. Каждый адрес является уникальным, но только с его помощью невозможно получить доступ к сетевому адаптеру на физическом уровне.

Для идентификации рабочих станций и упрощения процесса доставки сообщений используют логические адреса, называемые *сетевыми*. Сетевой адрес состоит из номера сети и номера станции. *Номер сети* соответствует номеру сегмента сети, которому принадлежит данная станция, а *номер станции* однозначно определяет станцию в сегменте.

Каждый сетевой протокол использует свою собственную схему сетевой логической адресации.

В протоколе межсетевого обмена пакетами (Internetwork Packet eXchange — IPX) сетевой номер и номер станции обрабатываются раздельно. Для присвоения адресов требуется незначительное вмешательство администратора. Достаточно каждому сегменту присвоить номер на сервере, которым может

служить любое случайное число. Присвоение номера станции выполняется автоматически во время загрузки сетевой ОС.

В протоколе TCP/IP сетевой номер и номер станции объединены в одном адресе IP, который анализируется с помощью второго параметра, называемого *маской подсети*. Какая часть является сетевым адресом, а какая — адресом станции, определяется с помощью специального ключа. Для взаимодействия по протоколу IP используются собственно адрес IP и маска подсети обеих рабочих станций. Если станции расположены в разных сегментах, то для установления соединения между ними необходим третий параметр — используемый по умолчанию шлюз или маршрутизатор. Если одна станция посылает сообщение станции другой сети, она должна передать его используемому по умолчанию маршрутизатору. Протокол IP (в отличие от IPX) не поддерживает автоматическое присвоение адресов. Все параметры устанавливаются сетевым администратором вручную или одним из двух автоматизированных способов: с помощью протокола начальной загрузки (Bootstrap Protocol — BootP) или протокола динамической конфигурации хост-компьютера (Dynamic Host Configuration Protocol — DHCP).

8.3. ВВЕДЕНИЕ В БЕЗОПАСНОСТЬ СЕТЕЙ

Сетевая безопасность охватывает множество мер и должна рассматриваться как часть общей политики, проводимой организацией (предприятием, компанией, фирмой) по информационной безопасности. В обеспечении безопасности сети занято много служб и используются различные средства. По сетевой безопасности написано огромное количество книг и статей, затрагивающих широкий круг различных вопросов. Основное внимание в дальнейшем уделено вопросам, которые, на взгляд авторов, могут быть полезны для администраторов небольших сетей, а именно вопросам защиты данных от потерь и неправильного (или злонамеренного) использования.

Основные понятия. Эффективность компьютерной сети во многом зависит от степени защищенности обрабатываемой и передаваемой информации. Степень защищенности информации от различного вида угроз при ее получении, обработке, хранении, передаче и использовании называют *безопасностью информации*. Актуальность проблеме сетевой безопасности придает широкое использование компьютерных технологий во всех сферах жизни

современного общества, а также переход от использования выделенных каналов к публичным сетям (Internet, Frame Relay), который наблюдается при построении корпоративных сетей.

Безопасная сеть (или безопасная связь) обладает свойствами:

- *конфиденциальности* (Confidentiality), т.е. защищает данные от несанкционированного доступа, предоставляя доступ к секретным данным только авторизованным пользователям, которым этот доступ разрешен;
- *доступности* (Availability), что означает обеспечение постоянного доступа к данным авторизованным пользователям. Безопасная связь характеризуется свойством *аутентичности*, т.е. способностью отправителя и получателя подтвердить свою личность: отправитель и получатель должны быть уверены в том, что каждый из них является тем, за кого он себя выдает;
- *целостности* (Integrity), гарантирующей сохранность данных, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом изменять, модифицировать, разрушать или создавать данные.

Политика безопасности, включающая в себя совокупность норм и правил, регламентирующих процесс обработки информации, формируется на этапе развертывания сети с учетом таких основополагающих принципов, как:

- *комплексный подход* к обеспечению безопасности, начиная с организационно-административных запретов и заканчивая встроенными средствами сетевой защиты;
- предоставление каждому сотруднику предприятия (пользователю компьютеров, информационной системы, сети) того *минимального уровня привилегий* на доступ к данным, который необходим ему для выполнения своих должностных обязанностей;
- *принцип баланса возможного ущерба от реализации угрозы и затрат на ее предотвращение*. Например, в некоторых случаях можно отказаться от дорогостоящих аппаратных средств защиты, ужесточив административные меры.

Основная задача политики безопасности состоит в защите от несанкционированного доступа к ресурсам информационной системы. Политика безопасности является эффективным средством, заставляющим всех пользователей корпоративной сети следовать раз и навсегда установленным правилам безопасности. Ее реализация начинается с выявления уязвимых компонентов и угроз и принятия соответствующих контрмер.

Уязвимым является такой компонент, некорректное использование или сбой которого может поставить под угрозу безопасность всей сети. К уязвимым компонентам относят пользователей сети, которые могут нанести вред сознательно, случайно или в силу отсутствия опыта. Примером уязвимого компонента может служить также система резервирования на лентах или других носителях. Если информация нерегулярно резервируется, перед всей корпоративной сетью возникает вполне реальная угроза потери данных в результате умышленного или случайного повреждения основного накопителя. *Угроза* — это потенциальная попытка использования недостатков уязвимого компонента для нанесения вреда. Примерами угроз могут служить взломщики, вирусы, пожары, природные катаклизмы.

После оценки возможных угроз (рисков) переходят к выработке контрмер. Под *контрмерой* понимают действие, позволяющее минимизировать риск от определенного уязвимого компонента или некоторой угрозы. Одной из самых эффективных контрмер минимизации риска потери данных является создание надежной системы резервного копирования.

Результаты оценки рисков и выработанные контрмеры используются для создания плана безопасности, который должен в мельчайших подробностях описывать системные стратегии организации, имеющие непосредственное и отдаленное отношение к вопросам безопасности.

Планирование безопасности сети и данных. Высокая степень безопасности может быть достигнута путем использования плана, предусматривающего применение различных мер и средств обеспечения безопасности.

Оценка требований к безопасности сетевых данных является первым этапом разработки плана по принятию мер их защиты. При этом должны быть учтены характер деятельности организации и хранящихся в сети данных, стратегия и стиль управления организацией, которые должен знать сетевой администратор и реализовать его в подведомственной ему сети.

Высокий уровень безопасности данных должен поддерживаться в организациях, располагающих данными, которые являются строго конфиденциальными по своей природе. Примером могут служить коммерческие организации, предоставляющие услуги или выпускающие продукцию в областях с высоким уровнем конкуренции. Некоторые виды данных должны быть защищены независимо от характера деятельности организации. К ним относятся бухгалтерская документация, налоговая информация, промыш-

ленные секреты (планы деятельности организаций и коммерческие планы, рецепты, технологии изготовления, тексты программ и т.д.).

Для принятия мер по защите данных в сети нужно выявить главные источники угроз их безопасности. Существуют следующие виды угроз:

- *непреднамеренные*, к которым относятся ошибочные действия лояльных сотрудников, стихийные бедствия, ненадежность работы программно-аппаратных средств и др.;
- *преднамеренные*, которые явно направлены на причинение ущерба информационной безопасности;
- *внешние*, которые проявляются в таких формах, как несанкционированное использование паролей и ключей; атаки DoS (Denial of Service — отказ в обслуживании), направленные на разрыв сетевого соединения или приведение его в неработоспособное состояние; подмена адреса; компьютерные вирусы и черви;
- *внутренние*, к которым можно отнести промышленный шпионаж, интриги и недовольство служащих, случайные нарушения и т.п.

В плане безопасности должны быть самым детальным образом перечислить процедуры, выполнение которых предписывается политикой безопасности. Каждый сотрудник, отвечающий за выполнение конкретной процедуры, должен быть предупрежден о возможных последствиях в случае отступления от предписанного способа выполнения процедуры. Рекомендуется взять с сотрудника письменное подтверждение того, что он понимает смысл стратегии безопасности, согласен с ней и обязуется ей следовать, а также регулярно обновлять план, т.е. пересматривать аспекты безопасности, пытаясь определить новые потенциально уязвимые компоненты, угрозы и контрмеры для борьбы с ними, и отражать изменения в плане.

8.4. СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Для безопасности сети используется широкий набор различных средств и технологий. Рассмотрим некоторые из них.

Базовые технологии безопасности. В разных программных и аппаратных продуктах, предназначенных для защиты данных, часто используются одинаковые подходы, приемы и технические ре-

шения, которые в совокупности образуют *технологию безопасности* [11].

Криптозащита. Разработкой методов преобразования информации в целях ее защиты занимается *криптография* (от др.-греч. κρυπτός — скрытый и γραφω — пишу). Преобразование общедоступных (понятных для всех) данных к виду, затрудняющему их распознавание, называется *шифрованием* (Encryption), а обратное преобразование — *дешифрованием* (Decryption). Шифрование является доступным средством для администраторов и пользователей и одним из эффективных средств обеспечения конфиденциальности информации. Следует выделить два основных способа шифрования данных: *перестановку* (Transposition), когда в исходных данных изменяют последовательность символов, и *замену* (Substitution), при которой с помощью некоторого шаблона производят замену всех символов используемого алфавита, например буквы заменяют цифрами.

Операции шифрования и дешифрования данных (информации) осуществляются с помощью ключей, которые создаются с привлечением математических формул. Метод, при котором для обеих операций используется один ключ, называется *симметричной криптографией* (Symmetric Cryptography). При *асимметричной криптографии* (Asymmetric Cryptography) каждый пользователь сети должен располагать двумя ключами: *общим* (Public key) и *частным* (Private key). Оба ключа связаны друг с другом с помощью некоторой математической функции. Общий ключ известен каждому пользователю. Зашифрованное с помощью общего ключа сообщение может быть прочитано только с помощью частного ключа. Поскольку предполагается, что пользователь, которому адресуется сообщение, не разглашает свой ключ, он является единственным человеком, который может прочитать сообщение.

Популярны два алгоритма шифрования: *симметричный* DES (Data Encryption Standard — стандарт шифрования данных, который является официальным стандартом правительства США) и *несимметричный* RSA, разработанный учеными Rivest, Shamir, Adleman и названный по начальным буквам их фамилий.

Для шифрования, аутентификации и проверки целостности передаваемых по сети пакетов разработан протокол IPSec (IP Security), включающий в себя *протокол AH* (Authentication Header), позволяющий проверять идентичность отправителя, и *протокол ESP* (Encapsulating Security Payloads), обеспечивающий конфиденциальность самих данных. Протокол IPSec поддерживают маршрутизаторы компании *Cisco Systems* и ОС Windows 2000/XP.

Для передачи через Internet зашифрованных, аутентифицированных сообщений используется протокол SSL (Secure Sockets Layer — уровень защищенных сокетов, или гнезд). В этом протоколе криптографическая система с открытым ключом комбинируется с блочным шифрованием данных.

Аутентификация (Authentication). Это процедура установления подлинности пользователя при запросе доступа к ресурсам системы (компьютеру или сети). Аутентификация предотвращает доступ нежелательных лиц и разрешает доступ всем легальным пользователям. В процедуре аутентификации участвуют две стороны, одна из которых доказывает свое право на доступ (аутентичность), предъявляя некоторые аргументы, другая — проверяет эти аргументы и принимает решение. Для доказательства аутентичности может использоваться некоторое известное для обеих сторон слово (пароль) или уникальный физический предмет (ключ), а также собственные биохарактеристики (отпечатки пальцев или рисунок радужной оболочки глаза).

Наиболее часто при аутентификации используют вводимые с клавиатуры пароли. *Пароль* представляет собой зашифрованную последовательность символов, которая держится в секрете и предъявляется при обращении к информационной системе.

Объектами аутентификации могут быть не только пользователи, но и различные устройства, приложения, текстовая и другая информация.

Идентификация субъектов и объектов доступа. Идентификация предусматривает закрепление за каждым субъектом доступа уникального имени в виде номера, шифра или кода, например, персональный идентификационный номер (Personal Identification Number — PIN), социальный безопасный номер (Social Security Number — SSN) и т. п. Идентификаторы пользователей должны быть зарегистрированы в информационной системе администратором службы безопасности. При регистрации в базу данных системы защиты для каждого пользователя заносятся такие данные, как фамилия, имя, отчество и уникальный идентификатор пользователя, имя процедуры для установления подлинности и пароль пользователя, полномочия пользователя по доступу к системным ресурсам и др. Идентификацию следует отличать от аутентификации. Идентификация заключается в сообщении пользователем системе своего идентификатора, в то время как аутентификация является процедурой доказательства пользователем того, что именно ему принадлежит введенный им идентификатор.

Авторизация (Authorization). Это процедура предоставления каждому из пользователей тех прав доступа к каталогам, файлам и принтерам, которыми его наделил администратор. Кроме того, система авторизации может контролировать возможность выполнения пользователями различных системных функций, таких как установка системного времени, создание резервных копий данных, локальный доступ к серверу, выключение сервера и т. п.

Система авторизации наделяет пользователя сети правами выполнять определенные действия над определенными ресурсами. Для этого могут быть использованы два подхода к определению прав доступа:

- *избирательный*, при котором отдельным пользователям (или группам), явно указанным своими *идентификаторами*, разрешаются или запрещаются определенные операции над определенным ресурсом;
- *мандатный*, при котором вся информация в зависимости от степени секретности делится на уровни, а все пользователи сети — на группы, образующие иерархию в соответствии с *уровнем допуска* к этой информации.

Процедуры авторизации реализуются программными средствами по *централизованной схеме*, в соответствии с которой пользователь один раз логически входит в сеть и получает на все время работы некоторый набор разрешений по доступу к ресурсам сети, и *децентрализованной схеме*, когда доступ к каждому приложению должен контролироваться средствами безопасности самого приложения или средствами той операционной среды, в которой оно работает.

Поскольку системы аутентификации и авторизации совместно выполняют одну задачу, необходимо предъявлять к ним одинаковый уровень требований. Ненадежность одной системы не может быть компенсирована высоким качеством другой.

Аудит (Auditing). Это фиксация в системном журнале событий, связанных с доступом к защищаемым системным ресурсам. Аудит используется для обнаружения неудачных попыток *взлома* системы. При попытке выполнить противоправные действия система аудита идентифицирует нарушителя и пишет сообщение в журнал регистрации. Анализ накопившейся и хранящейся в журнале информации может оказаться действенной мерой защиты от несанкционированного доступа.

Процедура рукопожатий. Для установления подлинности пользователей широко используется процедура рукопожатий

(Handshaking — согласованный обмен, квитирование), построенная по принципу вопрос-ответ. Она предполагает, что правильные ответы на вопросы дают только те пользователи, для которых эти вопросы предназначены. Для подтверждения подлинности пользователя система последовательно задает ему ряд случайно выбранных вопросов, на которые он должен дать ответ. Опознание считается положительным, если пользователь правильно ответил на все вопросы.

Технологии защищенного канала широко используются в виртуальных частных сетях, которые требуют принятия дополнительных мер по *защите* передаваемой информации. Требование конфиденциальности особенно важно, потому что пакеты, передаваемые по публичной сети, уязвимы для перехвата при их прохождении через каждый из узлов (серверов) на пути от источника к получателю. Технология защищенного канала включает в себя [10]:

- взаимную аутентификацию абонентов при установлении соединения;
- защиту передаваемых по каналу сообщений от несанкционированного доступа;
- подтверждение целостности поступающих по каналу сообщений.

В зависимости от места расположения программного обеспечения защищенного канала различают две схемы его образования [10].

1. *Схема с конечными узлами* (рис. 8.3, *а*). В этой схеме защищенный канал образуется программными средствами, установленными на двух удаленных компьютерах. Компьютеры принадлежат двум разным ЛС одной организации и связаны между собой через публичную сеть.

2. *Схема с оборудованием поставщика услуг* публичной сети, расположенным на границе между частной и публичной сетями (рис. 8.3, *б*). В этой схеме защищенный канал прокладывается только внутри публичной сети с коммутацией пакетов. Средствами защиты являются пограничные устройства доступа (ПУД).

Средства безопасности, предоставляемые операционными системами. Современные ОС способны обеспечить доступ к одному компьютеру и сетевым ресурсам многим пользователям. Для этого используются отдельные учетные записи, которым присвоены разные пароли. После правильного ввода регистрационной информации пользователь может получить доступ к ОС и сети; чи-

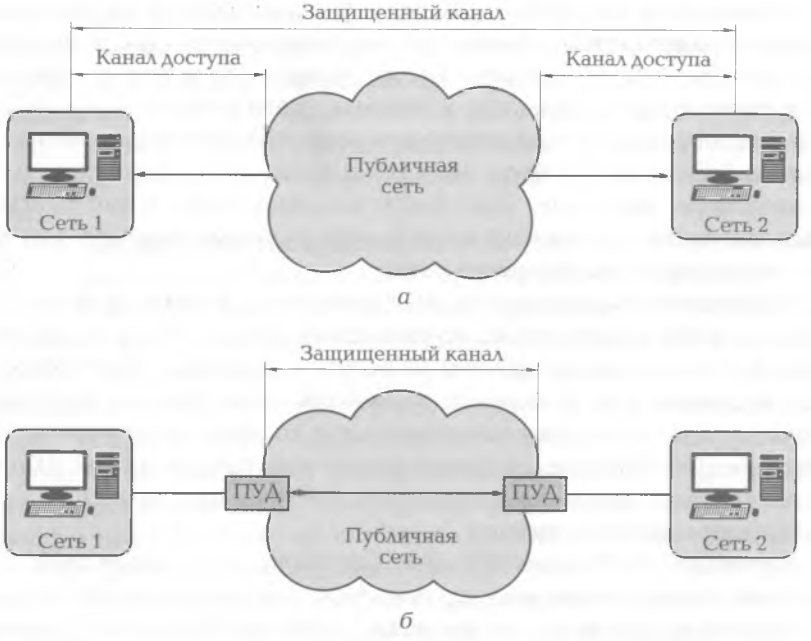


Рис. 8.3. Способы образования защищенного канала:

а — с конечными узлами, взаимодействующими через конечную сеть; *б* — с защитой между ПУД

тать, изменять ресурсы и выполнять любые другие действия, которые соответствуют правам его учетной записи, создавать желаемую конфигурацию пользовательского интерфейса (рабочую среду) и т.д.

Выбор (или назначение) паролей подчинен стратегии обеспечения сетевой безопасности. Пароли должны удовлетворять определенным требованиям. Многие сетевые ОС позволяют администратору задавать длину и время жизни пароля; проверять пароль на наличие заданного пароля в словаре и, если он есть, предотвращать использование пароля; следить, чтобы пароль пользователя не повторялся. Кроме того, администратору предоставляются широкие возможности контроля за доступом к ресурсам. Например, одной и той же учетной записи он может одновременно разрешить просматривать содержимое файла `file1.doc`, но запретить вносить в него изменения; предоставить право читать, изменять, удалять файл `file2.doc` и даже устанавливать права доступа к нему других пользователей, а к файлу `file3.doc` отменить все права доступа.

В файловых системах с высоким уровнем безопасности права доступа можно устанавливать как на разделение ресурсов по сети, так и на использование этих ресурсов на одном и том же локальном компьютере. Локальные и сетевые права доступа могут не совпадать. Например, пользователю можно предоставить право полного контроля над файлом `file4.doc`, когда он регистрируется на компьютере, хранящем этот файл, но ограничить право доступа того же пользователя к `file4.doc` при попытке получить к нему доступ с другого компьютера сети.

Администратор должен знать и учитывать, какими правами доступа наделена данная ОС по *умолчанию* (сразу после загрузки). Так, по умолчанию разделяемый ресурс в серверах Windows NT/XP *доступен* для любого пользователя сети. Для ограничения прав доступа к ресурсу администратор должен их изменить, а в серверах NetWare разделяемый ресурс *недоступен* ни для одного пользователя. Здесь предоставление доступа требует явного вмешательства администратора.

Сетевая ОС Windows NT позволяет каждому пользователю назначать четыре вида (или привилегии) доступа к совместно используемому ресурсу: *отсутствие доступа* (No Access); *полный доступ* (Full Control); *чтение* (Read), предоставляющее право просматривать перечень файлов, открывать файлы, изучать их содержимое и копировать файлы на свои носители; *редактирование* (Change), предоставляющее дополнительную (к Read) возможность изменять содержимое существующих файлов и каталогов. Windows NT позволяет также управлять доступом к локальным файлам. Для этого файлы или каталоги должны быть расположены в логическом разделе жесткого диска, размеченном файловой системой NTFS. Помимо указанных выше привилегий система NTFS позволяет просматривать файлы каталога (привилегия List), добавлять файлы в каталог без изменения их содержимого (Add), просматривать существующие и добавлять новые файлы (Add & Read).

Администратор должен понимать способы назначения привилегий и взаимоотношения между назначенными привилегиями доступа к локальным и совместно используемым ресурсам и применять наиболее эффективный способ назначения привилегий пользователям. При этом пользователи должны быть лишены возможности обращения к не нужным для работы ресурсам.

Система безопасности Windows NT предоставляет возможность регистрации всех происходящих событий. Однако ведение отчетности требует постоянно запущенных приложений, что снижает

производительность сети, поэтому к протоколированию событий, которое также отнимает время, администратор и пользователи сети должны походить избирательно и активизировать средства регистрации событий только на тех рабочих станциях, которые этого требуют. Журнал регистрации событий может оказаться полезным источником информации при администрировании сети.

Аппаратные средства защиты. Основой надежной защиты данных от многих неисправностей аппаратных средств является *избыточность*. При выходе из строя некоторого сетевого устройства начинает функционировать его резервный дублер. Потерю данных при выходе из строя винчестера можно восполнить файлами, хранящимися в системе резервного копирования. Некоторые серверы поддерживают возможность установки избыточных устройств, автоматически передающих полномочия отказавшего компонента исправному. Такая избыточность применима к охлаждающим вентиляторам, источникам питания, сетевым адаптерам, жестким дискам и центральным процессорам. При резервировании электропитания используют избыточные источники электроэнергии — устройство бесперебойного питания наряду с электросетью. Резервное копирование данных предполагает создание избыточных копий ценных файлов на дополнительных (резервных) носителях. В системах отказоустойчивых дисков данные записываются на избыточных дисках. Высшей степенью избыточности является *кластеризация*, когда несколько серверов объединяются в группу. В сети кластер серверов виден пользователям как один сервер. Если один из серверов кластера выходит из строя, его обязанности выполняет другой сервер. Пользователи не замечают этого перехода. Средства поддержки кластеризации встроены в такие ОС, как, например Windows 2000 Advanced Server.

Резервирование электропитания. Потери данных могут возникать вследствие скачков или перебоев в электропитании. Для защиты сети от сбоев электропитания может служить *источник бесперебойного питания* (ИБП), представляющий собой устройство с аккумулятором, в котором накоплен достаточный запас энергии, чтобы компьютер продолжал нормально работать некоторое время после отключения напряжения электросети. Обычно отводится время (от 5 до 20 мин), в течение которого пользователь должен закрыть файлы и приложения и правильно завершить работу ОС.

К ИБП должны быть подключены все критичные системы сети. В нормальном режиме аккумулятор источника непрерывно подза-

ряжается. В момент отключения электропитания ИБП подает звуковой сигнал или передает специальное сообщение по заданному сетевому адресу и переключает компьютер на аккумулятор. Программное обеспечение ИБП может быть сконфигурировано на автоматическое завершение работы компьютера.

Резервное копирование данных. Оно осуществляется с помощью специальных программ и является действенной мерой защиты от возможной их потери при регулярном выполнении этой процедуры. Наличие резервной копии позволяет быстро восстановить утерянные данные.

Используются следующие способы резервного копирования [13]:

- *полное*, при котором копируются все данные заданных дисков независимо от того, когда их копирование выполнялось последний раз и вносились ли с тех пор изменения;
- *дифференциальное*, когда копируются все файлы, которые изменялись со времени последнего полного копирования. Дифференциальное копирование выполняется в промежутках между полным копированием, благодаря этому экономится время. Для обновления данных нужно восстанавливать две последних копии — полную и дифференциальную;
- *инкрементное*. При этом способе копируются все файлы, которые изменялись со времени любого последнего копирования (а не последнего полного копирования). Это наиболее быстрый способ, однако он сложнее и занимает много времени на восстановление данных, так как необходимо восстанавливать последнюю полную копию и все инкрементные копии, созданные со времени последнего полного копирования.

Отказоустойчивая система дисков. Под *отказоустойчивостью* понимают способность системы к восстановлению после аварии. Объединение (конфигурация) нескольких физических жестких дисков в отказоустойчивый набор называется *системой RAID* (Redundant Array of Independent Disks — избыточный набор независимых дисков). Он может быть реализован в нескольких различных формах. В зависимости от уровня (0—5 и 7) предоставляются различные способы объединения дисков: RAID 0, RAID 1, RAID 2, RAID 3, RAID 4, RAID 5.

Рассмотрим некоторые способы объединения дисков.

1. *Зеркальное отображение дисков*. Для реализации этого способа используют два физических жестких диска, предпочтительно одного и того же объема. Все данные одного диска зеркально ото-

бражаются на другой. На втором диске хранится точный дубликат всех файлов и структур первого диска. Если один из дисков выходит из строя, вместо него подключается другой диск. Переключение может выполняться автоматически.

2. *Дуплексирование дисков*, отличающееся от зеркального отображения лишь тем, что оба диска подключаются к отдельным контроллерам дисководов, что повышает отказоустойчивость.

3. *Распределение дисковой памяти с контролем четности.* При этом способе объединяются три диска. Данные записываются на двух дисках полосами (слоями), а на специально выделенном третьем диске — информация контроля четности. Если диск данных терпит крах, то данные могут быть восстановлены с помощью информации контроля четности.

Способы RAID могут быть реализованы как программно, так и аппаратно. Аппаратный метод RAID более быстродействующий и надежный, однако его реализация обходится дороже. Некоторые ОС, такие как Windows NT Server и Windows 2000 Server, содержат встроенные средства поддержки программного RAID.

Брандмауэры позволяют организовать защиту по всему периметру ЛС, создавая барьер между внутренней ЛС и соединениями с внешним миром (Internet). Такая защищенная область может быть установлена также в подсети. Брандмауэр может быть реализован как аппаратным, так и программным способом. Фактически он является средством фильтрации входящих и исходящих пакетов. На основе правил безопасности, установленных сетевым администратором, брандмауэр определяет, следует ли пропустить поступивший пакет. Обычно брандмауэры располагают на *шлюзах* сети, являющихся точками ее соединения с другой сетью.

8.5. МОНИТОРИНГ СЕТИ

Основные понятия, термины и задачи мониторинга. Мониторинг (monitoring — текущий контроль; диспетчерское управление) будем рассматривать как одно из направлений администрирования для поддержания сети в работоспособном состоянии. Цель мониторинга состоит в обнаружении, диагностировании и последующем устранении любой угрозы нормальному функционированию сети. Процесс мониторинга включает в себя два этапа.

1. *Контроль сети.* На этом этапе производится сбор данных о состоянии отдельных устройств сети и сети в целом. Для этого используют программные и аппаратные измерители, тестеры, сете-

вые анализаторы, встроенные средства мониторинга коммуникационных устройств, агенты систем управления.

2. *Анализ данных.* Анализ состоит в обработке новых данных и сопоставлении с ранее собранными данными, выявлении возможных причин нарушения нормальной работы сети и выработке рекомендаций по их устранению. Проведение анализа требует активного участия человека, а также возможного привлечения экспертных систем, аккумулирующих накопленный опыт многих сетевых специалистов.

Постоянный контроль сети позволяет выявить узкие места и поддерживать базовый уровень производительности сети. *Узкое место* — это точка в сети, ограничивающая пропускную способность или производительность всей сети. Узкое место может быть порождено неполадками в каком-либо компоненте или присущими ему ограничениями, поэтому возникает задача оптимизации производительности, состоящая в отыскании узких мест и их устранении путем модернизации, повторного конфигурирования или замены компонентов для повышения их производительности до уровня остальных компонентов сети. *Базовый уровень* — это допустимый уровень производительности сети при типичной рабочей нагрузке. Сопоставляя текущий показатель с базовым уровнем, можно установить, например, как повлияла на производительность реализация новой службы или применение новой программы. Измерение базовых показателей следует проводить в процессе нормальной работы сети. Рекомендуется выполнить несколько отдельных измерений через определенные интервалы времени, а затем усреднить их. Базовый уровень позволяет определить загрузку отдельных участков сети и построить диаграмму использования сетевых ресурсов в течение дня, недели или месяца, обнаружить активных пользователей сети, обосновать расходы на модернизацию сетевых компонентов. Мониторинг позволяет выработать рекомендации (положительный опыт) по использованию наиболее эффективных и экономных способов выполнения задач администрирования.

Пропускная способность соединения с Internet является весьма важным показателем работы объединенной сети. Низкая пропускная способность соединения с Internet может быть вызвана:

- низким качеством соединения с сервером удаленного доступа провайдера, обусловленным проблемами с модемом на любом из концов, шумами в линии и т.д.;
- низкой производительностью сервера, которому передаются запросы;

- перегруженностью магистральных каналов Internet;
- уменьшением пропускной способности каналов вследствие их разделения с другими пользователями в ЛС или сети провайдера.

Располагая достоверными сведениями об уровне производительности отдельных компонентов и сети в целом, распределении объемов трафика во времени и другими статистическими сведениями, администратор может правильно диагностировать состояние сети и повысить эффективность процедур обслуживания.

Контроль сети, тестирование, диагностирование и определение производительности сети позволяют разработать общую стратегию упреждающих мероприятий по безопасности сети. Создаваемая в результате процесса управления сетью точная документация позволяет администраторам определить работоспособность сети и прогнозировать некоторые возможные события.

Для определения уровня производительности используются средства диагностирования. Протокольные анализаторы и серверы с большими жесткими дисками способны накапливать статистические данные и сохранять их для последующего анализа. Результатом диагностирования является создание точной документации, с помощью которой администратор может оценить потенциальные недостатки сети и предпринять действия по их устранению.

Тестирование также позволит администраторам оценить результат (пользу) установки нового программного и аппаратного обеспечения, не нанося при этом ущерб функциональности сети, выявить недостатки конфигурации и внести соответствующие изменения.

Регулярному тестированию должны подвергаться резервные носители данных, источники резервного питания, например дизель-генератор, снабжающий электроэнергией сетевые устройства в случае отказа внешнего питания.

Администратор должен осуществлять контроль за использованием лицензированного программного обеспечения, а также периодические и случайные проверки системы безопасности. Контроль правомочности использования программного обеспечения поможет организации избежать штрафов за пиратство в отношении программного обеспечения, а также определить некорректное использование лицензий на программное обеспечение (или их игнорирование), а случайные проверки системы безопасности позволят убедиться в ее целостности.

Средства мониторинга. В небольших сетях используются автономные средства мониторинга, которые можно разделить на несколько групп.

Средства мониторинга кабельных систем. Кабели и разъемы являются одной из возможных (и частых) причин неполадок в сетях, поэтому для обнаружения, диагностики и устранения неисправностей кабельных систем разработано и используется большое число разнообразных средств.

Кабельные тестеры представляют собой наиболее простые портативные приборы, способные обнаружить неисправность кабеля. *Специальные тестеры* кабелей наделены широкими функциональными возможностями. Они предоставляют сведения о сопротивлении, импедансе и аттенюации (затухании) кабеля; уровне сигналов; количестве ошибочных кадров и кадров со служебной информацией; ошибках, вызванных возникновением конфликтов, и др.

Рефлектометры (Time-Domain Reflectometer) — это измерительные приборы для обнаружения неисправностей (разрыва, короткого замыкания) в электрических и волоконно-оптические кабелях. Рефлектометр посылает в кабель зондирующий импульс, принимает его отражение (Reflect), анализирует и определяет с достаточно высокой точностью расстояние до предполагаемого разрыва или короткого замыкания.

Кабельные сканеры являются портативными приборами, которые могут измерить электрические параметры кабелей, а также обнаружить место повреждения кабеля. Основное назначение сканеров — измерение электрических и механических параметров кабелей: длины кабеля, параметра NEXT (near-end crosstalk — переходный разговор на ближнем, передающем конце), затухания, импеданса, схемы разводки пар проводников, уровня электрических шумов в кабеле.

Сетевые анализаторы предназначены для тестирования кабелей, а также для сбора данных о таких статистических показателях, как средняя интенсивность общего трафика сети или потока пакетов с определенным типом ошибки. Они позволяют с высокой точностью измерять электрические параметры кабельных систем, снимать на приемной паре амплитудно-частотную характеристику, определять перекрестные наводки, затухание и суммарное затухание. Сетевые анализаторы являются прецизионными приборами для сертификации кабельных систем по международным стандартам и могут выполнять некоторые функции анализаторов протоколов.

Анализаторы протоколов (Protocol Analyzers). Они представляют собой программные или аппаратно-программные системы, позволяющие захватывать и декодировать пакеты, представлять в удобной для администратора форме вложенность пакетов, расшифровывать содержания отдельных полей каждого пакета. Помимо этих основных функций анализаторы протоколов могут обеспечить широкий набор дополнительных функций, таких как измерение среднестатистических показателей трафика в сегменте ЛС, фильтрация захватываемых и отображаемых пакетов, возможность работы с несколькими агентами и др. С их помощью определяют узкие места сети, выявляют отказавшие сетевые адаптеры, вышедшие из строя концентраторы, повторители и другие сетевые компоненты, разорванные соединения, несоответствие настроек протоколов и т.д. Администратору предоставляется возможность анализа трафика на всех уровнях модели OSI. Аппаратные протокольные анализаторы могут быть использованы для оценки эффективности сегмента и измерения объема исходящего и входящего трафика данного сегмента.

Многофункциональные портативные приборы. Они сочетают в себе функции кабельных сканеров и анализаторов протоколов. Такие приборы снабжены многострочными дисплеями, контекстно-чувствительной системой помощи, встроенным микропроцессором с программным обеспечением и позволяют выполнять комплексную проверку сегментов сети на всех уровнях, от физического до прикладного. Поддерживают только базовый набор протоколов ЛС.

Программное обеспечение мониторинга. К настоящему времени разработано много программ для мониторинга сети, которые могут быть полезны для сетевых администраторов при выявлении неполадок в соединениях, определения производительности и обнаружения вторжений. Различают несколько видов программного обеспечения мониторинга сетей:

- *анализаторы протоколов* и *сетевые анализаторы*, разработанные поставщиками программных средств. Они перехватывают пакеты (кадры), передаваемые между компьютерами или сетевыми устройствами, и преобразуют их к виду, пригодному для анализа человеком; предоставляют статистическую информацию о перехваченных пакетах и позволяют вести наблюдение за передаваемыми по каналу данными (Sniffer — нюхачи);
- *встроенные системы* (Embedded Systems) *диагностики* и *управления*, которые устанавливаются в коммуникационное оборудование или встраиваются в ОС как программные модули. Они

обслуживают только одно устройство, а также выполняют функции SNMP-агентов, поставляя данные о его состоянии для системы управления;

- *встроенные в ОС* (Windows NT, Windows XP и др.) *программы*. Они проще и обладают меньшими функциональными возможностями, чем программы мониторинга независимых поставщиков. Их возможности ограничиваются определением базовых показателей производительности, а область применения — диагностированием и устранением некоторых неполадок в сети.

В качестве примера приведем краткое описание некоторых программных средств.

Сетевой анализатор Sniffer представляет собой сложный набор сетевых инструментов, с помощью которых можно выполнять фильтрацию пакетов на основе сопоставления образцов, а также адресов протоколов TCP/IP или DLC (Data Link Control — управление передачей данных). В состав Sniffer Pro входит генератор загрузки сети, облегчающий тестирование новых устройств и приложений. Его можно использовать для моделирования сетевой нагрузки, определения времени ответа и подсчета числа ретрансляций. В программы Sniffer встроены утилиты (`ping`, `tracert` и др.) для просмотра соответствия имен службы DNS (Domain Name System). В состав Sniffer входит программа Expert Analyzer, облегчающая диагностирование сетевых неполадок. Можно запустить одновременно несколько экземпляров этой программы или использовать только ее отдельные инструменты. В анализаторе Sniffer используется удобный для пользователя графический интерфейс, имеющий вид приборной панели.

Программа LANalyzer компании Novell содержит базовые инструменты мониторинга и устранения неполадок в сетях Ethernet и Token Ring. Она выполняется под управлением Windows и кроме перехвата пакетов может выдавать конкретные рекомендации по устранению неполадок и оптимизации производительности сети. Сетевые компоненты идентифицируются в программе именами и MAC-адресами. Графический интерфейс LANalyzer, как и в Sniffer Pro, похож на приборную панель. Программа LANalyzer поддерживает службу каталогов NDS (Novell Directory Services), обеспечивающую защиту и унифицированный доступ к ресурсам сети. Она может работать с NetWare, AppleTalk, NFS, SNA и TCP/IP.

Универсальная утилита Performance Monitor, входящая в комплект поставки ОС Windows NT, способна отсле-

живать все операции файлового сервера, службы и устройства сервера, а также объем обработанного сервером сетевого трафика. Она позволяет:

- измерять производительность многих системных компонентов и выводить данные в графическом формате, сохранять их в журнале и составлять по ним отчеты;
- просматривать результаты измерений в реальном времени, обновлять их автоматически или по требованию;
- для обнаружения узких мест выполнять мониторинг счетчиков сетевых интерфейсов, определяющих общее число, а также количество переданных и принятых байтов в секунду. Мониторинг счетчиков помогает правильно спланировать распределение пропускной способности.

Если накопить данные о производительности сервера за длительный промежуток времени, то любые значительные отклонения от средних значений этих данных можно рассматривать как возникновение проблемы (неисправности).

Сетевые инспекторы представляют собой программную реализацию протокольного анализатора. Инспекторы в состоянии захватывать, декодировать и анализировать пакеты, предоставлять статистические сведения о типе пакетов, ошибках и объемах исходящего (входящего) трафика. Инспектор сети, входящий в комплект поставки ОС Microsoft Windows NT Server, предоставляет рабочей станции возможность захвата и отслеживания входящего и исходящего сетевого трафика. Утилита Network Monitor компании *Microsoft* позволяет строить диаграммы сетевого трафика и накапливать данные о распределении объемов передаваемых данных во времени на жестком диске для последующего анализа.

Программа Microsoft Network Monitor, поставляемая в составе Windows NT/2000, предназначена для анализа работы процедур протоколов: пропускной способности сети, измерения количества кадров в секунду и получения дополнительной статистической информации о работе сети. Ее можно использовать для вывода отдельных кадров перехваченных данных различных протоколов, включая TCP, UDP и SMB.

8.6. НЕПОЛАДКИ В СЕТЯХ И ИХ УСТРАНЕНИЕ

Неполадки в сети — это нарушение ее нормальной работы. К неполадкам относят сбои, неисправности, отказы. Существует

множество причин появления неполадок (обрыв кабеля, неправильная конфигурация программ, повреждения файла вирусом и др.) и различных форм их проявления (низкая производительность сети, отсутствие доступа к сети, файлу, неработоспособность сетевого устройства и т. п.).

Объекты и причины неполадок. Рассмотрим некоторые наиболее распространенные факторы, препятствующие нормальному функционированию сети.

Физическая среда передачи из-за возможных повреждений представляет наибольшую опасность. При возникновении любых проблем в первую очередь следует осматривать кабели, разъемы и концентраторы. Причиной невозможности установления соединения между двумя абонентами сети зачастую оказывается разрыв или короткое замыкание кабеля. Администраторы должны разработать методику определения целостности кабелей, используемых для подключения отказавших рабочих станций. Это должен быть самый первый шаг перед выполнением других действий, таких как изменение конфигурации компьютеров, замена сетевых адаптеров, удаление (обновление) драйверов. Сначала следует проверить наличие физических соединений между рабочими стациями, после чего с помощью приборов убедиться в отсутствии разрывов и коротких замыканий в проводке; затем проверить исправность и соответствие спецификациям оконечных устройств и терминаторов.

Сетевые адаптеры являются другой распространенной причиной возникновения проблем в сети. Каждый адаптер обладает собственным набором параметров конфигурации, поэтому для нормальной работы его драйвер (управляющая программа) требует совместимости с ОС рабочей станции и корректной настройки. Если запросы на прерывание (Interrupt Request — IRQ), адреса портов ввода-вывода (Base I/O Port Address) и адреса используемых областей памяти (Base Memory Address) выставлены некорректно или конфликтуют с другим устройством, то и сетевой адаптер будет функционировать некорректно или не работать вообще.

Сетевым средам, серверы которых функционируют под управлением различных ОС (UNIX, NetWare, Windows NT Server, Windows Vista, Linux), необходимо устранить несоответствие сетевых протоколов. Адаптер рабочей станции и сетевые устройства, с которыми он взаимодействует, должны использовать одни и те же протоколы. При исправных и корректно настроенных сетевых адаптерах следует проверить соответствие протоколов и прежде всего установить, могла ли рабочая станция обращаться к ресур-

сам сервера ранее или она никогда не обладала такой возможностью. Затем необходимо определить, все ли протоколы, драйверы которых установлены на рабочей станции, корректно связаны с сетевым адаптером, убедиться в том, что все установленные протоколы корректно настроены и т. д.

Наибольшее влияние на работоспособность сети оказывают следующие проблемы серверов.

1. *Недостаточная производительность процессоров.* Общая производительность сети непосредственно зависит от производительности ее серверов. Чем больше служб, пользователей, сеансов аутентификации и операций ввода-вывода поддерживает сервер, тем более строгие требования формулируются к производительности его процессоров. Для отслеживания степени загрузки процессоров можно использовать утилиту Performance Monitor ОС Windows NT, которая способна распределить их функциональные обязанности на несколько машин и определить момент необходимости модернизации процессоров сервера.

2. *Недостаточный объем оперативной памяти,* доступной ОС, службам и приложениям. Объем памяти критически важен для серверов баз данных и серверов, отвечающих за систему безопасности и аутентификации.

3. *Потеря данных в результате сбоя жестких дисков.* При отсутствии резервных копий сбой диска сервера является катастрофическим событием. Вероятность потери данных в результате выхода из строя одного из жестких дисков может быть снижена с помощью отказоустойчивых систем RAID.

Возможность возникновения указанных проблем серверов следует учитывать еще на этапе проектирования и развертывания сети, а при ее обслуживании включать в планы мероприятий по предупреждению сбоя и восстановлению сети после его возникновения.

Перегруженность сети происходит во время обслуживания максимального числа пользователей и проявляется в снижении производительности в отдельных сегментах или во всей сети. Для выявления причин перегруженности следует определить используемую в разное время полосу пропускания, интервалы максимальной нагрузки на сеть, тип передаваемых пакетов, сегмент с максимальным объемом трафика, а также все узкие места в сети, ограничивающие пропускную способность или производительность сети. Кроме того, следует установить, впервые снижается производительность или такое явление наблюдалось и ранее. Второй случай свидетельствует о недостаточно продуманной архитек-

туре сети и требует модернизации магистральных линий связи. Вполне возможно, что снижение производительности вызвано появлением в сети новых приложений или увеличением числа пользователей.

При полном заполнении сети широковещательными пакетами возникает *лавина широковещательных передач* (Broadcast Storm). Причинами катастрофического снижения производительности могут быть использование протокола NetBEUI (NetBIOS Extended User Interface) для организации широковещательных передач через сеть или выход из строя сетевых адаптеров и концентраторов.

Проблемы питания и, в первую очередь, отключение и включение электроэнергии могут привести к самым непредсказуемым последствиям, поэтому серверы, рабочие станции и сетевые устройства должны иметь защиту от проблем питания, например с помощью источников бесперебойного питания.

Меры по предупреждению неполадок. Разработка предупреждающих процедур занимает много времени, тем не менее, этим заниматься необходимо, чтобы избежать неполадок. Все сведения о предпочтениях пользователей, а также перечень и настройки сетевых устройств должны быть тщательно документированы. Существование подробного реестра аппаратных устройств и программного обеспечения в значительной степени упростит текущее обслуживание сети и ее модернизацию.

Обсуждение мероприятий, упреждающих возникновение сбоя, было бы неполным без учета Internet и всех коммерческих интрасетей. Ключевая упреждающая стратегия в подобных средах — строгая безопасность, и сетевые администраторы должны рассматривать ее в качестве наиболее важного фактора, о котором следует позаботиться в собственной сети. Широкий ассортимент антивирусного программного обеспечения и многочисленность компаний, занимающихся разработкой продуктов, имеющих отношение к безопасности, также свидетельствуют о важности соблюдения требований безопасности.

Для защиты сети необходимо строго следовать разработанным мерам (политики, стратегии) безопасности сети. Сведения о пользователях, имеющих удаленный доступ, и времени предполагаемого доступа позволят администраторам определить места и способы возможного вторжения. Строгие требования к модемам рабочих станций и неразглашение паролей существенно снизят вероятность проникновения злоумышленников в сеть.

В некоторых случаях угрозу безопасности корпоративной сети могут нести сами сотрудники организации. Разъяснение важности

предусмотрительного использования компьютера и предупреждение всех пользователей о возможности ненамеренного создания условий для вторжения злоумышленников позволит существенно повысить безопасность сети.

Основными упредительными мерами, повышающими эффективность использования ограниченных ресурсов, являются документация и стандартизация, регулярное создание резервных копий информации, разработка эффективной стратегии хранения и ротации носителей с резервными копиями, чтобы в случае необходимости данные можно было восстановить с минимальными усилиями.

В небольших сетях можно реализовать достаточно эффективный план мероприятий по предупреждению сбоя. Многие утомительные операции, например такие, как создание резервных копий, могут быть автоматизированы. Даже в самой маленькой рабочей группе можно найти квалифицированного пользователя и возложить на него постоянную обязанность менять носители в резервном накопителе.

Если организация четко придерживается разработанной стратегии предупреждения сбоев, то она существенно облегчает себе задачи разрешения возникающих проблем и устранения последствий сбоев. Мониторинг и тестирование предоставляют администраторам возможность разработать план и воплотить в жизнь профилактические мероприятия, которые существенно повысят надежность сети и одновременно ее эффективность.

Создание резервных копий, ротация их носителей, использование бесперебойных источников питания, а также своевременное их проведение являются наиболее эффективными мерами в отношении обеспечения надежности и стабильности сети.

Логическая изоляция сбоя. Точная идентификация сбоя и причин его появления позволяет разработать комплекс противодействующих мероприятий для предотвращения и устранения многих неисправностей. Использование такого подхода называют *логической изоляцией сбоя* [11].

Процесс изоляции сбоя, называемый *методологией согласования* (Adjust Method), делится на шесть этапов.

1. *Оценка приоритетов.* Далеко не все проблемы требуют безотлагательного решения. В первую очередь должны решаться проблемы первостепенной важности независимо от того, насколько сложными они являются. В связи с этим рекомендуется оценить приоритеты и упорядочить известные проблемы в соответствии с их важностью.

2. *Сбор данных*. Для этого можно использовать два основных источника информации: пользователей и отчеты, которые создаются инструментами и утилитами, предназначенными для мониторинга сети. Чем больше *полезных сведений* (о симптомах сбоя, настройках ОС, программного обеспечения, аппаратных устройств, сообщениях об ошибках и т.д.) удастся накопить, тем быстрее и точнее будет идентифицирована сама проблема и причины ее возникновения. Накопление необходимых сведений — первый конкретный этап процесса решения любой сетевой проблемы.

3. *Обоснование возможных причин*. На этом этапе проводится анализ всех собранных данных, составляется перечень возможных (путем исключения второстепенных) причин сбоя и выполняется их сортировка.

4. *Тестирование и изоляция отдельных устройств*. Из списка возможных причин возникновения сбоя следует выбрать одну или несколько настоящих причин. Для этого используется итерационный *процесс тестирования и изолирования*, начиная с наиболее очевидной причины из перечня. Последовательная (по одной) проверка возможных причин позволяет с минимальными усилиями возвращаться к предыдущей конфигурации в случае их неподтверждения и снижает вероятность возникновения побочных явлений. Рекомендуется документировать вносимые изменения, чтобы иметь возможность корректно вернуть сеть в исходное состояние в том случае, если они оказались неэффективными.

5. *Изучение и анализ результатов*. Этот этап проводится, если в результате предпринятых действий проблема устраняется. В этом случае следует переходить к проверке следующей потенциальной причины в составленном перечне, а после того как подобным образом будет проанализирован весь перечень, а настоящая причина так и не будет найдена, рекомендуется заново выполнить процедуру согласования, начав ее с этапа сбора сведений, или прибегнуть к посторонней помощи.

6. *Документирование результатов*. Убедившись в том, что проблема успешно разрешена, необходимо записать ее симптомы, причины возникновения и способ устранения, а также внесенные изменения (если они имели место) в сетевую архитектуру, инфраструктуру и конфигурацию.

Точное следование приведенной последовательности действий позволит быстро определить причины возникновения любой, пусть даже самой сложной проблемы.

Устранение неполадок. Рассмотрим общие принципы и основные средства устранения неполадок.

Организационные принципы. Устранение неполадок — одна из наиболее трудных задач сетевого администрирования, требующая немалого опыта и мастерства администратора. Шансы на успех существенно повышаются при использовании структурированного метода обнаружения, анализа и решения проблемы. Процесс устранения неполадки необходимо выполнять шаг за шагом. Можно выделить следующие этапы решения проблемы:

- *сбор данных*. Прежде всего необходимо определить проблему и собрать о ней как можно больше информации с привлечением пользователей, правильно формулируя вопросы, ответы на которые помогут диагностировать проблему;
- *анализ информации*. Необходимо начать с наиболее очевидной возможной причины неполадки или отказа и путем последовательного перебора и отбрасывания выявить истинную причину. Такой подход существенно сужает круг поиска;
- *составление и реализация плана действий*. В план должны быть включены действия, выполняемые в случае неудачи первых этапов плана. За один шаг следует пробовать (выполнять) только один вариант действия;
- *проверка результатов предпринимаемых действий*. Необходимость такой проверки обусловлена тем, что действия по устранению неполадки могут вызвать побочные эффекты и создать новые проблемы в других местах;
- *документирование*. Несмотря на текущую работу, необходимо выделить время для записи подробностей возникшей проблемы, плана ее устранения и предпринятых для этого действий. Рекомендуется создавать электронную копию этих записей.

Использование файлов системного журнала. В большинстве ОС предусмотрены средства автоматического ведения (записи и просмотра) журнала таких событий, как отказы устройств, неудачные попытки установки соединения и другие ошибки. Например, в Windows NT/2000 есть программа Event Viewer, с помощью которой можно просматривать список системных событий. Эта информация может оказаться весьма полезной в качестве исходной точки процесса устранения неполадки.

Использование утилит TCP/IP. Большинство современных сетей используют протокол TCP/IP, поэтому для устранения неполадок можно воспользоваться предоставленными этим протоколом утилитами для сбора информации, проверки соединений и устранения сетевых неполадок. В разных реализациях TCP/IP

они могут иметь разные имена и обладать разными функциональными возможностями. Рассмотрим несколько категорий утилит TCP/IP, предназначенных для тестирования соединений, конфигурирования и устранения неполадок в сетях.

Для *проверки соединения* с другим компьютером и определения маршрута, по которому прошел пакет данных, можно использовать команды `ping` и `pathping`.

Команда `ping` (от Packet INternetwork Groper) представляет собой простую утилиту, передающую на выбранный целевой (надежный) компьютер запрос Echo Request с помощью протокола ICMP (Internet Control Message Protocol), обеспечивающего восстановление связи при сбойных ситуациях в передаче пользовательских пакетов. Целевой компьютер передает обратно ответ Echo Reply. Если ответ получен, значит, физическое соединение между двумя компьютерами работоспособно.

С помощью команды `ping` можно проверить правильность установки на компьютере и работы стека протоколов TCP/IP.

С помощью команды `pathping` можно обнаружить, какой маршрутизатор вызывает сетевые проблемы, или измерить число пакетов, потерянных на конкретном маршрутизаторе.

Утилиты трассирования (отслеживания) используются для определения маршрута, по которому пакет прошел на принимающий компьютер. Утилита трассирования выводит на экран все маршрутизаторы, через которые прошел пакет на своем пути от передающего компьютера к принимающему. Эта утилита весьма полезна для обнаружения точки, в которой соединение разрывается или замедляется продвижение пакетов. В разных ОС они имеют свои собственные названия, например в Windows NT — `tracer`.

Причиной неполадок в соединении часто оказывается его неправильное конфигурирование. Возможно, присвоенный компьютеру IP-адрес находится в неправильном диапазоне адресов подсети или неправильно введены маска подсети, шлюз по умолчанию, адрес DNS и т.д. Если любой из этих параметров неверен или случайно удален, то компьютер не может правильно сообщаться с сетью TCP/IP.

В каждой ОС есть *утилита вывода конфигурационных параметров*: используемый IP-адрес, маска сети (подсети) и шлюза, MAC-адрес (физический), сервер DNS и др. Эти параметры используются системой или сетевым адаптером.

Для вывода статистической информации используется утилита Netstat, для вывода и обновления кэша — `ARP`, для просмотра и обновлении записей в таблицах маршрутизации — `ROUTE`.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. В чем состоит смысл следующих терминов: «учетная запись», «конфиденциальность», «доступность», «целостность», «аутентичность», «уязвимый компонент», «угроза», «контрмера», «аутентификация», «идентификация», «авторизация», «аудит», «мониторинг», «узкое место», «базовый уровень», «логическая изоляция сбоя»?
2. Что такое сетевое администрирование? Какие группы задач включены в модель сетевого администрирования, разработанную Международной организацией по стандартизации ISO?
3. В чем состоят общие принципы взаимодействия агента, менеджера и управляемого объекта в системе управления сетью (см. рис. 8.1)? Каковы назначение составных частей системы управления и их функции?
4. Как строятся системы безопасности? Какие виды учетных записей используются в системах безопасности?
5. Какие общие принципы управления разделяемыми ресурсами и их основные типы вы знаете?
6. Каковы общие принципы управления сетевой адресацией и особенности их реализации в протоколах IPX и TCP/IP?
7. Что такое безопасность сети и какими свойствами она обладает? Что такое политика безопасности и в чем состоят ее основные задачи?
8. Какие базовые технологии безопасности вы знаете? Дайте их краткую характеристику.
9. Какие средства безопасности предоставляют операционные системы для администратора и пользователей и как они реализуются на практике?
10. Каковы основные аппаратные средства защиты сетей? Опишите их.
11. В чем состоит цель мониторинга и какие этапы он включает в себя? Для чего проводится регулярное тестирование сети?
12. На какие группы делят средства мониторинга?
13. Какие виды программного обеспечения используют для мониторинга сетей?
14. Каковы основные объекты неполадок в сетях и возможные причины их возникновения? Какие упредительные меры принимают для исключения неполадок?
15. Что такое логическая изоляция сбоя? Какие этапы включает в себя процесс изоляции сбоя?
16. Какие организационные принципы используют для устранения неполадок? Покажите, как можно использовать утилиты TCP/IP для обнаружения неполадок.

ЗАКЛЮЧЕНИЕ

Рассмотрим основные тенденции развития информационно-телекоммуникационных технологий (ИТТ). Приоритетными направлениями развития ИТТ в России являются следующие.

1. Формирование современной информационной и телекоммуникационной инфраструктуры, обеспечение высокого уровня ее доступности, предоставление на ее основе качественных услуг. Это направление связано с созданием единой сети электросвязи страны и единого информационного пространства; обеспечением радиочастотным ресурсом перспективных технологий; обновлением и развитием гражданских спутниковых систем связи и вещания государственного назначения; переходом к цифровому телерадиовещанию и решением других задач.

2. Распространение ИТТ для повышения качества образования, медицинского обслуживания, социальной защиты населения, развития культуры и средств массовой информации. Для этого необходимо оказывать содействие подключению к сети Internet образовательных учреждений, музеев, больниц, библиотек и других социально значимых организаций, а также внедрению дистанционного образования, дистанционного консультирования и обслуживания пациентов, предоставлению гражданам социальных услуг с использованием ИТТ.

3. Обеспечение условий для развития конкурентоспособной отечественной индустрии ИТТ. Для этого необходимо стимулировать применение ИТТ организациями и гражданами, развивать механизмы венчурного (с риском) финансирования ИТТ, создавать технопарки в сфере высоких технологий, совершенствовать законодательство и правоприменительную практику в области использования ИТТ.

4. Повышение эффективности государственного управления и местного самоуправления, взаимодействия гражданского общества и бизнеса с органами государственной власти, обеспечение эффективного межведомственного и межрегионального информационного обмена.

5. Противодействие использованию потенциала информационных и телекоммуникационных технологий в целях угрозы национальным интересам России, включая обеспечение безопасности функционирования информационно-телекоммуникационной инфраструктуры и информационных и телекоммуникационных систем.

Дальнейшему развитию ИТТ будут способствовать активная модернизация инфраструктуры, рост спроса на информационные услуги, увеличение предпринимательской активности, распространение компьютерной грамотности населения и ряд других мер.

Рассмотрим развитие некоторых конкретных направлений.

Сети связи следующего поколения (NextGeneration Network — NGN). В концепции NGN заложена идея конвергенции (объединения, сближения) существующих сетей разных операторов и технологий (телефонных сетей общего пользования, сетей мобильной связи и сетей с IP-технологией и др.). Основное назначение сетей нового поколения заключается в обеспечении взаимодействия существующих и новых телекоммуникационных сетей. Они должны предоставлять неограниченный набор услуг с гибкими возможностями по их управлению, поддерживать связь с подвижными объектами.

Сеть NGN строится на базе пакетов с использованием транспортных каналов и протоколов, способных транспортировать информацию любого типа, современных средств доступа к ресурсам сети и разнообразных терминальных устройств.

Цифровое телевизионное вещание (ЦТВ). По сравнению с аналоговым телевидением ЦТВ обеспечивает высокое качество изображения, приближающееся к качеству кинопленки; совместимость каналов, предназначенных для передачи различной информации, меньшие мощности передатчиков при той же зоне обслуживания и др.

Первыми на ЦТВ перешли Люксембург и Нидерланды. В Берлине аналоговое ТВ прекращено в 2003 г. В России разработана Федеральная целевая программа развития цифрового ТВ, которая должна быть реализована к 2015 г. В Японии разработан стандарт телевидения высокой четкости ТВВЧ (High Definition Television—HDTV) для передачи и приема телевизионных сигналов с разрешением 1 125 строк, вдвое превышающим разрешение, обеспечиваемое используемой в настоящее время технологией.

Наблюдается интеграция систем связи и вещания. По сетям кабельного ТВ и распределительным ТВ-системам типа MMDS (Multichannel Multipoint Distribution Service — многоканальная многоточечная распределенная служба связи) передаются не только программы ТВ, но и различные данные, в том числе IP-телефония. В системе цифрового телевидения DVB (Digital Video Broadcasting — европейский проект по цифровому телевидению) можно передать программы звукового вещания и дополнительную информацию. ТВ-программы можно принимать на мобильные телефоны.

Развитие систем мобильной связи будет происходить в направлении совершенствования транкинговой связи, при которой канал выделяется абоненту в начале сеанса и освобождается по его окончании, сотовой связи, мобильного ТВ, систем широкополосного радиодоступа, мобильного Internet с использованием систем подвижной и спутниковой связи. Широкому распространению и мобильности оконечных устройств и терминалов, а тем самым глобальной мобильности и повсеместности их использования способствуют беспроводные средства и миниатюризация.

Интеллектуализация телекоммуникационных сетей стала возможной благодаря применению микроэлектроники и использованию программного обеспечения в каждом сетевом устройстве. Она позволяет увеличить гибкость телекоммуникационных сетей, расширить их функциональные возможности и повысить надежность, а также упростить управление глобальными сетями даже в неоднородных средах.

Список литературы

1. *Виснадул Б.Д.* Основы компьютерной техники / Б.Д. Виснадул, С.А. Лупин, С.В. Сидоров и др. ; под ред. Л.Г. Гагариной. — М. : ФОРУМ : ИНФРА-М, 2007. — 272 с.

2. *Гук М.* Аппаратные средства локальных сетей. Энциклопедия / М. Гук. — СПб. : Питер, 2005. — 573 с.

3. *Кузин Л.В.* Компьютерные сети : учеб. пособие / А.В. Кузин. — 3-е изд., перераб. и доп. — М. : ФОРУМ : ИНФРА-М, 2011. — 192 с.

4. *Куроуз Д.* Компьютерные сети / Д. Куроуз, К. Росс. — 2-е изд. — СПб. : Питер, 2004. — 765 с.

5. *Максимов Н.В.* Компьютерные сети : учеб. пособие / Н.В. Максимов, И.И. Попов. — 3-е изд., испр. и доп. — М. : ФОРУМ, 2008. — 448 с.

6. *Нанс Б.* Компьютерные сети / Б. Нанс ; пер. с англ. — М. : Бином, 1996. — 400 с.

7. *Новожилов Е.О.* Компьютерные сети : учеб. пособие / Е.О. Новожилов, О.П. Новожилов. — М. : Издательский центр «Академия», 2011. — 304 с.

8. *Олифер В.Г.* Компьютерные сети: Принципы, технологии, протоколы : учебник / В.Г. Олифер, Н.А. Олифер. — 1-е изд. — СПб. : Питер, 2000. — 672 с.

9. *Олифер В.Г.* Компьютерные сети: Принципы, технологии, протоколы : учебник / В.Г. Олифер, Н.А. Олифер. — 3-е изд. — СПб. : Питер, 2006. — 958 с.

10. *Олифер В.Г.* Сетевые операционные системы / В.Г. Олифер, Н.А. Олифер. — СПб. : Питер, 2002. — 544 с.

11. *Спортак М.* Компьютерные сети и сетевые технологии / М. Спортак, Ф. Паппас и др. ; пер. с англ. — К. : ТИД «ДС», 2002. — 736 с.

12. *Таненбаум Э.* Компьютерные сети / Э. Таненбаум. — 4-е изд. — СПб. : Питер, 2008. — 992 с.

13. *Шиндер Д.* Основы компьютерных сетей / Д. Шиндер ; пер. с англ. ; под ред. В.С. Александрова. — М. : Вильямс, 2003. — 656 с.

Оглавление

Предисловие ... 4

Глава 1. СТРУКТУРНО-ФУНКЦИОНАЛЬНАЯ ОРГАНИЗАЦИЯ СЕТЕЙ ... 6

1.1. Общие сведения ... 6
1.2. Классификация сетей ... 10
1.3. Характеристики сетей и качество услуг ... 16
1.4. Сетевые устройства ... 20

Глава 2. КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ СЕТЕЙ ... 27

2.1. Стандартизация и сетевые модели ... 27
2.2. Семиуровневая сетевая модель ... 31
2.3. Стеки протоколов ... 38

Глава 3. ФОРМИРОВАНИЕ И ОБРАБОТКА СИГНАЛОВ ... 49

3.1. Сигналы как способ представления информации ... 49
3.2. Кодирование сигналов ... 58
3.3. Компрессия-декомпрессия данных ... 65
3.4. Обнаружение и исправление ошибок ... 67

Глава 4. БАЗОВЫЕ СЕТЕВЫЕ ТЕХНОЛОГИИ ... 72

4.1. Методы доступа к сети ... 72
4.2. Методы коммутации и передачи данных ... 77
4.3. Адресация узлов сети ... 83
4.4. Принципы, алгоритмы и протоколы маршрутизации ... 89

Глава 5. СЕТЕВОЕ ОБОРУДОВАНИЕ ... 94

5.1. Линии связи и их характеристики ... 94
5.2. Кабельные среды передачи данных ... 99
5.3. Беспроводная среда ... 106
5.4. Использование мостов для логической структуризации сети ... 109
5.5. Коммутаторы локальных сетей и их функции ... 113

Глава 6. ЛОКАЛЬНЫЕ СЕТИ ... 122

6.1. Сети Ethernet ... 122
6.2. Особенности сетей Token Ring, AppleTalk и ARCnet ... 140
6.3. Персональная радиосеть Bluetooth ... 142

Глава 7. ГЛОБАЛЬНЫЕ СЕТИ ... 145

7.1. Введение в глобальные сети ... 145
7.2. Сети плезиохронной цифровой иерархии ... 151
7.3. Синхронные сети SONET/SDH ... 153

7.4. Сети DWDM ... 158
7.5. Сети X25 ... 161
7.6. Сети Frame Relay ... 164
7.7. Сети ISDN ... 167
7.8. Сети ATM ... 169
7.9. Абонентские линии DSL ... 173
7.10. Сеть Internet ... 174

Глава 8. АДМИНИСТРИРОВАНИЕ СЕТЕЙ ... 182

8.1. Задачи и принципы управления сетями ... 182
8.2. Управление учетными записями, ресурсами и адресами ... 189
8.3. Введение в безопасность сетей ... 193
8.4. Средства обеспечения безопасности ... 196
8.5. Мониторинг сети ... 205
8.6. Неполадки в сетях и их устранение ... 211

Заключение ... 220
Список литературы ... 222

Учебное издание

Новожилов Евгений Олегович
Новожилов Олег Петрович

Компьютерные сети

Учебное пособие

4-е издание, стереотипное

Редактор *Л. В. Толочкова*
Технический редактор *Е. Ф. Коржуева*
Компьютерная верстка: *Р. Ю. Волкова*
Корректоры *А. П. Сизова, И. А. Ермакова*

Изд. № 104114714. Подписано в печать 01.07.2014. Формат 60 × 90/16. Бумага офс. № 1. Гарнитура «Балтика». Печать офсетная. Усл. печ. л. 14,0. Тираж 1 000 экз. Заказ № 945.

ООО «Издательский центр «Академия». www.academia-moscow.ru
129085, Москва, пр-т Мира, 101В, стр. 1.
Тел./факс: (495) 648-0507, 616-00-29.
Санитарно-эпидемиологическое заключение № РОСС RU. АЕ51. Н 16592 от 29.04.2014.

Отпечатано с электронных носителей издательства.
ОАО «Тверской полиграфический комбинат», 170024, г. Тверь, пр-т Ленина, 5.
Телефон: (4822) 44-52-03, 44-50-34. Телефон/факс: (4822) 44-42-15.
Home page — www.tverpk.ru Электронная почта (E-mail) — sales@tverpk.ru