

Высшее профессиональное образование

Р. Л. Смелянский

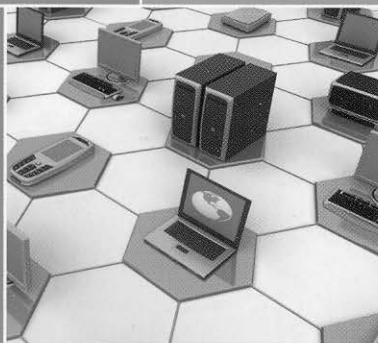
# КОМПЬЮТЕРНЫЕ СЕТИ

В двух томах

Том 1

СИСТЕМЫ ПЕРЕДАЧИ ДАННЫХ

Учебник



Информатика  
и вычислительная  
техника

УДК 004.7(075.8)  
ББК 32.973.202я73  
С501

Рецензенты:

зав. кафедрой вычислительной техники МЭИ (ТУ), д-р техн. наук, проф.  
*В. В. Топорков*; декан факультета вычислительной математики  
и кибернетики Казанского государственного университета, зав. кафедрой системного анализа и  
информационных технологий, проф. *Р. Х. Латыпов*;  
зав. кафедрой теоретической информатики Ярославского государственного универ-  
ситета им. П. Г. Демидова, д-р физ.-мат. наук, проф. *В. А. Соколов*

**Смелянский Р. Л.**

С501 Компьютерные сети : в 2 т. Т. 1. Системы передачи данных /  
Р. Л. Смелянский. — М. : Издательский центр «Академия»,  
2011. — 304 с.

ISBN 978-5-7695-7151-0

Приведены теоретические основы систем передачи данных, характери-  
стики основных видов физических сред, способы кодирования и передачи  
аналоговых и цифровых данных, основы организации компьютерных сетей и  
систем передачи данных. Рассмотрены основы международной и отечествен-  
ной систем стандартизации в области компьютерных сетей, эталонная модель  
взаимодействия открытых систем, основы сетевого стека OSI, организация и  
основные принципы функционирования современных систем передачи дан-  
ных, протоколы канального уровня, а также даны многочисленные примеры  
систем передачи данных.

Для студентов учреждений высшего профессионального образования.

УДК 004.7(075.8)  
ББК 32.973.202я73

*Оригинал-макет данного издания является собственностью Издательского  
центра «Академия», и его воспроизведение любым способом без согласия  
правообладателя запрещается*

ISBN 978-5-7695-7151-0 (т. 1)  
ISBN 978-5-7695-7152-7

© Смелянский Р. Л., 2011

© Образовательно-издательский центр «Академия», 2011

© Оформление. Издательский центр «Академия», 2011

## ПРЕДИСЛОВИЕ

Данный учебник написан на основе материалов лекций по курсу «Компьютерные сети», который читается на факультете «Вычислительная математика и кибернетика» (ВМиК) Московского государственного университета им. М. В. Ломоносова.

Учебник, прежде всего, предназначен для подготовки специалистов и бакалавров по направлениям «Прикладная математика и информатика» и «Фундаментальная информатика и информационные технологии», а также по направлению «Информатика и вычислительная техника».

В учебнике не рассматриваются сетевые операционные системы, поскольку, во-первых, сегодня само понятие сетевой операционной системы выглядит странно, так как любая современная операционная система предполагает наличие функциональности для поддержки сетевого взаимодействия; во-вторых, на эту тему уже достаточно много издано литературы, а в-третьих, на факультете ВМиК курсу «Компьютерные сети» предшествуют курсы «Операционные системы», «Базы данных» и «Программирование на языке Java».

Основной целью курса «Компьютерные сети» в т. 1 «Системы передачи данных» является приобретение студентами знаний и навыков в следующих областях:

- современные системы международной и отечественной стандартизации в области инфокоммуникационных технологий;
- основы построения и архитектуры сетей телекоммуникации;
- принципы построения, параметры и характеристики цифровых и аналоговых каналов передачи данных;
- современные технологии телекоммуникации;
- основные стандарты, используемые в инфокоммуникационных системах и технологиях;
- теоретические основы архитектурной и системотехнической организации вычислительных сетей, построение сетевых протоколов;
- выбор и комплексирование программно-аппаратных средств сетей телекоммуникации;
- конфигурирование локальных сетей и реализация сетевых протоколов с помощью программных средств.

На факультете ВМиК МГУ при изучении курса «Компьютерные сети» используется практикум, включающий в себя пять лабораторных заданий и семь контрольных тестов. Организация изучения

курса на факультете ВМиК также предусматривает систему промежуточного контроля знаний студентов. (Автор готов поделиться презентационными материалами, а также материалами практических упражнений и промежуточного контроля с желающими, для чего достаточно обратиться с вопросом по адресу [smel@CS.MSU.SU](mailto:smel@CS.MSU.SU).)

Изучение данного курса предполагает наличие определенного объема знаний у студентов, т.е. они должны *знать* архитектуру современных вычислительных систем, организацию и функционирование операционной системы Unix и ее файловой системы, организацию и функционирование систем управления базами данных, элементы интегрального и дифференциального исчисления, разложение функции одной переменной в ряд, основы теории рядов, основы теории вероятностей и математической статистики, элементы теории массового обслуживания (теории очередей), основы дискретной математики в части комбинаторики, теории графов и сетей, теории автоматов.

Помимо этого студенты должны иметь практический опыт программирования, например на ассемблере и на языке C. Также желательно знать объектно-ориентированное программирование и язык Java, уметь строить математические модели.

Темпы развития сетевых технологий и глубина их проникновения в жизнь общества столь велики, что за годы чтения данного курса автору постоянно приходилось дополнять материал, включать в него новые технологии, новые сетевые средства и протоколы. Каждый год курс дополнялся и изменялся.

Основными критериями при отборе материалов для включения в курс были следующие:

- перспективность технологии;
- наличие международного стандарта (или проведение процесса стандартизации) по данной технологии;
- актуальность данной технологии для России.

Как уже было сказано, материал курса разбит на два тома.

Первый том посвящен общим вопросам организации компьютерных сетей и проблематике телекоммуникационных сетей или сетей передачи данных. Во избежание путаницы термин «сеть» используется автором для сетей ЭВМ, а применительно к телекоммуникациям его заменяет термин «системы передачи данных».

Второй том данного учебника посвящен описанию работы сетевого, транспортного и прикладного уровней современных сетей ЭВМ.

Ну, и наконец, осталось самое приятное — поблагодарить всех тех, кто помогал автору, высказывая критические замечания, что способствовало улучшению данного курса.

Прежде всего, хотелось бы поблагодарить студентов третьего потока факультета ВМиК, которые слушали курс в 1995—2008 гг. и своими замечаниями, критикой способствовали его улучшению.

Автор также признателен Д. Гамаюнову, помогавшему ему работать с рукописью, С. Мониному — за материалы по технологии WiFi, Д. Чамберсу, Э. Перес, Р. Эйджи — за предоставленные материалы о компании Cisco Systems и ее продуктах, М. Свердликову, О. Типисову — за обсуждение разных разделов курса, труд по прочтению рукописи и критику, способствовавшую улучшению материала, Д. Козлову и М. Забейайло — за обсуждение и конструктивные предложения отдельных частей курса, Н. Трусовой и Е. Капинус — за работу по подготовке рукописи. Особенно хотел бы отметить доброжелательность Ю. В. Коровина, без поддержки которого эта книга вряд ли появилась.

Москва

1 августа 2010 г.

*Р. Л. Смелянский*

## ВВЕДЕНИЕ В ПРЕДМЕТ

### 1.1. Шок будущего

В каждом из трех предшествующих столетий существовала технология, уровень которой определял уровень развития цивилизации. Известный социолог и футуролог Э. Тоффлер в [42] выделяет три технологические эпохи: аграрную, индустриальную и эпоху, которой пока не найдено адекватного названия. Но, безусловно, информационные технологии — технологии сбора, передачи, обработки, визуализации и хранения информации играют в этой третьей эпохе определяющую роль.

Мы живем в уникальное время. Наука насчитывает 50 000 лет существования современного человека. Если, следуя Э. Тоффлеру, разделить этот срок на периоды по 62 года, то получим примерно 800 периодов, причем прошло только 150 таких периодов с тех пор, как люди вышли из пещер. При этом только на протяжении последних двух с небольшим периодов люди научились использовать паровые двигатели, электричество, двигатели внутреннего сгорания, атомную энергию, радио, телефон, телевизор, и лишь в последнем периоде люди узнали о вычислительной технике и информационных технологиях.

Для автомобилизации и телефонизации 80 % населения Земли потребовалось около 110 лет, для распространения использования электрической энергии — 80 лет, для персонального компьютера и Интернета — чуть более 20 лет, а для Всемирной паутины (World Wide Web) — всего 6 лет!

Из сказанного видно, что темпы смены технологий в мире [43], а также уровни интеллектуализации и энерговооруженности труда людей постоянно растут.

### 1.2. Предпосылки появления сетей ЭВМ и развития информационных технологий

#### 1.2.1. Появление технически сложных систем

Отметим две главные предпосылки появления сетей ЭВМ и развития информационных технологий: создание технически сложных

систем и необходимость быстрого получения, накопления и обработки информации.

Новые способы получения энергии открыли новые горизонты в развитии промышленности. Однако создание технически сложных систем потребовало принципиально новых подходов к их проектированию. Так, технически сложную систему (например, ядерный реактор, самолет, космический корабль, спутниковую систему) не всегда можно представить в натуральном виде. Требуются моделирование, сложные расчеты, вычислительные схемы, специальные методы борьбы со сложностью и создаваемого изделия, и его модели. Например, увеличение числа взаимодействующих компонентов системы ведет к усложнению ее конструкции, а следовательно, к снижению надежности. При этом возникает следующий не праздный вопрос: как убедиться, что создаваемая система при любых обстоятельствах будет функционировать корректно?

Новые задачи проектирования обусловили новые требования к скоростям расчетов, алгоритмам расчетов, численным методам, средствам моделирования. Уже в 1940-х гг. основным местом для ускорения ручных расчетов было их распараллеливание, при котором несколько человек — счетчиков — работали параллельно над разными частями одного и того же расчета.

При этом без моделирования и предварительного численного анализа создавать сложные технические системы было уже невозможно [55]. Здесь уместно вспомнить случай с Э. Ферми, рассказанный его женой Л. Ферми в [46]. В проекте «Манхеттен» по созданию атомной бомбы Э. Ферми отвечал за разработку системы безопасности ядерного реактора. После многомесячных усилий ему принесли на утверждение сложнейшую схему трубопроводов, клапанов и другого оборудования, которая занимала несколько ватмановских листов формата А1. Подумав некоторое время, Э. Ферми указал на несколько клапанов и спросил, что произойдет, если некоторые из них он закроет, а некоторые окажутся в определенных различных состояниях. Инженеры, проведя в размышлениях несколько часов, ответили, что произойдет взрыв, и спросили, как ему удалось так быстро найти изъян в их проекте. Тот ответил, что методы проектирования этой системы не соответствовали ее сложности, поэтому она должна быть ненадежной. А то, что он сразу нашел изъян — это случай. Этот пример говорит о том, что чем сложнее система, тем менее она надежна, и что для проектирования сложных систем требуются специальные методы. Также следует отметить, что именно проект «Манхеттен» оказал значительное влияние на развитие вычислительной техники [55].

При этом создать объект было уже мало: его надо было уметь поддерживать в работоспособном состоянии, выявлять неисправности, ремонтировать при выходе из строя, модифицировать и развивать в ходе эксплуатации, т. е. эксплуатация технически сложных систем

потребовала специальной организации работ, где без информационных технологий обойтись было нельзя.

### **1.2.2. Повышение эффективности управления**

Помимо технических предпосылок определяющую роль в развитии информационных технологий сыграли предпосылки социальные. Прежде всего, надо помнить, что информации всегда не хватало и стоила она дорого. Примерами к этому тезису могут служить истории дипломатии, разведок [4, 49, 78].

В обществе XX в. налицо были следующие тенденции:

- демографический рост;
- концентрация капитала, индустриализация развитых стран и децентрализация управления;
- рост числа людей, вовлекаемых в процессы принятия решений.

При развитии данных тенденций отсутствие эффективных методов коммуникации, распределенного доступа к информации, автоматизации ее сбора, обработки и хранения тормозили развитие индустриализации как на внутрисоюзном, так и на международном уровнях.

Скорость принятия решения можно представить в виде числового значения и измерить в стоимостном выражении. По аналогии с транспортным средством можно сказать, что чем медленнее вы реагируете на изменение обстановки на дороге (т.е. принимаете решение), тем ниже должна быть скорость движения автомобиля.

Старые технологии сбора и обработки информации предполагали сбор информации на местах с заполнением специально разработанных форм, собираемых соответствующими государственными структурами, где они, возможно, проходили предварительную обработку, после чего отправлялись далее по инстанциям. При этом в начале XX в. путешествие из Москвы за Урал, а следовательно, и обмен документами занимали несколько месяцев. Необходимыми стали новые быстрые средства коммуникации. Таким образом появились телеграф, телефон, радио, телевидение.

Обратим внимание, что каждый из перечисленных видов связи был предназначен для передачи вполне определенных видов данных: телефон — голоса, радио — аудиоданных, телевидение — видеоданных. Постепенно возникла необходимость интеграции этих видов связи. Например, передачи по радиоканалу как аудио-, так и видеоданных, или по телефонному каналу — видеоданных. Важной тенденцией наших дней является то, что телефонные, телевизионные, радио- и спутниковые сети связи, используемые в технологиях сбора, передачи, обработки и хранения информации, начинают сливаться и интегрироваться в единую сеть.

Интеграция компьютеров со средствами передачи данных коренным образом изменила представление об организации вычислитель-

ных систем. Появились сети ЭВМ. Правда, в первых сетях ЭВМ средства связи использовались именно для соединения между собой ЭВМ, т. е. изначально это были специализированные средства, предназначенные только для соединения ЭВМ. Потом пришло осознание того, что для этих целей можно использовать существующие средства коммуникации. Однако разнообразие этих средств создавало существенные сложности для их использования как средств коммуникации ЭВМ, т. е. желательно было научиться по одному и тому же каналу передавать как цифровые данные, так и аудио- и видеоданные. Другими словами, возникла проблема интеграции разнородных сетей связи между собой.

Появление и развитие сетей ЭВМ и средств коммуникации были востребованы военными и промышленностью. Военным требовались надежные живучие системы коммуникации, которые невозможно уничтожить однократным ударом, а также надежные высокоскоростные системы сбора и обработки информации. Промышленности требовались средства, обеспечивающие эффективное управление производством, развитие и расширение рынка.

*Сети ЭВМ стали основой информационных технологий.* Сегодня управление компаний или предприятием невозможно без информационных систем, которые во многом определяют скорость адаптации компании к изменяющимся внешним условиям и ее способность быстро и экономически эффективно управлять своей деятельностью.

Не меньшее значение информационные технологии имеют и для отдельной личности. Ярким примером является их применение для развития различных форм и методов обучения людей. Следует отметить, что в современных условиях изменилась роль и значение образования в деятельности любого государства.

По оценкам, приведенным в [48], в 1905 г. число рабочих мест, где требовалось образование, составляло 10... 15 % от общего числа рабочих мест в мире, а в 1995 г. уже 75... 80 % рабочих мест требовали образования не ниже среднего технического. Эти цифры говорят, во-первых, о росте интеллектуализации рабочих мест, а во-вторых, о том, что промышленность не может работать без притока образованных специалистов. Если в конце XIX и в начале XX вв. основной функцией образования было развитие личности, то теперь — это обеспечение промышленности профессиональными кадрами. Сегодня уже речь идет об образовании, проходящем через всю жизнь человека, поскольку темпы развития производственных технологий требуют постоянного развития обслуживающего персонала. Эти тенденции существенно усложняют процессы глобализации в экономике, требуя унификации образовательных стандартов в разных странах.

Таким образом, конкурентоспособность как отдельного предприятия, так и государства в целом напрямую теперь зависит от развития информационных технологий.

## 1.3. Три движущие силы информационных технологий

### 1.3.1. Некоторые факты из истории компьютеров

Состояние и направление развития информационных технологий определяют три основные составляющие: микроэлектроника, телекоммуникации и инженерия программного обеспечения.

Напомним основные исторические факты.

1946 г. считают годом создания первого компьютера ENIAC. Работа над этим проектом была начата в 1943 г. Руководителем этого проекта был Д. Моучли, а техническим лидером — Д. Эккерт. Машина весила 27 т, содержала 18 000 электронных ламп, 1 500 реле и потребляла около 150 кВт энергии [28].

В 1946 г. эти же специалисты начали работу по заказу правительства США над новым проектом EDVAC — электронным автоматическим вычислителем с хранимой программой. Идеи, положенные в основу этого проекта, были опубликованы Д. Нейманом, которому впоследствии они и были приписаны. В 1951 г. была создана машина UNIVAC, предназначенная для решения разнообразных задач.

Приведенные факты общеизвестны, и во многом благодаря этому родоначальниками ЭВМ считают американцев. Однако, как свидетельствуют документы, опубликованные в конце XX и в начале XXI вв., это первенство не столь однозначно.

Одним из претендентов на право лидерства является немецкий ученый К. Цузе [2, 14], под руководством которого в 1941 г. была построена машина Z3, основанная на двоичной системе исчисления. Эта машина, созданная по заказу Института аэродинамических исследований Люфтваффе, была оснащена языком программирования Plankalkul, а ввод данных в нее осуществлялся с перфолент. Работы К. Цузе активно использовались в фашистской Германии. Этот политический факт бросил тень на его работы, и сегодня они малоизвестны.

Претендентами на лидерство также являются создатели компьютера Colossus [63], который был создан в Великобритании в 1943 г. и запущен в эксплуатацию в феврале 1944 г. Возглавляли этот проект математик М. Ньюмен и инженер Т. Флауэрс. Машина создавалась для решения суперсекретных задач вскрытия зашифрованной дипломатической переписки, поэтому первая информация о них стала известна только в 1970-е гг. в результате рассекречивания американских документов [17, 47]. Эта машина, в частности, обеспечивала вскрытие переписки высшего командования фашистской Германии, благодаря чему время вскрытия шифровок сократилась с нескольких недель до 2—3 ч. Машина Colossus-Mk1 имела 1 500 электронных ламп.

В 1944 г. англичане построили более мощную машину Colossus-Mk2, которая состояла из 2 500 ламп и выполняла 100 булевских

операций в секунду. До конца Второй мировой войны было построено 10 таких машин. В 1945 г. Уинстон Черчилль, опасаясь, что руководство СССР узнает о проекте Colossus, лично приказал демонтировать и уничтожить восемь из десяти машин. Оставшиеся две машины эксплуатировались еще полтора десятка лет в условиях строжайшей тайны в Блетчли-Парк, в криптографической службе Великобритании. После чего также были уничтожены.

### **1.3.2. Микроэлектроника и закон Мура**

В 1947 г. В. Шокли, Д. Барден и У. Бретеин разработали точечный транзистор — первый полупроводной усилитель. В 1956 г. они получили Нобелевскую премию по физике. Любопытно отметить, что примерно в это же время был разработан электровакуумный прибор — нувистор, который по электрическим параметрам превосходил транзистор, а по массово-габаритным — уступал, но немного. Однако транзистор победил! Причина этой победы — принципиально новая технология — создание полупроводниковых схем на кремниевой пластинке. Так был дан старт кремниевой технологии, которая действует в области микроэлектроники по сей день.

Этот новый прибор совершил революцию в электронике. В 1971 г. появился первый микропроцессор Intel 4004, который работал с частотой 108 кГц и содержал 2 300 транзисторов. Но уже через семь лет, в 1978 г., в микропроцессоре Intel 8086 транзисторов было около 29 000, т.е. их число возросло больше, чем в 10 раз, и работал он с частотой 5 МГц, т.е. частота возросла почти в 50 раз! Еще через 23 года микропроцессор Pentium 4 работал уже с частотой 1,7 ГГц (т.е. за 30 лет частота выросла более чем в 1 000 раз), а число его транзисторов составило 42 млн (т.е. почти в 20 тыс. раз больше, чем в Intel 4004). С 1971 г. тактовая частота процессоров Intel возросла в 28 тыс. раз, т.е. со 108 кГц до 3 ГГц, а среднее число транзисторов в одном процессоре выросло в 350 тыс. раз.

Тенденция увеличения числа транзисторов на кристалле была сформулирована в 1965 г. Г. Муром (одним из основателей Intel) в виде закона, который носит его имя: количество транзисторов в интегральной схеме с минимальной ценой удваивается каждые 18 месяцев [11]. По оценкам экспертов, эта тенденция сохранится до 2011 г.

Если экстраполировать эту тенденцию, то в 2010 г. должен быть получен кристалл с 3 млрд транзисторов, а к 2020 г. — со 140 млрд транзисторов. Напомним, что мозг человека вмещает около 100 млрд нейронов. Если закон Мура будет действовать в течение ближайших 70 лет, то к концу этого срока появятся схемы памяти размером с песчинку, имеющие емкость 30 Тбайт. Это означает, что на таком кристалле можно будет сохранять видеозапись целой человеческой жизни.

В настоящее время параллельно с развитием кремниевых технологий активно развиваются новые виды полупроводников на основе

нанотехнологий и создаются оптические электронные схемы, способные работать с электромагнитными импульсами [24, 25, 54].

### **1.3.3. Компьютеры на основе микропроцессоров**

И сам компьютер, и его интерфейс с человеком подверглись существенным изменениям. Вспомним, что персональный компьютер (ПК) впервые появился в 1981 г., и за следующие 20 лет он совершил революцию: до этого он был доступен только специалистам, а теперь он «вошел» почти в каждый дом, с ним работают школьники, он стал мобильным. Оконный интерфейс, мышка, скоростной доступ в Интернет принципиально изменили область применения компьютеров. В настоящее время в мире функционирует более 1,5 млрд ПК!

В начале XXI в. появился новый класс компьютеров — карманный персональный компьютер (КПК), у которого есть мультипрограммный режим, большая RAM и процессор большой мощности. Тактовая частота процессора современного КПК более 500 МГц. Напомним, что у микропроцессоров первых ПК тактовая частота была всего 5 МГц. Современный КПК имеет оконный интерфейс, голосовое управление, беспроводные интерфейсы Bluetooth, WiFi, GPRS, он может работать с аудио- и видеофайлами, с GPS-приемниками и Интернетом.

Появился целый класс новых устройств, ориентированных на новые интерфейсы. Это, например, и Tablet PC, и электронные рамки для цифровых фото, в которых можно менять изображение. Эти устройства способны снимок, сделанный камерой сотового телефона на одном конце Земли, передать по сети и воспроизвести в такой рамке на другом конце Земли за считанные минуты.

Отдельный класс устройств на основе микропроцессоров составляют встроенные системы. Это весьма широкий класс устройств: от бытовых приборов до сложных технических систем. К бытовым приборам относятся такие устройства, как фото- и видеокамеры, аудиоустройства (iPod), микроволновые печи, холодильники, часы и т. д. Технически сложными являются космические системы (например, спутниковые системы связи), управляющие комплексы летательных аппаратов, автомобилей, кораблей, интеллектуальные дома и т. п.

Уже в 2002 г. устройства, не являющиеся персональными компьютерами, составляли около 50 % от всех устройств доступа в Интернет, а к 2005 г. число таких устройств превысило число ПК. К 2005 г. на одного жителя Европы и Северной Америки в среднем приходилось около 20 микропроцессоров, размещенных в бытовых приборах.

Сегодня микропроцессор можно встретить везде: в кроссовках, кастрюлях, автомобилях, самолетах, на кораблях. В 2007 г. число компьютеров, подключенных к Интернету, оценивалось в 1 млрд 370 млн штук, в то время как общее количество функционирующих чипов превысило 20 млрд.

Ирония наших дней состоит в том, что отдельный компьютер «сделал свое дело», эра компьютеров прошла! Дальнейшее развитие связано с интеграцией компьютеров и средств связи.

### **1.3.4. Телекоммуникации и закон Гилдера**

В настоящее время, с одной стороны, компьютеры объединяют в сети, оборудуя их необходимыми средствами телекоммукации, а с другой стороны, традиционные средства коммуникации, такие как телефон, превращают из простого средства передачи голоса в изощренные средства интерактивного беспроводного взаимодействия.

Уже в 1998 г. в Финляндии более 50 % населения имели сотовые телефоны. Сегодня мы звоним человеку не туда, где он может находиться, а непосредственно ему. К концу 2003 г. в мире было больше пользователей wireless, чем wired. В 2004 г. в Европе насчитывалось около 50 млн пользователей приложений WAP (Wireless Application Protocol). В настоящее время с сотовых телефонов ежедневно отправляется около 1 млрд SMS-сообщений. Это уже нечто большее, чем телефонный разговор. Технология GPRS (General Packet Radio Service) позволяет wireless-пользователям уже сегодня обмениваться данными со скоростью до 144 Кбит/с, а применение технологии UMTS обеспечивает скорость обмена данными до 2 Мбит/с. Это уже не телефон, это коммуникатор.

Скорость распространения этих устройств впечатляет. Например, только за последние три месяца 2006 г. их было продано 244,9 млн штук (больше, чем население России), а за весь 2006 г. — 1,02 млрд штук. Настоящий фурор произвело появление на рынке в 2007 г. iPhone от Apple. Фирма Apple заново изобрела телефон, который объединяет в себе возможности iPod, изменивший в 2001 г. всю музыкальную индустрию, инновационный мобильный телефон и интернет-коммуникатор с интерфейсом радикально нового типа.

Изменились и кабельные (wired) средства коммуникации. Сегодня по обычной домашней телефонной линии благодаря технологии ADSL обеспечивается скорость обмена информацией до 2 Мбит/с. В Европе число пользователей высокоскоростными соединениями с 2002 по 2005 г. выросло в шесть раз. В России общая цифра числа пользователей высокоскоростными каналами не столь велика, но она очень быстро растет, примерно на 30 % в год. Правда, пока такие темпы роста задают Москва и Санкт-Петербург, но уже в 2007 г. был отмечен большой рост числа подключений к высокоскоростным каналам связи и в регионах России.

Если в области микропроцессорной техники в настоящее время действует закон Мура, то в области телекоммуникаций действует закон Гилдера [67], выявивший на основании статистических данных следующую тенденцию: пропускная способность телекоммуникацион-

ных каналов удваивается каждые шесть месяцев, т. е. она растет почти втрое быстрее, чем производительность кристаллов!

Современная система передачи данных, или просто кабель, за секунду способна пропустить столько данных, сколько в 1997 г. пропускал весь Интернет. Так, например, в 1997 г. Ethernet обладал пропускной способностью в 100 Мбит, а сегодня это 100 Гбит, т. е. за 10 лет скорость выросла в 1 000 раз! К настоящему времени ежедневно через Интернет «прокачивается» около 10 Эксабайт (1 эксабайт =  $2^{60}$  байт) данных. Это примерно 50 тыс. лет просмотра DVD [20].

Рассмотренные тенденции (закон Мура и закон Гилдера) буквально «взорвали» общество. На рынке стали появляться такие сервисы, о которых люди раньше и не мечтали. Сотовый телефон превратился из средства голосового общения в средство доступа к разнообразной информации и в GPS-навигатор. Кроме того, он позволяет водителю, не выходя из машины, получать доступ к информации о пробках на дорогах, к своей электронной почте, просмотру видеоданных и многое, многое другое.

На сегодня ни один автомобиль бизнес-класса не обходится без бортовой сети, которая обеспечивает доступ к GPS-навигатору, Интернету, а также разнообразному multimedia-контенту. Если такой автомобиль обнаружит у себя какие-либо неполадки, то он сам свяжется с сервис-центром, оповестит водителя, проложит маршрут до ближайшего сервис-центра и даже вызовет такси.

Появление таких wireless-технологий, как WiFi и WiMAX, позволило кардинально изменить мобильность компьютеров. Сегодня трудно представить отель или аэропорт без точек беспроводного доступа. Развитие телефонных сетей, сотовых сетей связи, технологий WiFi и WiMAX заставляет переосмыслить многие сложившиеся представления об информационных сервисах.

Благодаря перечисленным сетевым возможностям кардинально изменилась роль видеoinформации в Интернете. Об этом красноречиво говорят следующие данные, предоставленные компанией Cisco Systems: в 2005 г. в Интернете насчитывалось 5 млрд видеопотоков в год, в 2006 г. — 31 млрд, а в 2007 г. — 70 млрд. Сейчас в США пять взб-сайтов за год генерируют столько видеопотоков данных, сколько их было сгенерировано в США за весь 2000 г., т. е. 60 % трафика в Интернете составляют видеоданные. Стремительно растет число пользователей технологии Telepresence, обеспечивающей новый вид коммуникации, создающий эффект присутствия собеседника, который физически находится совсем в другом месте. Поток данных, генерируемых таким приложением, как Telepresence, за 1 ч, равен объему переписки участников по e-mail за год.

Совершенно иначе начинают выглядеть и инженерные коммуникации современных жилищ. Если мыслить представлениями 1980-х и 1990-х гг., то наши жилища должны выглядеть, как джунгли из проводов электрических сетей, телевизионных сетей, радиосетей, про-

тивопожарных систем, кабельного телевидения, бытовых приборов и других, каждая из которых должна была бы иметь отдельный ввод в нашу квартиру. Теперь доступ к этим многообразным сетям можно обеспечить с помощью одного кабеля и технологии Unified Commu- cation.

Технология Jini [41], предложенная Б. Джойем из Sun Microsystems, произвела революцию в бытовой электронике. При ее использовании бытовой прибор ищет сеть, через которую сам может загрузить новое программное обеспечение, взаимодействовать с другими бытовыми приборами, сообщать в технический центр о своих неполадках и т. д.

Вдумываясь в приведенные факты, нельзя не согласиться с Г. Хамелом, который написал: «Технология доступна всем; что не так широко известно, так это умение предугадывать инновационные способы ее нового и уникального использования, которые позволят создать конкурентные преимущества» [68].

## **1.4. Кто, как и для чего использует сеть Интернет**

### **1.4.1. Общие сведения**

Сейчас в интересах логики изложения мы должны отложить рассмотрение последней движущей силы информационных технологий — инженерии программного обеспечения, а рассмотреть кто, как и для чего использует Сеть\*.

Итак, дальнейшее развитие компьютера в значительной степени определяют его сетевые возможности. Говоря о применении сетей, разделим все области их использования на использование в организациях и на предприятиях, которое для краткости будем называть бизнесом, и на использование в индивидуальных целях.

В сфере бизнеса можно выделить области применения сетей в следующих направлениях:

- интранет — использование сети для управления и производственных нужд внутри предприятия;
- B2B (Business To Business) — взаимодействие с другими предприятиями, которые, в свою очередь, можно подразделить на взаимодействие с предприятиями-заказчиками, взаимодействие с предприятиями-поставщиками и создание виртуальных предприятий;
- B2C (Business To Customer) — взаимодействие предприятия с конечными пользователями их продукции;
- электронное правительство, которое, в свою очередь, разделяется на B2G (Business To Government) — взаимодействие предприятия с государством и G2C (Government To Citizen) — взаимодействие государства с гражданами;

\* Далее по тексту Сеть — это сети ЭВМ и телекоммуникации.

• C2C (client-To-client) — набор услуг (технологий), которые позволяют клиентам-физическим лицам обмениваться товарами или оказывать взаимные услуги.

### 1.4.2. Интранет

**Интранет** — это средства, обеспечивающие и регулирующие доступ сотрудников компании к внутрикорпоративным средствам коммуникации, информационным и вычислительным сервисам.

Схема организации интранет-сети показана на рис. 1.1.

Упрощенно интранет — это внутренняя корпоративная сеть, построенная на интернет-технологиях. Обратите внимание, что не все пользователи, расположенные слева на рис. 1.1, находятся в зоне сети интранет. Некоторые из них подключаются к корпоративным информационным ресурсам извне.

Интранет обеспечивает для всех сотрудников единый способ доступа к информации, единую унифицированную среду работы, единый формат документов. Такой подход позволяет сотрудникам наи-



Рис. 1.1. Схема организации интранет-сети

более эффективно использовать накопленные корпоративные знания, оперативно реагировать на происходящие события, где бы они ни находились, а предприятию в целом предоставляет новые возможности организации своего бизнеса.

Интерфейс доступа в интранет внешне имеет вид web-сайта (а точнее портала), который кроме обычных функций может идентифицировать сотрудника компании, отличить его от простого пользователя сетью и открыть доступ к тем информационным и вычислительным внутрикорпоративным сервисам, с которыми ему разрешено работать. К типовым сервисам относятся, например, средства планирования и управления временем сотрудника (календарь), адресная книга, с помощью которой сотрудник может найти контактную информацию о другом сотруднике, средства передачи сообщений и другие средства, с помощью которых можно связаться с другими сотрудниками, где бы он сам ни находился и где бы не находился его vis-a-vis.

Важной информационной услугой, осуществляемой через интранет, является доступ сотрудника к системе управления знаниями предприятия. Эта система призвана аккумулировать и хранить информацию и знания, возникающие в голове каждого сотрудника. Хорошо известно, сколько проблем возникает при увольнении сотрудника из организации. Основная причина этих проблем заключается в том, что сотрудник уносит в своей голове много полезной и важной информации. Система управления знаниями предприятия позволяет так организовать работу сотрудников, чтобы они сами систематически пополняли ее своими знаниями, таким образом знания остаются на предприятии и после ухода сотрудника.

Важными характеристиками интранета являются открытость и масштабируемость. Интранет должен позволять наращивать функциональность и интегрировать информационные прикладные системы организации. Это свойство позволяет предприятию развивать информационные системы эволюционным путем по мере возникновения необходимости.

### **1.4.3. Взаимодействие с другими предприятиями**

**B2B** — условное обозначение набора услуг, которые одна фирма может оказать другой, используя сеть Интернет. На сегодня сформировались два основных направления в этой сфере: интернет-биржи и интернет-консалтинг. Интернет-биржи являются несколько расширенным представлением обычных бирж с тем только отличием, что за счет больших возможностей по отображению визуальной информации с их помощью стала реальной торговля не только классическими биржевыми товарами, такими как нефть, зерно, металлы, но и некоторыми стандартными видами товарной продукции (оборудованием, комплектующими, компьютерной техникой и т.д.).

Интернет-консалтинг в Сети обеспечивает, в первую очередь, поиск и обработку информации из самой Сети (поиск поставщиков и потребителей, мониторинг, анализ рынков и т. д.).

Многие электронные биржи позволяют не только заключать сделки, но и планировать, а также управлять поставками. Управление поставками очень важно, так как позволяет регулировать стоимость конечного продукта. Например, если у какого-то поставщика продукция привлекательного качества, но при этом заказчиков не устраивает ее цена, то можно помочь ему снизить затраты на производство, например изменив состав его поставщиков и поставщиков второго уровня, а также точнее спланировать сроки поставок, сократив затраты на складские помещения и т. д. Такой подход к организации производства называется управлением цепочкой поставщиков (Chain Supplier Management — CSM).

Как это не парадоксально на первый взгляд, но, несмотря на жесткую конкуренцию на рынке, основной формой взаимодействия в сфере B2B является сотрудничество. Именно сотрудничество в виде создания тесных связей между поставщиками, производителями, заказчиками и заказчиками заказчиков позволяет быстро и гибко реагировать на любые изменения в цепочке заказов и поставок. И все это благодаря Сети.

О роли электронной формы взаимодействия между предприятиями говорят следующие цифры. По данным агентства IDC, общая стоимость товаров, проданных во всем мире через систему B2B, возросла с 282 млрд долл. в 2000 г. до 4,3 трлн долл. к 2006 г. В Западной Европе стоимость закупок через систему B2B выросла в период с 2001 по 2006 г. при среднегодовом росте, равном 91 % , до 1,46 трлн долл. На долю системы B2B приходится 92 % всех сделок, заключенных в Интернете.

#### **1.4.4. Виртуальные предприятия**

Виртуальные предприятия являются одной из новых организационных форм производства. Эта форма организации и управления предприятием появилась в ответ на такие тенденции развития современной экономики, как глобализация рынков, растущие требования к качеству товара, его цене, степени удовлетворения потребителей, умению формировать устойчивые отношения с заказчиками, а также расширение возможностей информационных технологий и сетей.

Разработка идей виртуальных предприятий началась в начале 1990-х гг. [64]. Однако только к концу 1990-х гг. Сеть стала готова к реализации этой идеи и переходу к виртуальным и сетевым принципам организации предприятий [3, 29, 39, 66, 74].

Виртуализация предприятия включает в себя три основных компонента:

• виртуальный рынок — рынок товаров и услуг, созданный на основе коммуникационных и информационных возможностей Сети;

• отображения производственного процесса в виртуальном пространстве;

• виртуальные (сетевые) организационные формы.

Специальное программное обеспечение, предназначенное для электронных закупок на электронных биржах, интегрируется благодаря интранет с программным обеспечением, управляющим складскими системами, производственными процессами, системами управления продаж, системами управления и планирования ресурсов предприятия.

Ярким примером виртуального предприятия является компания Cisco Systems, годовой доход которой от использования сети составляет более 3 млрд долл. При годовом обороте около 35 млрд долл. 98 % всех своих заказов эта компания обрабатывает через Сеть. Из 38 заводов, производящих ее оборудование, только два принадлежат собственно этой компании. Через 15 мин после размещения заказа на одном из 700 серверов, разбросанных по всему миру, он берется в производство [75, 79]. Если тест покажет, что изготовленный продукт не соответствует заказу или бракованный, система не распечатывает отгрузочную документацию. Без отгрузочных документов система не выставит счета заказчику. Без счета изготовитель не получит оплату. Cisco Systems распределяет, выстраивает, управляет производственным процессом, но не дистанцируется от изготовителей, подрядчиков, поставщиков комплектующих и других ресурсов, от которых зависит поставка ее продуктов.

Предприятию традиционной организационной формы для разработки и выведения нового товара на рынок требуется привлечение значительных ресурсов. Виртуальное же предприятие ищет новых партнеров, обладающих соответствующими рыночными потребностями ресурсами, знаниями и способностями, для совместной организации и реализации этой деятельности, т.е. выбираются предприятия (организации, отдельные коллективы, люди), обладающие *ключевой компетенцией* в форме ресурсов и способностей для достижения конкурентного преимущества на рынке.

С учетом сказанного можно выделить ключевое достоинство виртуальных форм организации производства: возможность выбирать и использовать наилучшие ресурсы, знания и способности с меньшими временными затратами. Из этого достоинства и самой сетевой организации вытекают следующие основные конкурентные преимущества виртуальных предприятий:

- скорость выполнения рыночного заказа;
- возможность снижения совокупных затрат;
- возможность более полного удовлетворения потребностей заказчика;

- возможность гибкой адаптации к изменениям окружающей среды;
  - возможность быстрого выхода на новые рынки.
- И все это благодаря Сети.

#### **1.4.5. Взаимодействие с конечным потребителем**

**B2C** — условное обозначение набора услуг, которые фирма может оказать клиенту (конечному потребителю), используя возможности, предоставляемые Сетью. Типичными представителями данного направления применения Сети являются интернет-магазины. В настоящее время через Сеть продается практически все, причем с доставкой на дом. Вы можете выбрать по каталогу одежду или обувь, заказать обед, запросить понравившуюся книгу или видеокассету и все это будет немедленно доставлено вам по тому адресу, который вы укажете. Конечно, так успешно этот вид бизнеса работает далеко не везде (во всяком случае в России, это скорее относится к крупным городам), но темпы его развития внушают уверенный оптимизм.

Безусловно, к этому классу приложений относятся банковские услуги, разнообразные информационные и справочные услуги, ориентированные на конечного потребителя, туристические услуги, сетевые библиотеки игр, книг, фильмов, услуги по дистанционному обучению.

В современной Сети клиент может не только выбрать необходимый продукт по каталогу, но и сформировать свой индивидуальный, не типовый продукт, например, представив проект своего мебельного гарнитура. Клиент может оформить заказ и отследить его выполнение, получая необходимые уведомления о прохождении определенного этапа изготовления, вплоть до даты доставки товара.

Развитие данного вида предприятий предопределено резким снижением затрат (а следовательно, и снижением цены на продукцию), ведь «работая» в Сети, продавцу не требуется содержать большие торговые площади, нет нужды в избыточном обслуживающем персонале торговых залов, при этом торговля может вестись круглосуточно, а обработка всей поступающей информации производится автоматически. Остаются только затраты на склад и службу доставки.

По различным оценкам, оборот рынка B2C в 2001 г. составил около 118 млрд долл., в 2005 г. — уже 707 млрд долл., а число покупателей в сетевых магазинах увеличилось за это время с 119 до 317 млн.

#### **1.4.6. Электронное правительство**

Концепция электронного правительства (Electronic Government) была провозглашена в 1997 г. в США на самом высоком правительственном уровне. Цель программы была заявлена как снижение из-

держек при финансировании деятельности госаппарата и повышение открытости и прозрачности органов управления на основе внедрения технологии электронной коммерции. В России аналогичная программа была инициирована в 2003 г. под названием «Электронная Россия».

Новые тенденции в электронной коммерции ознаменовались появлением аббревиатур B2G, G2C, G2G, обозначающих новые сферы бизнеса, в которые так или иначе вовлечено государство (Government) — Business To Government, Government To Citizens, Government To Government. Государство также включилось в процесс электронизации.

Роль электронной коммерции в организации работы государственных органов двояка. С одной стороны, это снижение издержек и экономия средств налогоплательщиков на содержание и финансирование деятельности госаппарата (B2G). С другой стороны, это повышение открытости и прозрачности органов управления, обеспечение свободного доступа граждан ко всей необходимой государственной информации (G2C). Разделение новой индустрии на секторы B2G и G2C чисто функциональное. Однако в обоих секторах необходимую инфраструктуру обеспечивает Сеть.

В первую очередь «электронными» могут стать самые очевидные функции государства — сбор налогов, регистрация транспортных средств, регистрация патентов, выдача лицензий, получение необходимой информации, заключение договоров и оформление поставок необходимых государственному аппарату материалов, оборудования. В результате сокращается объем бумажной работы, и проведение необходимых процедур значительно ускоряется. То, для чего раньше требовалось долгое стояние граждан в очередях, общение с правительственными чиновниками, а также производство и перемещение большого количества бумажных документов будет происходить теперь за несколько минут.

Если немного помечтать, то в области электронизации правительственных процессов можно, например, представить принятие важных законов путем всеобщего тайного он-лайнового голосования на правительственном сайте. Также на федеральном сайте каждый недовольный каким-либо законом сможет зарегистрировать свое мнение, и при накоплении определенного количества «черных шаров» такой закон автоматически будет включен для рассмотрения в повестку дня законодателей. Гражданский брак можно будет зарегистрировать на муниципальном сайте за минуту, при этом государственная пошлина и оплата услуги будут автоматически сниматься со счетов супругов.

B2G может стать эффективным оружием в борьбе с коррупцией. Представьте, как бы мы зажили, если все те средства, которые сегодня уходят на взятки, с помощью систем B2G и G2C пошли бы на развитие услуг государства, бизнеса и граждан. Без преувеличения

можно сказать, что в случае успеха программы «Электронная Россия» изменится сама природа власти, появится новая форма демократии — это eDemocracy (eD).

#### **1.4.7. Использование Сети в индивидуальных целях**

**C2C** — условное обозначение процесса (технологии) client-to-client (потребитель — потребителю), т.е. набор услуг (технологий), которые позволяют клиентам-физическим лицам обмениваться товарами или оказывать взаимные услуги, не прибегая к помощи посредников за счет использования возможностей Сети. К этому понятию относятся прежде всего интернет-аукционы, которые берут на себя функцию технического обеспечения сделки (дать объявление о продаже или запрос на покупку, продемонстрировать товар, оговорить предварительные условия и т.д.) и позволяют клиентам самостоятельно покупать и продавать предметы личной собственности. При этом можно, находясь во Владивостоке, приобрести то, что хотел бы продать житель Мадрида или Киева. Такой «размах» взаимодействия на сегодня кроме Сети не может обеспечить ни одно другое техническое средство.

Мы уже упоминали о таких использованиях Сети в индивидуальных целях, как обучение, игры, покупки, информационный поиск, получение справочной информации, общение. Этот список можно было бы продолжать долго. Вот, например, только краткий список основных средств общения в Интернете:

- веб-форумы;
- блоги;
- вики-проекты (в частности, википедия);
- электронная почта;
- группы новостей (в основном Usenet);
- интернет-радио;
- интернет-телевидение;
- Skype;
- IP-телефония;
- мессенджеры;
- FTP-серверы;
- ICQ;
- поисковые системы (Google, Yahoo, Yandex);
- социальные сети (Одноклассники.ru, Мой круг, Мой мир, В контакте, Мир тесен, Livejournal.com, Соседи.ru).

Однако Сеть таит и много опасностей. Это и психологическая зависимость, при которой виртуальное пространство и общение заменяют реальную жизнь. В этом случае Сеть выступает как наркотик, средство ухода от реальности [15]. Определенную опасность представляют всевозможные формы социального хакинга (несанкционированного доступа, атаки на страницы социальных сайтов в целях

**Наиболее распространенные преступления в Интернете\***

Категория преступления	Число жалоб, %
Мошенничество на торгах	44,9
Обман, связанный с доставкой	19
Махинации с чеками	4,9
Мошенничество с кредитками	4,8
Компьютерное мошенничество	2,8
Мошенничество с личными данными	2,2
Финансовое мошенничество	1,6
Кража идентификационной информации	1,6
Мошенничество с инвестициями	1,3
Детская порнография	1,0

\* Cyberstyle.ru по материалам physorg.

получения доступа к конфиденциальной информации: паролей к e-почте, электронным денежным ресурсам и пр.).

Социальный хакинг в последнее время становится все более распространенным видом разбоя. Если раньше для получения пароля необходимо было перебрать миллионы комбинаций цифр или букв, то сейчас «хорошим тоном» считается «знакомство» с жертвой, ее образом жизни, привычками, увлечениями, связями. Ведь несмотря на все предупреждения, в качестве пароля люди нередко используют один и тот же набор символов — имя любимого человека, дату рождения, номер телефона или почтовый адрес. Формы жульничества в Сети весьма и весьма разнообразны. В [51] можно найти описание популярных форм жульничества в Интернете.

В табл. 1.1 приведен перечень наиболее распространенных преступлений в Интернете.

Серьезную проблему представляет использование Интернета в экстремистских целях. Достаточно вспомнить, что Интернет являлся одним из средств координации действий экстремистов при подготовке и проведении атаки на небоскребы в США 11 сентября 2001 г.

### 1.5. Сетевая этика

Общение и использование Сети требует чувства профессиональной ответственности или хотя бы минимального знания Netiquette [35]. Что такое Netiquette? Это сетевой этикет, или этикет в Интернете. Этикет — это правила хорошего тона, принятые в той или иной социальной группе.

Другими словами, Netiquette — это набор предписаний о том, как себя вести в Сети. Когда вы осваиваете новую культуру (а Интернет, конечно, имеет собственную культуру), то вполне можете совершить ошибку. Например, обидеть человека без причины. Или, не поняв о чем идет речь, выступить со своей резкой позицией. При этом важно не забывать, что в виртуальном пространстве вы общаетесь с живыми людьми, а не просто набираете на клавиатуре некий текст.

## 1.6. Инженерия программного обеспечения

Рассмотрим теперь третью движущую силу информационных технологий — инженерию программного обеспечения.

В первые десятилетия компьютерной истории профессионального программирования как такового не было. К этому виду деятельности приобщались инженеры, учителя, специалисты самого разного профиля и конечно же математики. Это «вавилонское смешение», полное самостоятельности и энтузиазма, было изначально трудно структурировать, отделить главное от второстепенного.

Программирование рассматривалось как кодирование. Если в качестве примера посмотреть на первые учебники по программированию, то они представляли собой подобие поваренной книги, т.е. это были сборники профессиональных рецептов, как ввести число, строку символов, преобразовать запись числа в форме с плавающей запятой в запись в форме с фиксированной запятой и т.д. Программирование было ремеслом, а не видом индустриальной деятельности. Программы в массе своей не были продуктами.

Только к концу 1960-х гг. стало складываться представление о новой специальности. В это время А.А. Ляпунов открывает свой (ставший впоследствии знаменитым) семинар по программированию, а в 1970 г. академиком А.Н. Тихоновым был основан факультет вычислительной математики и кибернетики в Московском государственном университете им. М.В. Ломоносова, где появились профильные кафедры.

При этом программирование из кустарного производства стало трансформироваться, с одной стороны, в науку, а с другой — в отрасль промышленности. Пришло осознание того, что программа — это самостоятельный продукт, не зависящий от изготовителя «железа», а программирование — это область инженерии.

Отправной точкой в истории инженерии программного обеспечения считается конференция, состоявшаяся в 1968 г. в Западной Германии в г. Партенкирхен по инициативе Комитета по науке НАТО [50]. Поводом для нее стало осознание кризисной ситуации, сложившейся к этому времени в области разработки программного обеспечения, суть которой заключалась в том, что сложность программ и

**Показатели развития индустрии ЭВМ  
(за единицу приняты показатели 1955 г.)\***

Показатель	1965 г.	1975 г.	1985 г.
Объем продаж продукции	20	80	320
Число выполняемых вычислительных операций на единицу цены (на 1 долл. США)	$10^2$	$10^4$	$10^6$
Скорость выполнения вычислительных операций (млн/с)	$2 \cdot 10^3$	$8 \cdot 10^5$	$32 \cdot 10^7$
Удельная стоимость запоминающего устройства (бит на доллар США)	$10^3$	$10^6$	$10^9$
Производительность труда программиста	2,4	5,5	13,3

\* 01 Informatique-Hebdo, 1980. IV. P. 10 (США — экономика, политика, идеология. — 1983. — № 8. — С. 106).

мощность компьютеров вступили в противоречие с технологически-ми возможностями программирования.

Закона, постулирующего количественное развитие программного обеспечения и подобного закону Мура, не существует. Однако рост производительности труда программистов отмечают многие. Достоверных оценок этого роста автору неизвестно, слишком уж сложен предмет анализа.

Программирование в 1970-х гг. существенно отличается от программирования в 1990-х или в 2000-х гг. В [7] приведены данные, согласно которым рост производительности труда программистов к концу 1990-х гг. устойчиво составлял не менее 100 % за 10 лет (табл. 1.2). Здесь же отмечено, что в последнее десятилетие темпы роста производительности труда программистов только в самых автоматизированных секторах обрабатывающей промышленности достигли 80 %. Средние же темпы роста производительности их труда, например в обрабатывающей промышленности США, за тот же период не превысили 30 %.

Таким образом, можно сделать вывод, с одной стороны, о рекордных, невиданно высоких темпах роста производительности труда программистов, а с другой стороны, в сравнении с темпами роста, определяемыми законами Мура и Гилдера, приведенные показатели непропорционально низкие.

С уверенностью можно сказать одно, что рост производительности труда программистов представляет собой плохо управляемый процесс: программирование губит иллюзия простоты и вседозволенности, отсутствие между разработчиком и конечным продуктом в большин-

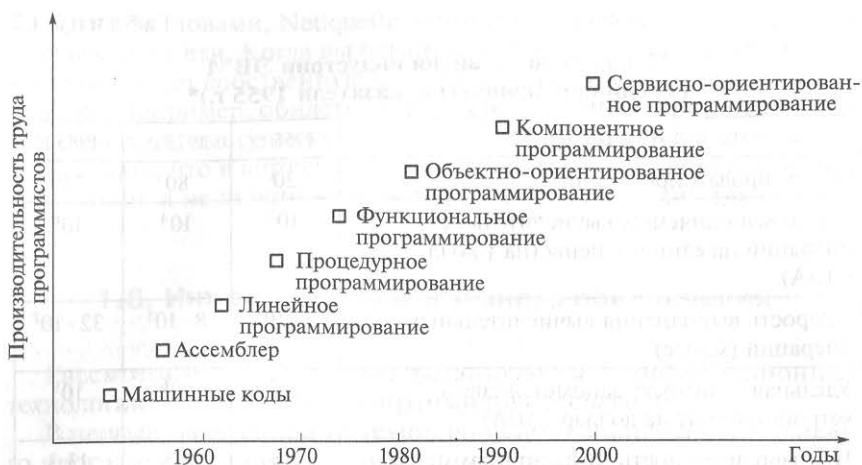


Рис. 1.2. Хронология развития методов программирования

стве проектов череды специалистов-технологов и производственников. Сравните, как долго и дорого создавать самолеты или автомобили, сколько времени уходит на их проектирование, создание опытных образцов, испытания, запуск в производство, и как соблазнительно быстро пишутся программы. Следствием такой иллюзии являются многочисленные аварии, вызванные ошибками, что особенно эффективно, а порой и трагически, проявляется во встроенных системах. Ошибки в офисных программах менее заметны.

Тем, кто интересуется хроникой программных техногенных катастроф, можно порекомендовать [8], где описано большое количество соответствующих эпизодов, зафиксированных в период с 1986 г. до наших дней.

На рис. 1.2 представлена хронология развития методов программирования, направленных на повышение производительности труда программистов, повышение скорости разработки и надежности создаваемых программ. Уже в 1970-е гг. пришло понимание того, что программы как продукт инженерной деятельности имеют беспрецедентную в истории человеческой цивилизации сложность, а следовательно, нельзя каждый раз разработку программной системы начинать с нуля. Поэтому активно стали развиваться методы программирования, основная идея которых состояла в использовании при создании программных систем ранее написанных компонентов — «кирпичиков», в которых аккумулировался бы опыт предшествующих разработок и корректность работы которых не надо было бы каждый раз обосновывать.

Однако реализация этой идеи потребовала решения череды очень непростых задач, осознание которых во многих случаях приходило

не сразу. Так, например, эти компоненты должны были работать в разных операционных средах, быть многократно используемыми в разных программных контекстах, а также они должны были уметь обмениваться данными, взаимодействовать друг с другом, т. е. быть интероперабельными, и т. д.

## 1.7. Сервис-ориентированные архитектуры и web-сервисы

Современным воплощением заветной мечты индустрии программирования о замене «кустарного» кодирования программ «от и до» на «промышленную» сборку приложений из стандартных комплекующих, как в автомобильной и других традиционных отраслях промышленности, явилось создание сервис-ориентированной архитектуры (service-oriented architecture — SOA) — подхода к разработке программного обеспечения, основанного на использовании сетевых сервисов (служб) со стандартизированными интерфейсами [34].

В самом общем виде SOA предполагает наличие трех основных участников [45]: поставщика сервиса, потребителя сервиса и реестра сервисов (рис. 1.3), где указаны стандарты языков и протоколов, используемых при реализации SOA, многие из которых будут рассмотрены далее. Взаимодействие участников SOA организовано доста-

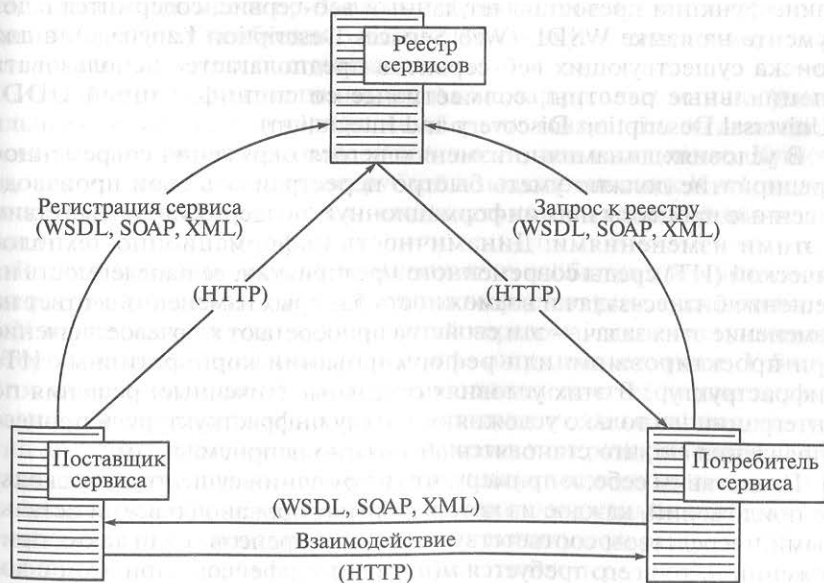


Рис. 1.3. Общая схема SOA

точно просто: поставщик сервиса регистрирует свои сервисы в реестре, а потребитель обращается к реестру с запросом.

Для использования сервиса необходимо следовать соглашению об интерфейсе обращения к сервису: интерфейс должен не зависеть от среды разработки сервиса. SOA предполагает возможность добавления сервисов, а также их модернизацию. Поставщик сервиса и его потребитель оказываются несвязанными, т. е. они общаются с помощью сообщений. Поскольку интерфейс должен не зависеть от платформы разработки, то и технология, используемая для определения сообщений, также не должна зависеть от платформы.

Интерфейс компонентов SOA-программы инкапсулирует, т. е. скрывает детали реализации конкретного компонента (операционной системы, платформы, языка программирования, вендора и т. п.) от остальных компонентов. Таким образом, SOA предоставляет гибкий и элегантный способ комбинирования и многократного использования компонентов программы для построения сложных распределенных программных комплексов, т. е. компоненты программы могут быть распределены по разным узлам сети и предлагаться как независимые слабосвязанные заменяемые сервисы-приложения.

Программные комплексы, разработанные в соответствии с SOA, часто реализуются как набор веб-сервисов, интегрированных с помощью известных стандартных протоколов.

Веб-сервис — это набор логически связанных функций, которые могут быть вызваны удаленно через Интернет. Информация о том, какие функции предоставляет данный веб-сервис, содержится в документе на языке WSDL (Web Services Description Language), а для поиска существующих веб-сервисов предполагается использовать специальные реестры, совместимые со спецификацией UDDI (Universal Description Discovery and Integration).

В условиях динамично изменяющегося окружения современное предприятие должно уметь быстро перестраивать свои производственные процессы и их информационную поддержку в соответствии с этими изменениями. Динамичность информационно-технологической (ИТ) среды современного предприятия, ее нацеленность на решение бизнес-задач и возможность быстрых изменений в ответ на изменение этих задач — эти свойства приобретают ключевое значение при проектировании или реформировании корпоративных ИТ-инфраструктур. В этих условиях отдельные (точечные) решения по интеграции настолько усложняют и саму инфраструктуру, и процесс управления ею, что становятся абсолютно неприемлемыми.

Представим себе, к примеру, что в компании существует несколько приложений, каждое из которых интегрировано со всеми остальными посредством соответствующих интерфейсов. Если таких приложений  $n$ , то всего требуется  $n(n - 1)$  интерфейсов. При этом с добавлением всего лишь одного нового приложения появляются  $2n$  новых интерфейсов, для которых требуются соответствующее доку-

ментирование, тестирование и поддержка. Придется вносить модификации в код каждого из существующих приложений для учета новых интерфейсов и проводить соответствующее тестирование. SOA позволяет избежать такой ситуации, максимально упростить процесс добавления новых приложений и минимизировать число интерфейсов взаимодействия.

Другими словами, SOA обеспечивает предприятию высокую скорость адаптации к динамично изменяющимся условиям современного рынка, а, по мнению таких лидеров современного бизнеса как Д. Уелч (General Electric), Б. Гейтс (Microsoft), Д. Чамберс (Cisco Systems), Л. Элисон (Oracle), в современных условиях самое главное — это то, насколько быстро компания может адаптировать свои цели и организацию к новым динамично изменяющимся условиям.

Итак, мы видим, что перспективы развития компьютера связаны не с развитием компьютера, как такового, а с развитием его сетевых возможностей, что отражает и общую тенденцию в развитии человеческой цивилизации: интеграция и глобализация. Это порождает и новый тип экономики (да простят меня экономисты) — сетевую экономику, основные принципы которой можно сформулировать следующим образом. Скорость развития общества столь велика, что сегодня речь идет не об оптимизации существующих структур, а об инновационном, прорывном, создании новых. При этом только гибкость и разнообразие сетей способны успевать за все ускоряющимися темпами появления нового. В сетевой экономике все меньше и меньше остается места привычному. Традиционной становится инновация, поэтому необходимо вырабатывать вкус к переменам, надо говорить о переменных постоянно.

Изменяется и понятие ценности. Аксиома прошлых лет: чем уникальнее предмет, тем он дороже, чем больше товара, тем он дешевле. В сети все не так: чем больше узлов в сети, тем она ценнее. Купив компьютер за несколько тысяч рублей и подключив его к Интернету, вы получаете доступ к ресурсам, стоимость которых даже трудно подсчитать.

В такой экономике ценность вырастает из изобилия и возрастает от распространения, при этом также резко возрастает роль стандартов.

У эпидемиологов есть понятие точки перелома, после наступления которой процесс не надо подталкивать, он развивается сам. У биологов имеется хороший пример с разрастанием листьев лилии: лилия удваивает поверхность своих листьев ежедневно. Это означает, что за день до того как лилия полностью закроет поверхность пруда, она будет закрывать только половину его поверхности, а за два дня до «финиша» — лишь четверть и т. д. Следовательно, заметной для нашего глаза лилия станет, когда займет половину поверхности пруда, а это произойдет через много дней после точки перелома.

Сеть можно сравнить с разрастанием лилии, и точка перелома здесь давно пройдена.

## ОСНОВНЫЕ ПОНЯТИЯ, МОДЕЛИ И ПРИМЕРЫ КОМПЬЮТЕРНЫХ СЕТЕЙ

### 2.1. Организация компьютерных сетей

#### 2.1.1. Общие сведения

Компьютерная сеть состоит из множества абонентских машин, способных взаимодействовать друг с другом через транспортную среду. Другими словами, на самом верхнем рассматриваемом уровне компьютерная сеть состоит из двух компонентов: *абонентских машин* и *транспортной среды*.

*Абонентскими*, или *A-машинами*, называются машины, на которых работают приложения. Абонентские машины, обеспечивающие доступ пользователей к приложениям и работу приложений в сети, подсоединены к среде передачи данных, которая является компонентом транспортной среды. Назначение транспортной среды — обеспечить эффективную доставку данных от приложения на одной *A-машине* к приложению на другой *A-машине*. Значение в данном случае термина *эффективность* в полной мере будет раскрыто по ходу изложения. Здесь же лишь отметим, что доставка данных должна быть надежной, оптимальной и поддерживаться необходимыми сервисами.

Транспортная среда включает в себя *сети передачи данных* и *коммуникационные машины* (далее *R-машины*, или кратко *RM*).

Во избежание неоднозначности использования термина *Сеть* далее сети передачи данных будем называть *системами передачи данных* (СПД).

Коммуникационные машины — это специализированные компьютеры, подсоединенные к двум и более системам передачи данных. *A-машины* и *R-машины* часто называются *хостами* (от *англ.* host — компьютер, являющийся узлом в сети).

На рис. 2.1 показана общая схема организации компьютерной сети. Примером *R-машины* здесь является *маршрутизатор (R)* — компьютер, вычисляющий оптимальный маршрут, по которому должны следовать данные между абонентскими машинами в сети, управляющий переключением потоков данных согласно вычисленному оптимальному маршруту, отслеживающий динамику изменений в конфигурации транспортной среды и выполняющий многое, многое другое. Другим примером *R-машины* является *шлюз (G)* — компьютер, со-

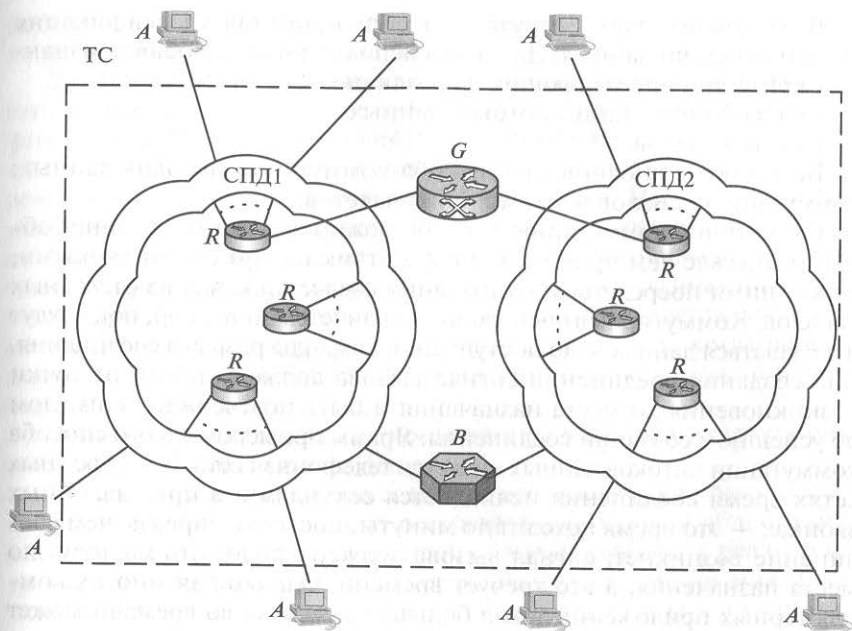


Рис. 2.1. Организация компьютерной сети

единяющий две разные по архитектуре транспортные среды. Устройство, обозначенное *B* на рис. 2.1 и называемое *мост*, предназначено для соединения двух СПД. Штриховой линией здесь показана граница транспортной среды для *A*-машин.

### 2.1.2. Системы передачи данных

Система передачи данных, обеспечивающая передачу данных между *R*-машинами и между *A*-машинами и *R*-машинами, состоит из каналов и коммутирующих элементов (коммутаторов) или переключателей.

Каналы передачи данных — это физические линии связи самой различной природы и каналообразующая аппаратура. Примерами линий связи являются: витая пара медных проводов, используемых в телефонии; коаксиальный кабель, используемый для телевизионного антенного ввода; волоконно-оптический кабель, обеспечивающий передачу данных с помощью электромагнитных импульсов в световом диапазоне, а также беспроводные радиочастотные каналы связи. Подробно эти линии связи и их свойства рассматриваются в гл. 3. Каналообразующая аппаратура обеспечивает интерфейс между линией связи и компьютером.

В настоящее время отсутствует общепринятая классификация систем передачи данных. Для этого используются два общепризнанных критерия, определяющих их различие:

- способ коммутации потоков данных;
- типы каналов.

Выделяют два основных способа коммутации потоков данных: коммутацию каналов и коммутацию пакетов.

Схематично коммутацию каналов можно описать следующим образом: прежде чем приемник и передатчик начнут обмен данными, между ними посредством коммутации создается канал из отдельных каналов. Коммутированный канал сохраняется до тех пор, пока будут передаваться данные и до поступления команды разрыва соединения. Для создания соединения сигнал вызова должен пройти от точки возникновения до места назначения и быть подтвержден сигналом об успешном создании соединения. Ярким примером такого способа коммутации потоков данных является телефонная сеть. В телефонных сетях время соединения исчисляется секундами, а при удаленных звонках — это время доходит до минуты, поскольку прежде чем соединение возникнет, сигнал вызова должен проложить маршрут до места назначения, а это требует времени. Однако для многих компьютерных приложений такая большая задержка во времени может оказаться неприемлемой. При этом если соединение установлено, то нет опасности, что во время разговора вы услышите сигнал «занято» из-за нехватки свободных линий у какого-либо коммутатора.

Для коммутации потоков данных посредством коммутации каналов характерно следующее:

- сохранение порядка передаваемых данных, т.е. соблюдение принципа «раньше посланный — раньше будет получен»;
- наличие огромного опыта создания и эксплуатации;
- наличие хорошо развитой инфраструктуры.

В то же время этому способу коммутации потоков данных присущ ряд недостатков:

- неэффективное использование ресурсов, т.е. скорость передачи определяют в этом случае приемник и передатчик, а не возможности коммутированного канала;
- низкая надежность, т.е. достаточно разрушить либо один из промежуточных каналов, составляющих коммутированный канал, либо один из узлов коммутации, и весь коммутированный канал будет разрушен;
- медленная установка соединения.

Альтернативой коммутации каналов является коммутация сообщений. Изначально этот метод использовался при передаче телеграмм. Сообщение получали на узле коммутации целиком, затем целиком передавали по каналу, ведущему к абоненту. И так от оператора к оператору, от одного узла коммутации к другому, пока сообщение не приходило к адресату. В этом случае не требуется создавать соединение заранее. Однако при таком способе передачи необходимо обе-

спечить на каждом узле коммутации необходимое количество памяти для буферизации любого сообщения, сколь угодно большого.

Для преодоления этого недостатка был предложен метод коммутации пакетов, при котором сообщение разбивается на фрагменты фиксированной длины. Эти фрагменты называются пакетами. Пакеты одного сообщения передаются от одного узла коммутации к другому, пока они не достигнут места назначения. При этом каждый пакет можно передавать независимо от других. Поскольку пакет имеет фиксированную длину, абонент не может монополизировать линию. Одну и ту же линию могут разделять пакеты разных пользователей. Другим достоинством коммутации пакетов является конвейерность: второй пакет можно отправить, не дожидаясь, когда первый достигнет места назначения. Послав второй пакет, можно начать передачу третьего и т. д.

Основные различия между коммутацией каналов и коммутацией пакетов заключаются в следующем:

- при коммутации каналов создается соединение, пропускная способность которого полностью резервируется за двумя абонентами, вне зависимости от того, какая пропускная способность реально им требуется. При коммутации пакетов физическая линия может использоваться пакетами разных абонентов. Следует иметь в виду, что, поскольку при коммутации пакетов не происходит жесткого закрепления канала, то резкое увеличение потока пакетов в узле коммутации может привести к его перегрузке и потере части пакетов;

- при коммутации каналов гарантировано, что все данные поступят абоненту и в том порядке, в каком их послали. При коммутации пакетов каждый пакет следует своим маршрутом, и принцип «ранее посланный — будет раньше принят» уже не выполняется, например хотя бы потому, что у разных пакетов маршруты могут быть разной длины. Кроме того, пакеты могут быть искажены при передаче либо вовсе потеряны, поэтому сохранение исходного порядка пакетов в сообщении получателю не гарантируется;

- коммутация каналов абсолютно прозрачна для абонентов. Они могут пересылать данные в любой кодировке и любом формате. При коммутации пакетов формат и способ кодировки пакетов заданы заранее и определяются оператором связи;

- при коммутации пакетов плата взимается за время соединения и число переданных пакетов. При коммутации каналов плата берется исключительно за время и длину соединения.

Приведенные различия способов коммутации сведены в табл. 2.1.

Различают каналы двух типов:

- каналы точка — точка;
- каналы с множественным доступом;

*Канал типа точка — точка* соединяет только две машины между собой. Все потоки данных, протекающие по каналу этого типа, доступны лишь этим двум машинам.

## Сравнение способов коммутации каналов и коммутации пакетов

Признак	Коммутация каналов	Коммутация пакетов
Выделенный канал передачи	Есть	Нет
Пропускная способность	Фиксированная	Динамическая
Неиспользуемая пропускная способность	Возможна	Невозможна
Передача с буферизацией пакетов	Нет	Есть
Единый путь для всех пакетов	Есть	Нет
Установление соединения	Требуется	Не требуется
Возможность перегрузки	При установлении соединения	На любом пакете
Оплата	За время соединения	За переданные пакеты

*Канал с множественным доступом* образует общую для нескольких машин среду передачи данных. Короткое сообщение, называемое пакетом, имеющее специальную структуру и отправленное какой-то машиной, «видят» все другие машины, подключенные к этому каналу. В определенном поле пакета указывается адрес получателя. Каждая машина проверяет это поле, и если она обнаруживает там свой адрес, приступает к обработке пакета. Если же в этом поле нет ее адреса, машина просто игнорирует пакет.

Системы передачи данных, имеющие каналы с множественным доступом, как правило, имеют режим вещания, при котором один пакет адресуется всем машинам, подключенным к одному и тому же каналу с множественным доступом. Имеется в таких сетях и режим групповой передачи, при котором один и тот же пакет получают машины, принадлежащие к определенной группе.

Системы передачи данных, имеющие каналы с множественным доступом, подразделяются по методам выделения канала на динамические и статические.

В *статических* СПД канал разделяется по времени (time-sharing) между машинами, т. е. заранее составляется расписание, по которому каждой машине выделяется квант времени для передачи. Причем канал простаивает, если машине нечего передавать в выделенный ей квант времени.

В *динамических* СПД канал выделяется машине только, если у нее возникает необходимость что-то передать. При этом встает про-

стой вопрос: что делать, если сразу несколько машин запросили канал.

Все механизмы выделения канала по запросу подразделяются на *централизованные* и *распределенные*.

СПД с каналами точка—точка соединяют каждую пару машин индивидуальными каналом. При этом не следует думать, что канал типа точка—точка — это физическая монолитная линия. Канал этого типа может быть сформирован динамически по запросу, например если две машины соединяются через телефонную сеть.

СПД с множественным доступом, как правило, используются на небольших территориях, а СПД типа точка—точка — для построения крупных сетей, охватывающих большие регионы.

Коммутирующие элементы — это либо коммутаторы, подобные тем, что применяются в телефонных сетях (см. гл. 5), либо компьютеры со специальным программным обеспечением, осуществляющим выбор одного из каналов для передачи фрагмента данных посредством несложных вычислений на основе, как правило, заранее заложенной в них статической информации. Эти вычисления не предполагают оптимизации каждого маршрута и динамического отслеживания топологии СПД. Как правило, выбор направления коммутации для потока данных определяют предварительно сделанные настройки.

Транспортную среду различают по составу входящих в нее СПД и топологии. В транспортную среду может входить несколько различных СПД. При этом одна и та же  $R$ -машина или маршрутизатор может

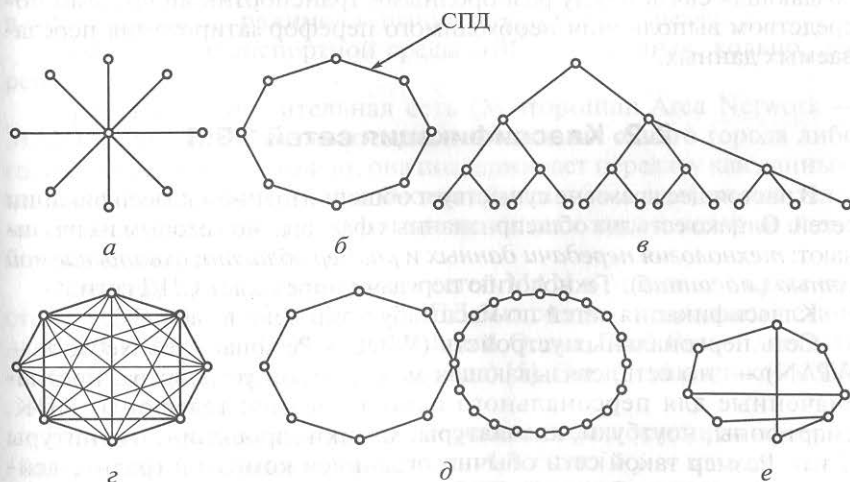


Рис. 2.2. Топологии транспортной среды для соединений типа точка—точка:

$a$  — звезда;  $b$  — кольцо;  $v$  — дерево;  $g$  — полностью связанная;  $d$  — пересекающиеся кольца;  $e$  — нерегулярная

подключаться к разным СПД. Если изобразить транспортную среду в виде графа, где вершины — это  $R$ -машины, а дуги — это те каналы, которые обеспечивают СПД, входящие в транспортную среду, то полученный граф и будет представлять собой типологию транспортной среды.

*Топология соединения маршрутизаторов* — это важный фактор конструкции транспортной среды. От нее зависит время задержки пакета в сети, условия возникновения перегрузки (т.е. когда через СПД стремятся передать пакетов больше, чем возможно) и многие другие параметры функционирования сети, которые подробно будут рассмотрены далее.

На рис. 2.2 показаны типичные топологии транспортных сред, в которых каждая вершина обозначает  $R$ -машину.

### 2.1.3. Сопряжение транспортных сред

Необходимость сопряжения транспортных сред возникает, когда требуется обеспечить взаимодействие приложений, расположенных на разных  $A$ -машинах, которые подключены к разным транспортным средам.

Мосты и шлюзы — это средства сопряжения транспортных сред на разных уровнях (на рис. 2.1 обозначены соответственно  $B$  и  $G$ ).

При этом мост соединяет две СПД, а шлюз — две разные по архитектуре ТС.

Шлюз — это машина с надлежащим программным обеспечением, создающая связь между разнородными транспортными средами посредством выполнения необходимого переформатирования передаваемых данных.

## 2.2. Классификация сетей ЭВМ

В настоящее время не существует общепризнанной классификации сетей. Однако есть два общепризнанных фактора, по которым их различают: *технология передачи данных* и *размер области, охватываемой сетью (масштаб)*. Технологию передачи определяет СПД сети.

Классификация сетей по масштабу приведена в табл. 2.2.

Сеть персональных устройств (Wireless Personal Area Network — WPAN) — это сеть, связывающая между собой устройства, предназначенные для персонального использования: телефоны, КПК, смартфоны, ноутбуки, клавиатуры, мышки, проекторы, гарнитуры и т.п. Размер такой сети обычно ограничен комнатой (радиус действия 10... 100 м). Основой СПД является технология Bluetooth, работающая со скоростью 1... 3 Мбит/с (см. подразд. 2.6.1). Топология связи типа «каждый с каждым».

Для локальной вычислительной сети (ЛВС) типичны следующие характеристики:

## Классификация сетей по территориальному масштабу

Расстояние между машинами*	Местонахождение процессоров	Класс вычислительной сети
1 м	Система	Многомашинный комплекс
10 м	Помещение	Сеть персональных устройств
100 м		Локальная сеть
1 км		
10 км	Город	Городская сеть
100 км	Страна	Региональная сеть
1 000 км	Континент	Региональная сеть
10 000 км	Планета	Интернет

\* Расстояния указаны ориентировочно.

- размер — комната, здание, группа зданий (известна максимальная задержка сигнала при передаче);
- система передачи данных — это, как правило, канал с множественным доступом (скорость передачи от 10 Мбит/с до нескольких гигабит в секунду, наличие режимов вещания и групповой передачи);
- топологии транспортной среды ЛВС — линейная, кольцо, дерево.

Городская вычислительная сеть (Metropolitan Area Network — MAN) охватывает несколько зданий в пределах одного города либо город целиком. Как правило, она поддерживает передачу как данных, так и голосовых сообщений и иногда объединяется с кабельной телевизионной сетью. По своей организации сети этой категории очень близки к локальным сетям.

Основная причина выделения сетей MAN в отдельный класс состоит в том, что для них как для СПД был создан специальный стандарт IEEE 802.6 — DQDB (Distributed Queue Dual Bus — двойная магистраль с распределенной очередью) [5]. Организация такой СПД показана на рис. 2.3.

Если машине с номером  $i$  надо передать данные машине с номером  $j$  при  $j > i$ , то  $i$  использует магистраль  $A$ , а если  $i < j$  — магистраль  $B$ . Магистрали  $A$  и  $B$ , проложенные в метро вдоль туннелей, обеспечивают охват большой территории.

Региональная вычислительная сеть (Wide Area Network — WAN) охватывает крупные географические области, страны и континенты. Транспортная среда таких сетей строится на основе коммутации па-

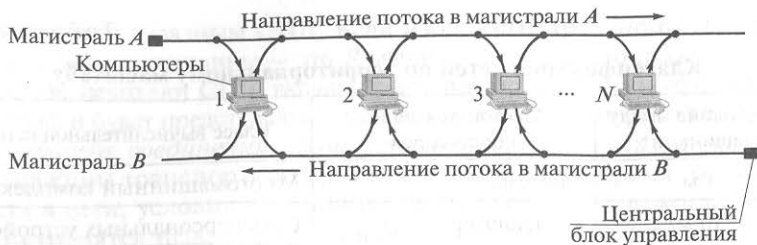


Рис. 2.3. Архитектура стандарта СПД городского масштаба DQDB

кетов с помощью каналов типа точка—точка. Как правило, в качестве СПД в таких сетях используются уже существующие системы связи, например телефонные сети, спутниковые и наземные радиосистемы.

## 2.3. Сетевое программное обеспечение

### 2.3.1. Иерархия протоколов

Рассмотрим иерархию сетевого программного обеспечения, т. е. программного обеспечения, служащего для передачи данных между приложениями, работающими на абонентских машинах. Это программное обеспечение определяет функционирование транспортной



Рис. 2.4. Иерархия протоколов

среды, системы передачи данных и взаимодействие абонентских машин с транспортной средой.

Сеть является сложной инженерно-технической системой, поэтому в целях упрощения ее программное обеспечение строго структурировано и организовано в виде иерархии слоев, или уровней. В разных сетях число уровней, их названия, состав и функции могут быть разными. Однако во всех сетях каждый уровень имеет следующее назначение:

- обеспечить определенный сервис вышерасположенному уровню;
- сделать работу верхнего уровня независимой от деталей реализаций сервиса на нижних уровнях.

Программное обеспечение уровня  $n$  на одной машине взаимодействует с программным обеспечением уровня  $n$  на другой машине. Правила и соглашения по установлению и поддержанию связи, обеспечивающей такое взаимодействие, называются *протоколом* (рис. 2.4).

При этом уровень  $n$  на одной машине непосредственно с уровнем  $n$  на другой машине не взаимодействует. Их взаимодействие возможно только через посредство нижерасположенных уровней. Сказанное можно пояснить аналогией общения двух человек, говорящих на разных языках, которые общаются между собой, хотя каждый из них непосредственно взаимодействует с переводчиком, а не со своим *vis-à-vis*, т. е. переводчик обеспечивает сервис.

### 2.3.2. Основные понятия

Между каждой парой соседних уровней Сети есть *интерфейс*, определяющий, как вышерасположенный уровень получает доступ к услугам нижележащего уровня. Этот доступ осуществляется с помощью примитивов — элементарных операций, которые нижерасположенный уровень может выполнять по требованию вышерасположенного уровня.

Набор уровней и протоколов называется *архитектурой сети*. Описание архитектуры сети должно содержать достаточно информации, чтобы разработчик сетевого программного обеспечения мог создать надлежащие программы для каждого уровня, а инженер-электронщик — надлежащую аппаратуру. Ни вопросы реализации, ни вопросы определения интерфейсов не относятся к архитектуре сети.

Конкретный набор протоколов, используемых на конкретной машине, называется *стеком протоколов*. Архитектуры сетей, стеки протоколов, сами протоколы являются основными предметами рассмотрения в данном курсе.

При передаче сообщения между уровнями Сети выполняются определенные его преобразования, показанные на рис. 2.5. На каждом уровне к сообщению добавляется заголовок, который содержит управляющую информацию (кому адресовано сообщение, время, дату, порядковый номер и другие данные, необходимые для управления

Уровень Сети



Рис. 2.5. Пример организации потока информации при виртуальном взаимодействии на 5-м уровне Сети:

$M$  — сообщение;  $H_k$  — заголовок уровня  $i$ ;  $M_j$  — фрагмент сообщения  $M$ ;  $T_i$  — концевик уровня  $i$

процессом передачи). На уровне 3 исходное сообщение уровня 4 разбивается на два, поскольку длина сообщения уровня 4 с заголовком уровня 3 превышает заранее определенную длину, допустимую для передачи на нижерасположенном уровне.

### 2.3.3. Интерфейсы и сервис

Как уже говорилось, одно из главных предназначений каждого уровня Сети — обеспечить надлежащий сервис для вышерасположенного уровня.

Активные элементы уровня, т.е. элементы, которые могут сами совершать действия, в отличие от тех, над которыми совершают действия, называются *активностями*. Активности могут быть программными и аппаратными. Активности одного и того же уровня на разных машинах называются *равнозначными*, или *одноименными*. Активности уровня  $n + 1$  являются *пользователями сервиса*, создаваемого активностями уровня  $n$ , которые, в свою очередь, называются *поставщиками сервиса*. При этом сервис может быть разного качества, например связь может быть быстрой и дорогостоящей либо медленной и дешевой.

Доступ к сервису осуществляется через так называемые *точки доступа к сервису* (Service Access Points — SAP). Каждая точка доступа к сервису имеет уникальный адрес. Например, телефонная розетка на стене — это точка доступа к сервису АТС. Каждой розетке соответствует определенный номер — номер телефона.

Чтобы два уровня могли обмениваться информацией, необходимо определить интерфейс между ними. Типичный интерфейс сле-

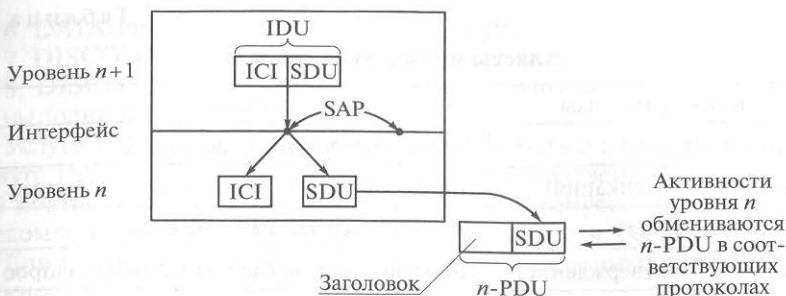


Рис. 2.6. Взаимосвязь уровней Сети через интерфейс:

SAP — точка доступа к серверу; IDU — интерфейсная единица данных; SDU — сервисная единица данных; PDU — единица данных протокола; ICI — контрольная информация интерфейса

дующий: активность на уровне  $n + 1$  передает интерфейсную единицу данных — IDU (Interface Data Unit) на уровень  $n$  через SAP (рис. 2.6). IDU состоит из сервисной единицы данных (Service Data Unit — SDU) и управляющей информации. SDU передается далее по сети равнозначной сущности, а затем — на уровень  $n + 1$ . Управляющая информация требуется нижерасположенному уровню, чтобы правильно передать SDU, но она не является частью передаваемых данных.

Чтобы передать SDU по сети нижерасположенному уровню, может потребоваться разбить его на части. При этом каждая часть снабжается заголовком и концевиком и передается как самостоятельная единица данных протокола — PDU (Protocol Data Unit). Заголовок PDU используется протоколом при передаче. В этом протоколе указывается, какая PDU содержит управляющую информацию, а какая — данные, порядковый номер PDU и т. д.

### 2.3.4. Примитивы сервиса

Формально сервис можно описать в терминах примитивных операций, или *примитивов*, с помощью которых пользователь или какая-либо активность получает доступ к сервису. С помощью этих примитивов активность на вышерасположенном уровне сообщает активности на нижерасположенном уровне, что необходимо сделать, чтобы вышерасположенная активность получила требуемую услугу (сервис). В свою очередь, нижерасположенная активность может использовать эти примитивы, чтобы сообщить вышерасположенной активности о выполненном действии. Примитивы подразделяются на четыре класса (табл. 2.3).

Для иллюстрации работы примитивов рассмотрим, как можно установить и разорвать соединение. Сначала активность выполняет

## Классы примитивов сервиса

Класс примитивов	Значение
Request (Запрос)	Запрос определенных действий
Indication (Индикация)	Информирование о каком-либо событии
Response (Ответ)	Ответ на полученный ранее запрос
Confirm (Подтверждение)	Получен ответ на сделанный ранее запрос

примитив `CONNECT.request`, в результате чего в транспортную среду выпускается пакет. Адресат-получатель, указанный в пакете, получает примитив `CONNECT.indication`, указывающий на то, что с ним хотят установить связь. В ответ получатель через примитив `CONNECT.response` сообщает отправителю, также указанному в пакете, либо что он готов к взаимодействию, либо что он отказывается от обмена данными. В результате активность — инициатор установления связи — получает через примитив `CONNECT.confirm` уведомление или отказ об установлении соединения.

Большинство примитивов имеет параметры. Параметры примитива `CONNECT.request` определяют адресат, соединение, желаемое качество сервиса и максимальный размер сообщения, допустимый для данного соединения. Параметры примитива `CONNECT.indication` указывают, кто обратился, желаемое качество обслуживания, предлагаемый размер сообщений. Если активность, к которой обратились, не согласна, например с предлагаемым размером сообщений, то она предлагает свой размер через примитив `response`, который становится известным активности, добивающейся соединения, через примитив `confirm`. Подробности этих переговоров — существо протокола. Например, в случае конфликта при установлении максимального размера сообщения протокол может установить, что выбирается размер, наименьший из предложенных. Услуга может быть либо с подтверждением, либо без подтверждения. При услуге с подтверждением используются все четыре примитива — `request`, `indication`, `response`, `confirm`. При услуге без подтверждения используются только два примитива — `request` и `indication`.

Продемонстрируем сказанное на примере простых услуг с соединением, реализуемым следующими восемью примитивами:

1. `CONNECT.request` — запрос на установление соединения;
2. `CONNECT.indication` — сигнал для удаленной активности;
3. `CONNECT.response` — примитив, используемый удаленной активностью для получения согласия-несогласия на соединение;
4. `CONNECT.confirm` — примитив, сообщающий активности, иницирующей соединение, принято оно или нет;
5. `DATA.request` — запрос на передачу данных;

6. DATA.indication — сигнал поступления данных;
7. DISCONNECT.request — запрос на разрыв соединения;
8. DISCONNECT.indication — сигнал равнозначной активности на выполнение запроса.

Услуга CONNECT обязательно должна быть с подтверждением. Услуга DATA\_TRANSFER может быть как с подтверждением, так и без подтверждения, в зависимости от того, требуется отправителю уведомление или нет. Оба вида услуг используются в сетях.

Для примера покажем, как в терминах приведенных примитивов можно описать телефонный разговор:

1. CONNECT.request — вы набираете номер друга;
2. CONNECT.indication — друг слышит звонок;
3. CONNECT.response — друг берет трубку;
4. CONNECT.confirm — вы слышите, что гудки прекратились;
5. DATA.request — вы предлагаете другу встретиться;
6. DATA.indication — друг слышит ваше приглашение;
7. DATA.request — друг говорит, что согласен;
8. DATA.indication — вы слышите его ответ;
9. DISCONNECT.request — друг кладет трубку;
10. DISCONNECT.indication — вы слышите, что друг положил трубку и тоже кладете трубку.

### **2.3.5. Сервисы с соединением и без соединения**

Нижерасположенные уровни Сети могут предоставлять ее выше-расположенным уровням два вида сервисов: сервис, ориентированный на соединение, и сервис без соединения.

*Сервис с соединением* реализуется только после того, как между получателем и отправителем установится соединение. Например, телефонная сеть: сначала между абонентами устанавливается соединение и только потом они могут разговаривать. Процесс установления соединения включает в себя: прокладку маршрута между одноименными уровнями, проверку готовности получателя и отправителя к обмену данными, установление качества сервиса (например, вероятность разрыва соединения, скорость передачи данных, вероятность ошибки при передаче данных и т.д.).

*Сервис без соединения* действует подобно почтовой службе. Каждое сообщение содержит адрес получателя. В надлежащих точках оно маршрутизируется независимо от других сообщений. При таком сервисе вполне возможно, что сообщение, посланное позже других, придет к получателю раньше. При использовании сервиса с соединением это невозможно.

Любой сервис характеризуется определенным качеством. Например, надежный сервис, гарантирующий доставку данных без потерь, предполагает подтверждение получения каждого сообщения. Несомненно, это требует определенных накладных расходов, что является

платой за качество. Пример надежного сервиса с соединением — передача файлов. Ясно, что вряд ли кто-то рискнет передавать файл (пусть даже ценой скорости) с риском потерять часть битов или нарушить их порядок.

Надежный сервис с соединением может быть двух видов: последовательность сообщений и поток байтов. В первом виде четко различаются границы каждого сообщения: если было послано два сообщения по 1 Мбайт, то получено будет два сообщения по 1 Мбайт. Ни при каких условиях у получателя не окажется одно сообщение в 2 Мбайт.

В случае использования потока байтов адресат получит сообщение в 2 Мбайт. При этом у него нет способа распознать то ли это два сообщения по 1 Мбайт, то ли одно сообщение в 2 Мбайт, то ли 2 048 сообщений по 1 Кбайт. Следовательно, при передаче книги на фотонаборное устройство необходимо проследить, чтобы каждая страница имела четкие границы. В то же время для поддержки соединения между терминалом и сервером в режиме командной строки потока байтов вполне достаточно.

Другой важной характеристикой качества сервиса является задержка данных в канале. Для некоторых приложений задержки данных из-за уведомления об их получении неприемлемы. Примерами таких приложений являются цифровая телефонная связь, цифровые видеоконференции. При телефонном разговоре люди готовы смириться с шумом на линии, искажениями слов, но паузы вследствие уведомлений будут просто неприемлемы. Аналогично при видеоконференции или передаче видеofilма, если небольшие дефекты картинки допустимы, то подергивание экрана из-за уведомлений будет раздражать зрителя.

Пример приложения, не требующего соединения, — электронная почта. Вряд ли отправитель второстепенного сообщения захочет ждать установки и разрыва соединения и оплачивать весь этот сервис. Ему также вряд ли потребуется стопроцентная гарантия доставки, особенно если это связано с увеличением стоимости. Все, что в этом случае требуется — простой и дешевый способ передачи сообщения, которое с большой вероятностью будет принято, но без всяких гарантий. ненадежный сервис (т. е. без уведомления) часто называют дейтаграммным (datagram) по аналогии с телеграммой без уведомления. Однако для приложений, требующих гарантии доставки даже небольшого сообщения, используется дейтаграммный сервис с подтверждением (подобно телеграмме с уведомлением о получении).

Сервис и протоколы — понятия разные, хотя их часто путают. Различие между ними настолько важное, что рассмотрим его еще раз. Сервис — это набор услуг, который данный уровень предоставляет вышерасположенному уровню. Сервис определяется в терминах примитивных операций. Иницируя выполнение определенной послед-

довательности примитивных операций через интерфейс между уровнями, вышерасположенный уровень определяет, какой сервис ему требуется, но он ничего не говорит о том, как эти операции должны быть реализованы. В этом случае нижерасположенный уровень является поставщиком сервиса, а вышерасположенный — пользователем.

Протокол — это набор правил, определяющих формат, назначение и порядок передачи PDU (фреймов, пакетов, сообщений), которыми обмениваются равнозначные активности на определенном уровне. Активности используют сервис для реализации протокола. При этом они могут изменить протокол, но не сервис, видимый их пользователями.

### **2.3.6. Основные вопросы организации уровней**

Все функции организации и работы сети распределены между уровнями. В сетях с разной архитектурой это распределение может быть разным. Однако на каждом уровне должны решаться следующие вопросы.

1. Определение адресов отправителя и получателя на одноименных уровнях: на каждом уровне необходим механизм для определения отправителей и получателей.

2. Определение правил установления соединения на одноименных уровнях.

3. Определение правил передачи данных:

- только в одном направлении (simplex), в обоих направлениях, но не одновременно (half-duplex) или в любом направлении в любое время (duplex);
- допустимое число виртуальных каналов через одно соединение и приоритеты между ними;
- как мультиплексировать и демуплексировать виртуальные каналы.

4. Обнаружение и исправление ошибок.

5. Сохранение исходной последовательности данных при передаче.

6. Наличие механизма, предотвращающего ситуацию, когда получатель начинает «захлебываться», т.е. отправитель шлет пакеты с большей скоростью, чем получатель на одноименном уровне успевают их обрабатывать.

7. Поскольку не все процессы на любом уровне могут работать с сообщениями произвольной длины, необходимо предусмотреть возможность разбиения сообщения на части и сборки сообщения из частей, а также что делать, если процесс работает со столь короткими сообщениями, что их раздельная пересылка неэффективна.

8. Когда между получателем и отправителем имеется несколько маршрутов, требуется определить, какой из них выбрать.

## 2.4. Модель системы передачи данных

### 2.4.1. Общие сведения

Постараемся увязать рассмотренные ранее абстрактные понятия в единую модель. За основу возьмем эталонную модель OSI (Open Systems Interconnection — модель взаимодействия открытых систем — МОС), которая была разработана Международной организацией по стандартизации (International Standards Organization — ISO) для установления международных стандартов компьютерных сетей. Точнее, возьмем ту ее часть, которая описывает передачу данных в компьютерных сетях.

Модель OSI описывает, как должна быть организована любая система, открытая для взаимодействия с другими системами.

Открытой системой называется совокупность программных аппаратных средств и средств коммуникации между ними, к которой

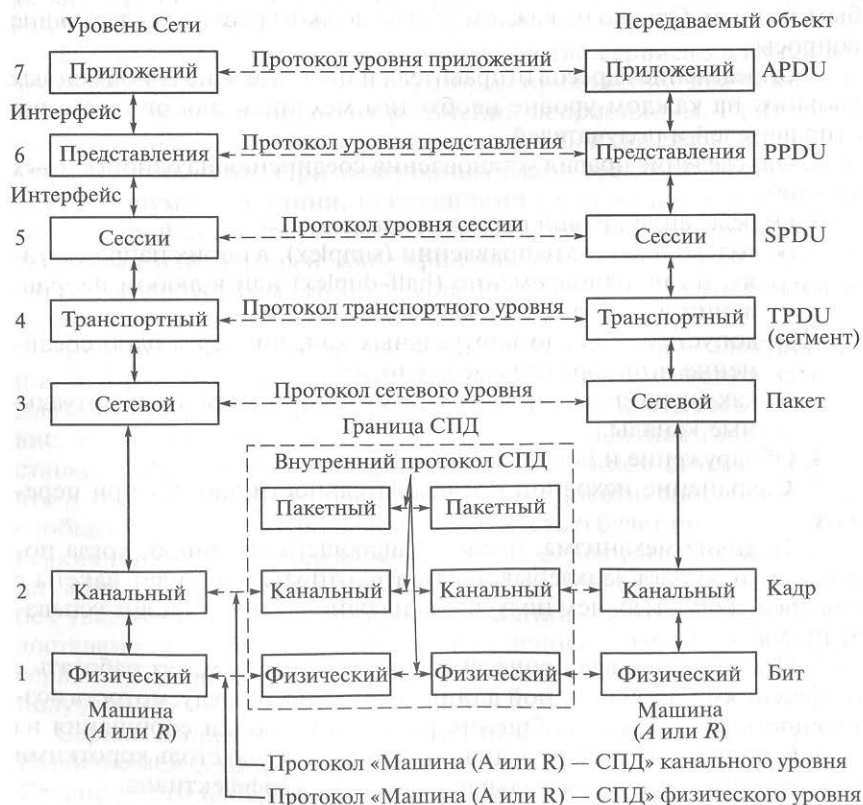


Рис. 2.7. Модель взаимодействия открытых систем

можно добавлять новые компоненты, удалять существующие компоненты или модифицировать их в целях развития и совершенствования функций и сервисов системы. Причем делать это может не только разработчик самой системы. Примером открытой системы является персональный компьютер, к которому можно подключить широкий спектр внешних устройств разных производителей, не имеющих никакого отношения к разработке или производству самих персональных компьютеров. Также можно вводить в состав его программного обеспечения новые приложения, изготовитель которых не имел никакого отношения к созданию операционной системы этого компьютера. Из сказанного ясно, что сеть ЭВМ — это открытая система.

Модель OSI имеет иерархическую структуру с четко выделенными уровнями (рис. 2.7). Принципы выделения этих уровней следующие:

1. Каждый уровень имеет определенное назначение.
2. Каждый уровень защищает вышерасположенный уровень от различий в возможных реализациях.
3. Назначение каждого уровня выбиралось, прежде всего, из условия возможности определения для него международного стандарта.
4. Границы между уровнями определялись условием минимизации потока информации через интерфейсы.
5. Число уровней достаточно большое, т. е. позволяет не объединять разные функции на одном уровне, но и не создает громоздкой архитектуры.

Всего в этой модели семь уровней: физический, канальный, сетевой, транспортный, сессии, представления, приложений. Здесь в качестве модели системы передачи данных мы рассмотрим только первые три уровня, относящиеся к СПД сети (выделены штриховым прямоугольником на рис. 2.7).

Функции остальных четырех уровней (модель TCP/IP) будут рассмотрены во втором томе данного учебника при построении модели транспортной среды и взаимодействия приложений в сети.

Отметим, что OSI — это модель, а не архитектура сети. Она не определяет протоколы и сервисы каждого уровня, а лишь указывает, какие функции должны быть реализованы на каждом уровне.

### **2.4.2. Физический уровень**

Физический уровень отвечает за передачу последовательности битов через физическую линию. Основной проблемой здесь является, как при передаче с одного конца линии 1 получить на другом ее конце также 1, а не 0.

На физическом уровне решаются следующие вопросы:

- каким электромагнитным сигналом следует представлять 1, а каким — 0;

- сколько микросекунд должно тратиться на передачу одного бита;
- следует ли поддерживать передачу данных в обоих направлениях одновременно по одной и той же линии;
- как устанавливать начальное соединение и как его разрывать;
- каково должно быть количество контактов на разъеме устройства и для чего используется каждый контакт.

Следовательно, здесь в основном решаются вопросы механики, электрики и способов представления данных в виде электромагнитных сигналов.

### 2.4.3. Канальный уровень

Основной задачей канального уровня является превращение несовершенной физической среды передачи данных в надежный канал, свободный от ошибок передачи. Эта задача решается разбиением данных отправителя на *фреймы* или *кадры* (обычно содержащие от нескольких сотен до нескольких тысяч байтов), которые передаются последовательно с использованием кадров уведомления, поступающих от получателя. Поскольку физический уровень не распознает структуру в передаваемых данных, то определение границы кадра — это целиком и полностью задача канального уровня данных, которая имеет разные решения (см. гл. 4).

Помехи при передаче на физическом уровне могут разрушить кадр. В этом случае он должен быть передан повторно. Например, посланный и принятый кадр будет послан повторно, если кадр с уведомлением о его получении был потерян. И это уже забота канального уровня, как бороться с дубликатами одного и того же кадра, потерями или искажениями кадров, ошибками при передаче на физическом уровне. Канальный уровень может поддерживать сервис разных классов, т. е. разных качества и стоимости.

Другая проблема, возникающая на канальном уровне (как и на других вышерасположенных уровнях), — это как управлять потоком передачи. Например, как предотвратить «захлебывание» получателя, если отправитель передает данные слишком быстро? Как сообщить передающему размер буфера, имеющийся у получателя, для приема передаваемых данных в этот момент?

Если канал позволяет передавать данные в обоих направлениях одновременно, т. е. если кадры уведомления для потока от *A* к *B* используют тот же канал, что и трафик от *B* к *A*, то можно использовать для передачи уведомлений о кадрах от *B* к *A* попутные кадры от *A* к *B*.

В сетях с вещательным способом передачи, т. е. при котором к одному каналу имеют доступ сразу несколько устройств, возникает проблема управления доступом к общему каналу. За это отвечает специальный подуровень доступа к среде — MAC (Media ACcess) канального уровня.

#### 2.4.4. Сетевой уровень

Основная проблема, решаемая на сетевом уровне, — как построить маршрут между отправителем и получателем. Эта проблема возникает как в СПД, например при коммутации канала в телефонной сети, так и в транспортной среде, когда надо построить маршрут между двумя А-машинами.

Основное отличие решения этой проблемы в СПД от решения в транспортной среде состоит в следующем. Как уже отмечалось (см. подразд. 2.1.2), в СПД маршрут строится методами коммутации на основе информации, заранее закладываемой в узлы коммутации СПД. Эти методы не предполагают трудоемких вычислений, связанных с многокритериальной оптимизацией каждого маршрута, и динамического отслеживания изменений в топологии СПД. Как правило, направление коммутации для потока данных определяют предварительно сделанные настройки.

В транспортной среде основная сложность заключается в выборе именно оптимального маршрута между отправителем и получателем. Во втором томе данного учебника будет показано, что здесь могут применяться разные критерии оптимизации маршрута в зависимости от конкретной ситуации. Маршруты могут определяться заранее и прописываться в статической таблице в каждом узле коммутации, которая не изменяется. Они также могут определяться в момент установления соединения и действовать в течение всего времени жизни этого соединения. Наконец, они могут строиться динамически по ходу передачи в зависимости от загрузки сети и ее текущей конфигурации.

Хочется обратить особое внимание на то, что в транспортной среде на сетевом уровне при построении маршрута фактически решается две задачи: оптимизации и коммутации, т. е. реализации маршрута, тогда как в СПД решается только задача коммутации.

Если в транспортной среде циркулирует слишком много пакетов, то они могут использовать одни и те же маршруты, что приводит к перегрузкам, которые, в свою очередь, приводят к потере пакетов. Эта проблема также решается на сетевом уровне.

Еще одно отличие этого уровня в СПД от его аналога в транспортной среде состоит в том, что в СПД структура и размер PDU на канальном и сетевом уровнях одинаковые, тогда как в транспортной среде это не так. В силу сказанного в СПД этот уровень будем называть пакетным (см рис. 2.7).

Поскольку операторы, регулирующие работу СПД и транспортной среды, разные, то необходимо уметь считать отдельно, сколько пользователь должен заплатить за использованное СПД, а сколько за использование транспортной среды. Что же делать, если абоненты расположены в разных странах, где действуют разные тарифы?

Если пакет адресован в другую сеть, то могут возникнуть следующие проблемы: в ней может быть другой формат пакетов, другой

способ адресации, другой размер пакетов, другие протоколы и т. д., и все эти проблемы решаются на сетевом уровне.

На сетевом уровне решается также задача управления потоком (что делать, если получатель «захлебывается», так как отправитель слишком часто шлет пакеты) и определяется, что надо предпринять, если какой-то канал стал недоступен.

Из сказанного видно, что функции сетевого уровня в СПД и функции сетевого уровня в транспортной среде разные. Обратим внимание, что на рис. 2.7 сетевой уровень в СПД нигде не взаимодействует с сетевым уровнем транспортной среды, тогда как канальный и физический уровни СПД и транспортной среды взаимодействуют по соответствующим общим протоколам. Более того, если на канальном и сетевом уровнях адресация разная, то на канальном и пакетном она одна и та же.

Дальнейшее рассмотрение уровней модели OSI (сетевого, транспортного, сессии, представления и приложений) применительно к сетям ЭВМ продолжим во втором томе данного учебника при построении модели работы транспортной среды и взаимодействия приложений в компьютерных сетях. Здесь же в качестве модели СПД примем первые три уровня эталонной модели ISO с оговорками, сделанными ранее для третьего (пакетного) уровня.

## 2.5. Примеры СПД

### 2.5.1. СПД на основе стандарта Bluetooth

Напомним, что основная задача СПД, которая является частью транспортной среды, — это передача данных между А-машинами и коммуникационными машинами в сети. Напомним также, что основные элементы СПД — это линии связи, каналообразующая аппаратура и всевозможные коммутаторы.

Стандарт Bluetooth относится к классу беспроводных персональных сетей (WPAN).

Спецификация Bluetooth\* [60] представляет собой стандарт обмена информацией между такими устройствами, как карманные и обычные персональные компьютеры, мобильные телефоны, ноутбуки, принтеры, цифровые фотоаппараты, мышки, клавиатуры, джойстики и наушники, на надежной недорогой повсеместно доступной радиочастоте для ближней связи. Протокол Bluetooth обеспечивает сообщение между этими устройствами на расстоянии 10... 100 м друг от друга.

Эта спецификация была разработана компанией Ericsson. Для связи в этом протоколе используется свободный от лицензирования

---

\* Названа в честь датского короля Гарольда Блутуса (X в. н. э.), объединившего скандинавские земли.

диапазон частот 2,40 ... 2,48 ГГц. Среди рассматриваемых беспроводных протоколов Bluetooth является одним из самых медленных. Максимальная скорость передачи здесь не более 2 Мбит/с, а максимальный размер пакета данных 341 байт.

### **2.5.2. СПД на основе стандарта X.25**

Стандарт X.25 (когда-то широко распространенный) в настоящее время используют некоторые телефонные сети, особенно в Европе, для подключения банкоматов. Этот стандарт, разработанный Международным союзом электросвязи (МСЭ) в 1970-х гг., определяет интерфейс между СПД с коммутацией пакетов и терминалом, а также взаимодействие терминалов через сеть передачи данных с коммутацией пакетов. С помощью специального служебного пакета в сети X.25 прокладывается виртуальное соединение между взаимодействующими терминалами.

Поясним это положение. При установлении виртуального соединения не происходит физического соединения линий связи, как в телефонной сети. Инициатор соединения посылает пакет, который содержит имя прокладываемого им виртуального соединения. Далее в каждом узле коммутации выбирается канал, по которому этот пакет направляется, и запоминается, что все пакеты, приписанные к виртуальному соединению с таким именем, следует направлять по выбранному каналу. Таким образом, физически никакого «единого» канала не формируется, но в то же время он существует. После установки по созданному соединению передают пакеты. По окончании передачи отправитель направляет пакет разрыва виртуального соединения, который «стирает» в узлах коммутации записи, «связывающие» имя виртуального соединения с каналом.

Различают виртуальные соединения постоянные и создаваемые по требованию. Соединения, создаваемые по требованию, прокладываются так, как описано ранее. Постоянные виртуальные соединения прописываются «вручную» в таблицах коммутации узлов СПД.

Рекомендации стандарта X.25 определяют способ передачи цифровых данных с коммутацией пакетов по телефонным каналам, который характеризуется следующими свойствами:

- пакеты длиной до 128 байт;
- доступная скорость 64 Кбит/с;
- ориентация на соединение и поддержку режима коммутируемых виртуальных каналов и режима постоянного виртуального канала.

Поскольку к моменту появления стандарта X.25 в мире было уже много оконечных устройств, не рассчитанных на него, появилось решение этой проблемы в виде устройства PAD (Packet Assembler Disassembler), с помощью которого можно было подключать к данной сети оконечные устройства, не предназначенные для работы в ней.

### **2.5.3. СПД на основе Frame Relay**

Ретрансляция кадров (Frame Relay — FR) — это метод доставки сообщений в сетях передачи данных с коммутацией пакетов. К числу достоинств этого метода, прежде всего, необходимо отнести малое время задержки сообщений, простой формат кадров, содержащих минимум управляющей информации, и независимость от протоколов верхних уровней эталонной модели ISO.

Службу FR можно рассматривать как аренду виртуального соединения, позволяющую передавать пакеты длиной до 1 600 байт. Можно заказать постоянную виртуальную линию типа «от одного ко многим». Разница между арендуемой физической линией и виртуальной линией состоит в том, что по физической линии можно передавать данные с максимальной скоростью целый день, а средняя скорость передачи данных по виртуальной линии будет несколько меньше.

Служба FR предоставляет минимальный сервис. Если фрейм поступил с ошибкой, то он просто сбрасывается, и дело пользователя определить, какой фрейм пропущен, и как его восстановить. В отличие от стандарта X.25 служба FR не поддерживает уведомления о доставке и обычное управление потоком.

В настоящее время служба FR предоставляет услуги по передаче пакетов данных через постоянные виртуальные каналы (PVC) и интерфейс пользователь—сеть (UNI). Маршрутизация пакетов по PVC фиксируется заранее в момент установления такого канала и впоследствии не изменяется.

В существующую версию FR не вошли коммутируемые виртуальные каналы (SVC) и интерфейс межсетевое взаимодействия. Однако работа в этих направлениях продолжается, и ее результаты найдут свое отражение в новых стандартах FR.

### **2.5.4. Универсальные СПД и асинхронный способ передачи**

Кроме проблем, связанных с быстро растущими требованиями в области сервиса, существует еще и проблема интеграции различных СПД. Например, проблема интеграции стандарта X.25 и службы FR с СПД DQDB. Связывать и обслуживать все это разнообразие сетей — не простая задача. А имеется еще и кабельное телевидение и т. д.

Выходом из этой ситуации является создание единой сети, обеспечивающей такую высокую скорость передачи, которая будет способна поддерживать любую услугу, т. е. так называемых универсальных систем передачи данных (unified communication).

Интегрированный сервис поддерживает передачу видео-, аудио-, цифровых данных с высоким качеством и обеспечивает высокоскоростную связь между локальными сетями. Одной из основных технологий, которая делает возможным реализацию такого сервиса,

является ATM (Asynchronous Transfer Mode — асинхронный способ передачи).

Главная идея ATM заключается в передаче данных малыми порциями фиксированной длины, называемыми *ячейками*. Каждая такая ячейка имеет длину 53 байт, из которых 48 байт приходится на данные и 5 байт на заголовок.

Существует несколько причин, определяющих удобство передачи данных небольшими пакетами — ячейками:

- ячейки удобно использовать для управления и передачи разнородных данных (звук, видео- и цифровых данных);
- при больших скоростях связи проще управлять коммутацией небольших ячеек, чем использовать старую технику мультиплексирования.

ATM — это технология, ориентированная на соединение, т.е. прежде чем передавать данные необходимо сначала установить соединение. Однако в отличие от телефонных сетей это виртуальное соединение. Доставка данных здесь не гарантируется, но их порядок сохраняется.

ATM, как и любая другая СПД, состоит из каналов и коммутаторов. В настоящее время в ней достигается скорость передачи данных от 155 до 622 Мбит/с.

### 2.5.5. Сравнение различных СПД

В табл. 2.4 для сравнения приведены основные данные по каждой из ранее рассмотренных СПД. При этом может возникнуть вопрос: почему их так много?

Таблица 2.4

Возможности разных СПД

Свойство	DQDB	Bluetooth	X.25	Frame Relay	ATM
Ориентированность на соединение	Есть	Нет	Есть	Есть	Есть
Стандартная скорость передачи, Мбит/с	45	2	0,064	1,5	155
Коммутируемость	Нет	Нет	Есть	Нет	Есть
Фиксированная длина кадра	Есть	Нет	Нет	Нет	Есть
Максимальная длина кадра, байт	44	341	128	1 600	53
Постоянные виртуальные каналы	Нет	Нет	Есть	Есть	Есть
Групповое вещание	Нет	Есть	Нет	Нет	Есть

Все приведенные СПД появились в разное время, под давлением потребностей разных категорий пользователей и разрабатывались разными компаниями из разных областей применения (телефония, цифровые сети, телевизионные сети).

## **2.6. Стандартизация**

### **2.6.1. Стандарты**

Согласно [6] стандартизация — это деятельность по установлению норм, правил и характеристик в целях обеспечения:

- безопасности продукции, работ и услуг для окружающей среды, жизни, здоровья и имущества человека;
- технической и информационной совместимости, а также взаимозаменяемости продукции;
- качества продукции, работ и услуг в соответствии с уровнем развития науки, техники и технологии;
- единства измерений;
- экономии всех видов ресурсов;
- безопасности хозяйственных объектов с учетом риска возникновения природных и техногенных катастроф и других чрезвычайных ситуаций;
- обороноспособности и мобилизационной готовности страны.

Стандарт — это документ, устанавливающий комплекс норм, правил и требований к объекту стандартизации. Стандарт может быть разработан как на материальные предметы (продукцию, эталоны, образцы веществ) и услуги, так и на нормы, правила и требования в различных областях.

### **2.6.2. Кто и как вводит стандарты**

Все организации, имеющие право выпускать документы в области стандартизации, можно подразделить по масштабам географических территорий, на которых документы, выпущенные этими организациями, признаются и соблюдаются как стандарт. С этой позиции различают:

- международные организации;
- региональные международные организации;
- международные промышленные консорциумы и профессиональные ассоциации;
- национальные организации;
- отраслевые организации (действующие в рамках отрасли отдельного государства).

К официальным организациям в международной системе стандартизации информационных технологий относятся:

**ISO** (International Organization for Standardization) — Международная организация по стандартизации — ИСО;

**IEC** (International Electrotechnical Commission) — Международная электротехническая комиссия — МЭК;

**ITU** (International Telecommunication Union) — Международный союз электросвязи — МСЭ.

Кратко изложим историю, основные функции, задачи, структуру и взаимосвязи этих организаций [38].

### **2.6.3. Международная организация по стандартизации**

International Standard Organization (ISO) была создана в 1946 г. двадцатью пятью национальными организациями по стандартизации. Фактически работа ее началась с 1947 г. При создании организации и выборе ее названия учитывалась необходимость одинаковой аббревиатуры этого названия на всех языках, поэтому было решено использовать греческое слово *isos* — равный. Вот почему на всех языках мира Международная организация по стандартизации имеет краткое название ISO (ИСО).

Деятельность ИСО касается стандартизации во всех областях, кроме электротехники, электроники и связи. Стандартизация информационных технологий, микропроцессорной техники и т. п. — это объекты совместных разработок ИСО, Международной электротехнической комиссии и Международного союза электросвязи.

На сегодняшний день в состав ИСО входят 135 стран в лице своих национальных организаций по стандартизации.

Непосредственную работу по созданию международных стандартов выполняют технические комитеты (ТК), подкомитеты (ПК), которые могут учреждать ТК, и рабочие группы (РГ) по конкретным направлениям деятельности. По данным на 2000 г. ИСО насчитывала 2 832 рабочих органа, в том числе 187 ТК, 572 ПК, 2 063 РГ и 75 целевых групп [38]. Обеспечивают работу всех секретариатов ТК и ПК 35 организаций — членов ИСО, в том числе за Россией закреплено 10 ТК, 31 ПК и 10 РГ. При этом заинтересованные организации могут быть активными участниками любого ТК или ПК, а также наблюдателями. Россия является активным участником в 145 ТК, а наблюдателем — в 16. Официальные языки ИСО — английский, французский, русский. На русский язык переведено около 70 % всех стандартов ИСО.

Схема разработки международного стандарта следующая: заинтересованная сторона в лице организации — члена ИСО, технического комитета или комитета Генеральной ассамблеи (либо организации, не являющейся членом ИСО) направляет в ИСО заявку на разработку стандарта. Генеральный секретарь по согласованию с организациями — членами ИСО предоставляет в Техническое руководящее бюро предложение о создании соответствующего ТК. Этот ТК создается при следующих условиях: если большинство организаций — членов ИСО голосуют «за» и не менее пяти из них намерены стать его участниками, а Техническое руководящее бюро убеждено в междуна-

родной значимости будущего стандарта. Все вопросы в процессе работы обычно решаются на основе консенсуса организаций — членов ИСО, активно участвующих в деятельности ТК. После достижения консенсуса ТК передает проект стандарта в Центральный секретариат для регистрации и рассылки всем комитетам на голосование. Если проект одобряется 75 % голосовавших, он публикуется в качестве международного стандарта.

В упрощенном виде в процессе разработки стандарт проходит следующие этапы:

- заявка на разработку стандарта (New Work Item Proposal — NP);
- рабочий документ (Working Draft — WD);
- проект предложения (Draft Proposal — DP);
- проект международного стандарта (Draft International Standard — DIS);
- международный стандарт (International Standard — IS).

Стандарты ИСО не имеют статуса обязательных для всех стран — участниц этой организации. Любая страна мира вправе применять или не применять их. Решение вопроса о применении стандарта ИСО связано в основном со степенью участия страны в международном разделении труда и состоянием ее внешней торговли. В российской системе стандартизации нашли применение около половины всех стандартов ИСО.

#### **2.6.4. Международная электротехническая комиссия**

International Electrotechnical Commission (IEC) — международная организация, занимающаяся разработкой стандартов в области электротехники.

Международная электротехническая комиссия (МЭК), образованная в 1906 г., как и ИСО, является добровольной неправительственной организацией. Ее деятельность в основном связана со стандартизацией физических характеристик электротехнического и электронного оборудования. Основное внимание МЭК уделяет таким вопросам, как электроизмерения, тестирование, способы использования и безопасность электротехнического и электронного оборудования. Членами МЭК являются национальные организации (комитеты) стандартизации технологий в соответствующих отраслях, представляющие интересы своих стран в деле международной стандартизации. В настоящее время в состав МЭК входит более 50 стран.

С организационной точки зрения МЭК похожа на ИСО. Процесс создания стандартов в МЭК аналогичен процессу стандартизации, принятому в ИСО. Только правильнее было бы говорить об аналогичности организации ИСО организации МЭК, так как ИСО создавалась во многом по образу и подобию МЭК. Как и в ИСО, основную работу по разработке стандартов в МЭК выполняют технические комитеты и подкомитеты, общая численность которых более 200.

## 2.6.5. Международный союз электросвязи

International Telecommunications Union (ITU) — международная межправительственная организация, занимающаяся вопросами стандартизации и развития электросвязи.

Международный союз электросвязи (МСЭ) объединяет более 500 правительственных и неправительственных организаций. В состав этой организации входят телефонные, телекоммуникационные и почтовые министерства, ведомства и агентства разных стран, а также организации — поставщики оборудования для обеспечения телекоммуникационного сервиса. Основная задача МСЭ состоит в координации разработки сбалансированных на международном уровне правил и рекомендаций, предназначенных для построения и использования глобальных систем передачи данных и их сервисов.

МСЭ — старейшая международная профессиональная организация. Она была основана в 1865 г. после подписания 20 европейскими государствами первой международной конвенции по телеграфии. Первое ее название было Международный союз по телеграфии (International Telegraph Union), а позднее Международный комитет по телеграфии и телефонии (МКТТ).

В 1947 г. МСЭ получила статус специализированного агентства Организации Объединенных Наций (ООН). Все время своего существования МСЭ отвечал за разработку правил и рекомендаций по развитию глобальных телекоммуникационных сетей и способствующих стандартизации услуг в них, а также за стандартизацию операций по эксплуатации систем электросвязи. МСЭ оперативно отслеживал новейшие достижения, например изобретение телефона и радиотелеграфии, появление спутниковой связи и цифровых систем передачи данных, современных компьютерных сетей и систем мобильной связи и интегрировал эти достижения в глобальные телекоммуникационные услуги.

Поскольку деятельность ИСО и деятельность МЭК часто пересекались в области стандартизации информационных технологий (ИТ), то в 1987 г. этими организациями было принято совместное решение о создании Объединенного технического комитета 1 (Joint Technical Committee 1 — JTC1), основная функция которого была определена как формирование системы стандартов в области ИТ и их расширений для конкретных сфер деятельности.

В документах, регламентирующих работу JTC1, определено, что *информационные технологии включают в себя спецификацию, проектирование и разработку систем и средств, имеющих дело со сбором, представлением, обработкой, безопасностью, передачей, организацией, хранением и поиском информации, а также ее обменом и управлением* [38].

Основными задачами JTC1 являются разработка, поддержание, продвижение стандартов ИТ, необходимых для глобального рынка,

удовлетворяющих требованиям бизнеса и пользователей и относящихся:

- к проектированию и разработке систем и средств ИТ;
- производительности и качеству продуктов и систем ИТ;
- безопасности систем ИТ и информации;
- переносимости прикладных программ;
- интероперабельности продуктов и систем ИТ;
- унифицированным средствам и окружениям;
- гармонизированному словарю понятий в области ИТ;
- дружеским и эргономичным пользовательским интерфейсам.

### **2.6.6. Региональные межправительственные организации по стандартизации**

Региональными межправительственными организациями стандартизации, представляющими интересы крупных регионов или континентов в международном процессе стандартизации, например, являются:

- общеевропейские организации по стандартизации CEN, CENELEC, ETSI [18, 38];
- межскандинавская организация по стандартизации (INSTA);
- международная ассоциация стран Юго-Восточной Азии (АСЕАН);
- панамериканский комитет стандартов (КОПАНТ);
- межгосударственный совет стран — членов СНГ (МГС).

Рассмотрим систему официальных европейских организаций по стандартизации в области ИТ.

#### **CEN (the European Committee for Standardization)**

CEN — европейский комитет по стандартизации широкого спектра товаров, услуг и технологий, в том числе связанных с областью ИТ. Европейский комитет по стандартизации (до 1970 г. — Европейский комитет по координации стандартов) существует с 1961 г. Членами CEN являются национальные организации по стандартизации 18 европейских государств: Австрии, Бельгии, Великобритании, Греции, Дании, Германии, Испании, Исландии, Италии, Люксембурга, Норвегии, Нидерландов, Португалии, Финляндии, ФРГ, Франции, Швеции, Швейцарии. Это закрытая организация, в которую до 1992 г. входили только члены ЕС и ЕАСТ (Европейской Ассоциации Свободной Торговли). Высший орган CEN — Генеральная ассамблея, где представлены национальные организации по стандартизации, правительственные органы стран — членов ЕС и ЕАСТ, а также ассоциированные организации.

В 1998 г. было создано новое подразделение CEN, названное ISSS (the Information Society Standardization System), целью которого является обеспечение участников рынка европейского информационного сообщества системой стандартов для продуктов и сервисов в области информационных и телекоммуникационных технологий.

Основная цель CEN — содействие развитию торговли товарами и услугами посредством:

- разработки европейских стандартов (евронорм, EN);
- применения в странах — членах этого комитета стандартов ИСО и МЭК;
- сотрудничества со всеми организациями региона, занимающимися стандартизацией;
- предоставления услуг по сертификации на соответствие европейским стандартам.

### **ETSI (European Telecommunications Standards Institute)**

Европейский институт стандартизации в области систем передачи данных образован в 1988 г. Основной задачей этой организации является разработка стандартов в области сетевой инфраструктуры.

ETSI ведет работы по следующим основным направлениям:

- кабельные сети (X.25, ISDN, SDN, ATM и пр.);
- беспроводные и мобильные сети (GSM, TETRA, HIPERLAN, радиосети и телевизионные спутниковые сети);
- прикладные телекоммуникационные сервисы глобальной информационной инфраструктуры;
- архитектура сетей и управление сетями;
- межотраслевые решения, включая решения по электромагнитной совместимости, терминальному оборудованию, эргономике и человеческому фактору.

Предметом гордости ETSI является разработанный этим институтом стандарт для мобильной связи GSM, насчитывающий порядка 200 документов.

Значительное внимание ETSI уделяет разработке стандартов базовых и сервисных элементов глобальной информационной инфраструктуры.

ETSI действует в тесном сотрудничестве с CEN. В целях максимальной координации усилий по стандартизации ИТ и систем связи этими организациями был образован Совет по стандартам информационных и коммуникационных технологий (Information and Communication Technologies Standardization Board — ICTSB), с помощью которого осуществляются совместные проекты по разработке наиболее актуальных стандартов.

## Стандартизация в СНГ

Стандартизация в рамках СНГ осуществляется в соответствии с Соглашением о проведении согласованной политики в области стандартизации, метрологии и сертификации, которое является межправительственным и действует с 1992 г. Создан Межгосударственный совет стран — участниц СНГ (МГС), в котором представлены все национальные организации по стандартизации этих государств. МГС принимает межгосударственные стандарты.

В 1995 г. Совет ИСО признал МГС региональной организацией по стандартизации в странах СНГ. Работа по стандартизации ведется в соответствии с программами, которые МГС составляет на основе обобщения предложений, поступающих от национальных органов по стандартизации.

МГС подписал соглашения с МЭК и CEN о сотрудничестве. В МГС также принято соглашение об условиях прямого применения европейских стандартов в качестве межгосударственных для стран СНГ.

### **2.6.7. Промышленные консорциумы и профессиональные ассоциации**

В последнее десятилетие особенно быстрыми темпами стандартизация развивалась силами промышленных консорциумов и профессиональных ассоциаций. Основным достоинством этого вида стандартизации является высокая скорость процесса разработки и согласования стандартов (например, в форме открытых спецификаций). Заинтересованность участников консорциума в достижении конечного результата в сжатые сроки, как правило, позволяет успешно решать вопросы, связанные с финансовым обеспечением проектов стандартизации. Отслеживает и специфицирует деятельность консорциумов CEN/ISSS. К началу 2000 г. этой организацией было зарегистрировано около 150 консорциумов, работающих в области стандартизации ИТ [38].

Наиболее известными представителями этой группы организаций — разработчиков стандартов являются:

- **IEEE** (Institute of Electrical and Electronic Engineers — Институт инженеров по электротехнике и электронике) — профессиональная международная организация, являющаяся разработчиком ряда важных международных стандартов ИТ;
- **OMG** (Object Management Group — группа управления объектами) — международный консорциум, осуществляющий разработку стандартов унифицированного распределенного программного обеспечения, созданного на принципах объектно-ориентированного подхода;

• **ЕСМА** (European Computer Manufacturers Association — Европейская ассоциация производителей вычислительных машин) — международная ассоциация, осуществляющая промышленную стандартизацию информационных и коммуникационных систем;

• **W3C** (World Wide Web Consortium) — консорциум, который специализируется в области разработки и развитии стандартов WWW-технологий, например HTTP, HTML, URL, XML;

• **ATM Forum** (Asynchronous Transfere Mode) — консорциум, осуществляющий разработку и развитие стандартов широкополосных сетей асинхронного режима передачи данных;

• **Gigabit Ethernet Alliance** — консорциум, осуществляющий разработку стандартов технологий Ethernet нового поколения (совместно с комитетом IEEE с индексом 802.3z), обеспечивающих скорость передачи данных в 1 Гбит/с.

Следует подчеркнуть, что одной из главных тенденций процесса стандартизации является все более тесная интеграция деятельности этих организаций, направленная на создание единой системы стандартизации информационного общества.

### **2.6.8. Национальные организации по стандартизации**

К этому уровню относятся государственные организации, отвечающие в своих странах за процесс стандартизации. В каждой современной индустриально развитой стране существует одна организация по стандартизации, представляющая данную страну в ИСО в качестве участника международного процесса стандартизации.

Такие организации, входящие в состав ИСО и называемые организациями национальных стандартов (National Standards Bodies), выполняют следующие задачи:

• участвуют в разработке и принятии международных стандартов с учетом национальных интересов;

• выполняют локализацию и адаптацию международных стандартов для их успешного применения в своих странах, а также способствуют разработке национальных стандартов в соответствии с международными стандартами;

• передают в ИСО для стандартизации на международном уровне разработанные ими спецификации (или разработанные аккредитованными ими организациями), являющиеся национальными стандартами.

Примерами национальных организаций, внесших значительный вклад в развитие международной системы стандартов в области ИТ, являются:

• **ANSI** (American National Standards Institute) — американский институт национальных стандартов. Организация, устанавливающая государственные стандарты в США в различных сферах деятельности, включая информационные технологии;

- **AFNOR** (Association Francaise de Normalisation) — французская ассоциация по стандартизации, аналогичная по назначению ANSI;
- **BSI** (British Standards Institute) — британский институт стандартов;
- **DIN** (Deutsches Institute fur Normung e.v.) — германская организация национальных стандартов;
- **JISC** (Japanese Industrial Standards Committee) — японский комитет промышленных стандартов.

Как уже отмечалось, только одна организация может представлять свою страну в ИСО. При этом в любой стране могут существовать и другие организации по стандартизации национального уровня.

Национальным органом по стандартизации в России является Госстандарт России. Это федеральный орган исполнительной власти, осуществляющий межотраслевую координацию, а также функциональное регулирование в области стандартизации, метрологии и сертификации в стране. С основными функциями Госстандарта России можно ознакомиться в [26].

Составление планов в области информационных технологий находится в ведении Госстандарта России, который является основным заказчиком по государственным основополагающим стандартам, а также по исследованиям в области международных и региональных стандартов относительно принятия и применения их в качестве государственных или национальных. Заказчиками могут быть также отраслевые ведомства, предприятия, научно-технические и другие общества, в том числе общества по защите прав потребителей.

Постоянными рабочими органами в системе Госстандарта России являются технические комитеты, но это не исключает разработки нормативных документов по стандартизации предприятиями, общественными объединениями и другими субъектами хозяйственной деятельности. Технические комитеты могут заниматься стандартизацией как в инициативном порядке, так и по договорам на выполнение такого задания в соответствии с программами ТК и планами государственной стандартизации. Технические комитеты специализируются в зависимости от объекта стандартизации. В рамках этой специализации в ТК проводится также работа и по международной (региональной) стандартизации.

Более подробно система стандартизации в Российской Федерации рассматривается в [27].

**ФИЗИЧЕСКИЙ УРОВЕНЬ****3.1. Теоретические основы передачи данных****3.1.1. Общие сведения**

Рассмотрим самый нижний уровень в иерархии сетевых протоколов. Изучение этого уровня начнем со знакомства с теоретическими принципами передачи данных, чтобы понять физические законы, ограничивающие возможность передачи данных по какой-либо физической среде. Затем рассмотрим основные виды физических сред, пригодных для передачи сигналов, и примеры систем, использующих эти физические среды.

Любая информация может передаваться с помощью электромагнитных импульсов (сигналов). В зависимости от среды передачи и организации СПД используются либо аналоговые, либо цифровые сигналы (см. подразд. 3.1.3).

Любой сигнал можно рассматривать либо как функцию времени, т.е. как изменение различных параметров сигнала во времени, либо как функцию частоты, поскольку любой сигнал можно рассматривать как композицию составляющих сигналов определенной частоты. Такие составляющие сигнала называются гармониками разной частоты. Важной характеристикой является ширина полосы сигнала, которая покрывает весь спектр частот гармоник, составляющих сигнал. Чем шире эта полоса, тем больше информационная емкость сигнала, но тем более строгие требования предъявляются к той среде, по которой он может эффективно распространяться. Далее будут подробно рассмотрены эти понятия и их взаимосвязи.

Основной проблемой при построении СПД является искажение сигнала при передаче, основными причинами которого являются затухание сигнала, неравномерность затухания по частоте, искажение формы сигнала, разные виды шумов. Шумы возникают, например, вследствие термодинамических свойств проводника, интерференции гармоник, составляющих сигнал, и внешних электромагнитных воздействий.

В случае аналогового сигнала эти искажения носят случайный характер и приводят к потере информации. В случае цифрового сигнала они приводят к ошибкам передачи. Далее на примере покажем, почему так происходит.

При создании любой СПД приходится искать компромисс между следующими четырьмя основными факторами: шириной полосы сигнала, скоростью передачи сигнала, уровнем шумов и искажений сигнала, допустимым уровнем ошибок при передаче.

### 3.1.2. Разные формы представления сигнала

Как уже было сказано, любой сигнал можно рассматривать либо как функцию времени, либо как функцию частоты. В первом случае функция показывает, как изменяются со временем параметры сигнала, например напряжение или сила тока. Если такая функция имеет непрерывный характер, то говорят о непрерывном, или аналоговом, сигнале. Если же эта функция имеет дискретный вид, то говорят о дискретном сигнале.

Частотное представление функции основано на том факте, что любую функцию от вещественной переменной можно представить в виде ряда Фурье:

$$g(t) = \frac{1}{2}c + \sum_{n=1}^{\infty} a_n \sin(2\pi nft) + \sum_{n=1}^{\infty} b_n \cos(2\pi nft), \quad (3.1)$$

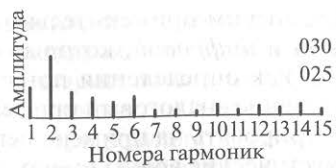
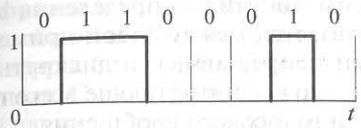
где  $a_n, b_n$  — амплитуды  $n$ -й гармоники;  $f$  — частота.

Ясно, что на практике невозможно учесть бесконечно много гармоник, но все их учитывать и не требуется, поскольку энергия сигнала распределяется неравномерно между гармониками разной частоты. В общем случае низкочастотные составляющие сигнала несут большую часть энергии. Однако, чем больше учитывается составляющих, тем точнее можно воссоздать вид функции.

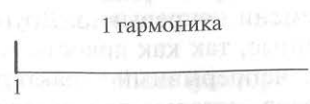
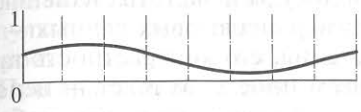
На рис. 3.1 показаны зависимость формы сигнала от числа используемых гармоник и представление сигнала как функции частоты.

Ни в какой среде сигнал не может передаваться без потери энергии. Однако разные среды по-разному поглощают энергию в зависимости от частоты сигнала, и поэтому по-разному искажают его форму. С ростом частоты сигнала искажения растут. При этом любая среда передачи ограничивает максимальную частоту передаваемого сигнала, а следовательно, и частоту гармоник, которые можно использовать для аппроксимации функции  $g(t)$ . Тем самым ограничивается число гармоник, а следовательно, и точность воспроизведения формы сигнала, а также понижается скорость передачи (см. рис. 3.1).

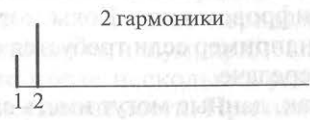
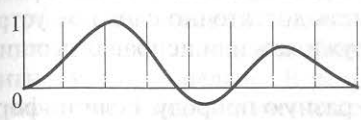
Характеристика канала, определяющая спектр частот, которые физическая среда канала пропускает без существенного понижения мощности сигнала, называется *полосой пропускания канала*. Значение «существенного» понижения мощности определяется для конкретных случаев. Обычно падение мощности сигнала считается существенным, если оно составляет более 50 % от ее начального зна-



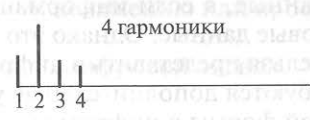
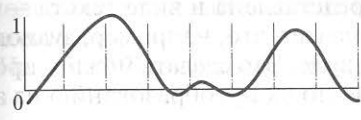
a



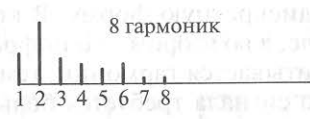
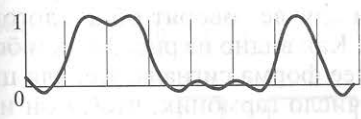
б



в



г



д

Рис. 3.1. Сигнал, представленный как функция частоты:

a — передаваемые данные; б...д — формы воспроизводимого сигнала в зависимости от числа используемых гармоник

чения на единицу длины проводника. Полосу пропускания канала можно ограничивать искусственно с помощью специального частотного фильтра.

### 3.1.3. Сигналы, данные, передача

Важно различать следующие три основных понятия:

- *данные* — это то, с помощью чего мы описываем явление или объект;
- *сигнал* — это представление данных;
- *передача* — это процесс взаимодействия передатчика приемника в целях получения приемником сигналов от передатчика.

Рассмотрим применительно к этим понятиям определения *аналоговый* и *цифровой*, которые соотносятся между собой примерно так же, как определения понятиями непрерывный и дискретный. Определение аналоговый применительно к данным проще всего проиллюстрировать на примере передачи голосового сообщения.

Акустические волны имеют аналоговый характер, т. е. значения их основных параметров, например амплитуды и частоты, изменяются во времени непрерывно. Другой пример аналоговых данных — видеоданные, так как яркость изображения, его контрастность также имеют непрерывный характер. Совсем иное дело текст — цепочка символов, которые представлены в виде кодов, например, наборов из нулей и единиц. Эти коды можно легко представить в дискретном или цифровом виде. Коды могут иметь достаточно сложное устройство, например если требуется обнаруживать или исправлять ошибки при передаче.

Итак, данные могут иметь самую разную природу. Если информация представлена в виде аудио- или видеоданных значит, это аналоговые данные, а если информация представлена в виде текста — это цифровые данные. Однако это не означает, что, например, аудиоданные нельзя представить в цифровом виде. Это сделать можно, просто потребуются дополнительные усилия по их преобразованию из аналоговой формы в цифровую.

Сигналы, как уже говорилось, могут иметь либо непрерывную, либо дискретную форму. В первом случае говорят об аналоговом сигнале, а во втором — о цифровом. Как видно из рис. 3.1, чем больше учитывается гармоник, тем точнее форма сигнала, т. е. для цифрового сигнала требуется большое число гармоник, чтобы он имел ступенчатую форму.

Очень важно также, какое количество уровней может иметь сигнал. Чем больше число уровней сигнала, тем больше информации можно передать за один переход с уровня на уровень. Например, при наличии у сигнала только двух уровней, соответствующих 0 и 1, для передачи 8-разрядного кода символа требуется восемь сигналов. Если же сигнал может иметь восемь уровней, то для такой передачи потребуется только три таких сигнала, т. е. три изменения его уровня. Причем если скорости изменения уровня сигнала при его передаче в первом и во втором случаях одинаковые, то скорость передачи данных во втором случае будет выше более чем в два раза.

Процесс передачи также может иметь аналоговую или цифровую форму. Аналоговая передача предполагает непрерывное изменение параметров передаваемого сигнала. Цифровая передача представляет собой резкое дискретное изменение параметров передаваемого сигнала или импульса.

Сигнал в цифровой форме нельзя непосредственно передать средствами аналоговой передачи, или, как ее еще называют, аналоговой модуляции. Для этого требуется специальное оборудование — модем.

Цифровое кодирование, или цифровая передача, позволяет передавать оба вида сигнала. В случае использования аналогового сигнала и цифровой модуляции происходит предварительное оцифровывание сигнала. Смысл процесса оцифровки состоит в том, что с определенной частотой замеряется уровень сигнала, и результаты замера представляются в виде некоторого кода, который передается с помощью цифрового кодирования. Далее будет показано, что уровни и вид импульса при цифровом кодировании имеют большое значение для скорости и надежности передачи.

При аналоговой и цифровой передачах влияние факторов, искажающих передаваемый сигнал, различное. Поскольку при передаче всегда происходит потеря энергии сигнала, то при передаче на большие расстояния передаваемый сигнал необходимо периодически усиливать. Однако при этом будет усиливаться и шум, примешанный к сигналу при передаче. В результате после нескольких усилений форма сигнала может измениться до неузнаваемости. При использовании цифровых сигналов это приведет к ошибке передачи, а при использовании аналоговых сигналов — к искажению или просто потере сигнала.

На рис. 3.2 показано влияние шума на цифровой сигнал.

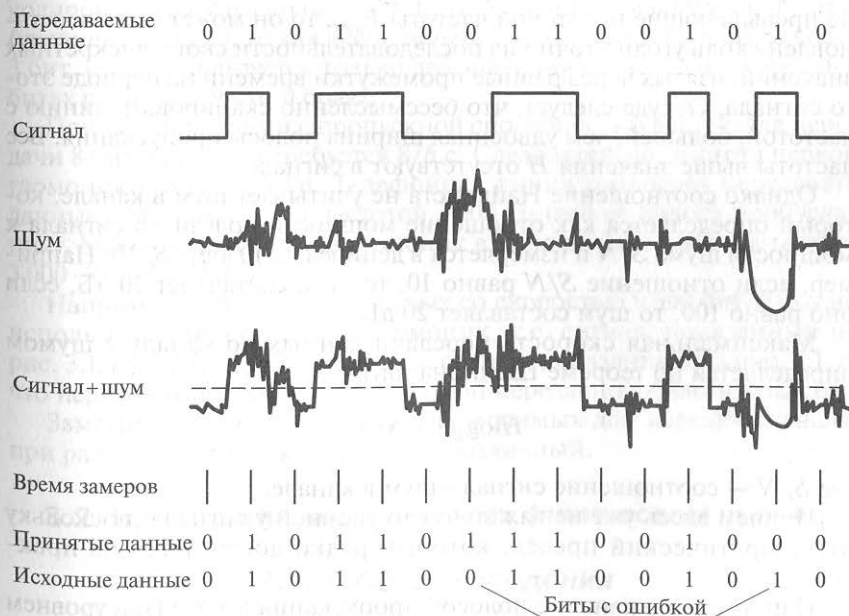


Рис. 3.2. Влияние шума на цифровой сигнал

### 3.1.4. Взаимосвязь пропускной способности канала и его полосы пропускания

Максимальная скорость, с которой канал способен передавать сигнал, называется *пропускной способностью канала*.

В 1924 г. Найквист открыл взаимосвязь пропускной способности канала и его полосы пропускания, согласно которой максимальная скорость передачи данных, бит/с, не может превышать значение

$$2H\log_2 V,$$

где  $H$  — ширина полосы пропускания канала, Гц;  $V$  — число уровней в сигнале.

Из этой формулы следует, что, например канал с полосой 3 кГц не может передавать двухуровневые сигналы со скоростью более 6 000 бит/с.

В 1933 г. В. А. Котельниковым было доказано одно из фундаментальных положений теории связи: аналоговый сигнал  $u(t)$ , не содержащий частот выше  $F_{\max}$ , Гц, полностью определяется последовательностью своих значений в моменты времени, отстоящие друг от друга на  $1/(2F_{\max})$ .

Согласно теореме Котельникова, если сигнал имеет ограниченный спектр, т. е. если все его спектральные составляющие имеют частоты, не превышающие некоторой частоты  $F_{\max}$ , то он может быть восстановлен сколь угодно точно из последовательности своих дискретных значений, взятых через равные промежутки времени на периоде этого сигнала. Откуда следует, что бессмысленно сканировать линию с частотой, большей, чем удвоенная ширина полосы пропускания. Все частоты выше значения  $H$  отсутствуют в сигнале.

Однако соотношение Найквиста не учитывает шум в канале, который определяется как отношение мощности полезного сигнала к мощности шума  $S/N$  и измеряется в децибелах:  $10 \log_{10}(S/N)$ . Например, если отношение  $S/N$  равно 10, то шум составляет 10 дБ, если оно равно 100, то шум составляет 20 дБ.

Максимальная скорость передачи данных по каналу с шумом определяется по теореме Шеннона, бит/с:

$$H\log_2(1 + S/N),$$

где  $S/N$  — соотношение сигнал—шум в канале.

Причем здесь уже не важно число уровней у сигнала, поскольку это теоретический предел, который редко достигается на практике.

Например, по каналу с полосой пропускания в 3 000 Гц и уровнем шума 30 дБ (это характеристики стандартной телефонной линии) нельзя передать данные быстрее, чем со скоростью 30 000 бит/с.

### 3.1.5. Сигналы с ограниченной полосой пропускания

Рассмотрим теперь, как влияет на скорость передачи данных способ их представления.

Пусть требуется передать символ  $b$  в ASCII-коде — 01100010.

На рис. 3.1,  $a$  показаны форма сигнала и его основные гармоники. Коэффициенты этих гармоник могут быть получены из уравнения (3.1) в следующем виде:

$$a_n = \frac{2}{T} \int_0^T g(t) \sin(2\pi nft) dt; \quad b_n = \frac{2}{T} \int_0^T g(t) \cos(2\pi nft) dt.$$

На рис. 3.1,  $b...d$  показаны формы передаваемого сигнала в зависимости от числа используемых гармоник.

Как уже отмечалось (см. подразд. 3.1.3), скорость передачи зависит от способа представления данных на физическом уровне и сигнальной скорости, или скорости модуляции, т. е. скорости изменения уровня сигнала. Скорость изменения уровня сигнала в секунду измеряется в единицах, называемых бод (в честь изобретателя кода для телетайпа Э. Боде).

Иногда ошибочно считают, что если скорость изменения значения сигнала составляет  $b$  бод, то это означает, что данные передаются со скоростью  $b$  бит/с. Это верно лишь в том случае, если мощность множества значений сигнала равна двум. Многое при этом зависит от способа кодирования сигнала: одно изменение значения может кодировать сразу несколько бит. Если используется восемь значений (уровней) сигнала, то каждое изменение его значения кодирует сразу 3 бит. Если используется только два значения сигнала, то скорость в битах равна скорости в бодах.

При наличии линии с пропускной способностью  $b$  бит/с для передачи 8 бит данных потребуется  $8/b$  с. Следовательно, частота первой гармоники будет  $b/8$  Гц. Телефонная линия позволяет передавать данные с максимальной частотой 3 000 Гц (это ее полоса пропускания). Максимальное число гармоник в этом случае может составлять  $3\,000 \cdot 8/b = 24\,000/b$ .

Например, для передачи данных со скоростью 9 600 бит/с можно использовать не более двух гармоник, т. е. сигнал, показанный на рис. 3.1,  $a$ , будет передаваться, как сигнал, показанный на рис. 3.1,  $c$ , что переводит проблему качественной передачи в область фокусов.

Заметим, что спектр частот, необходимых для передач сигнала, при разных способах кодирования различный.

## 3.2. Представление данных на физическом уровне

### 3.2.1. Общие сведения

Как уже известно, способ представления данных существенно влияет на скорость их передачи. Ранее уже отмечалось, что данные



Рис. 3.3. Схемы цифровой (а) и аналоговой (б) передач

могут быть представлены либо в аналоговой, либо в цифровой форме.

На рис. 3.3 показаны схемы цифровой и аналоговой передач. При цифровой передаче данные из источника  $g(t)$  преобразуются в цифровой сигнал  $x(t)$ . Причем данные  $g(t)$  могут быть как аналоговыми, так и цифровыми. Форму сигнала  $x(t)$  должно обеспечивать оптимальное использование возможности среды передачи. Например, создание канала с максимальной пропускной способностью.

Основной аналоговой передачей является непрерывный сигнал с постоянной частотой, который называется *несущим сигналом*. Частоту несущего сигнала выбирают исходя из характеристик физической среды передачи. Данные передают, изменяя параметры несущего сигнала, или, как говорят в этом случае, модулируя несущий сигнал. Процесс модуляции состоит в управляемом изменении трех основных параметров сигнала: частоты, амплитуды и фазы.

Как видно из рис. 3.3, на практике возможны следующие четыре комбинации данные — сигнал:

- цифровые данные — цифровой сигнал. Оборудование для преобразования данных в цифровой форме в цифровой сигнал дешевле и проще, чем оборудование для преобразования данных в аналоговой форме в цифровой сигнал;
- аналоговые данные — цифровой сигнал. Использование сигнала в цифровой форме позволяет использовать современные средства цифровой передачи, преимущества которой по сравнению с аналоговой отмечались ранее;
- цифровые данные — аналоговый сигнал. Такая комбинация возможна при необходимости подключения к аналоговому каналу передачи данных источника данных в цифровой форме;

• аналоговые данные — аналоговый сигнал. Аналоговые данные в электрической форме могут легко и дешево передаваться с помощью аналоговых сигналов. Хорошим примером здесь является телефония (см. гл. 5), а также радиоканалы.

Рассмотрим каждую из этих комбинаций.

### 3.2.2. Цифровые данные — цифровой сигнал

Рассмотрим представление цифровых данных с помощью сигналов в цифровой форме и то, как это представление влияет на передачу данных.

Цифровой сигнал — это дискретная последовательность импульсов напряжения, каждый из которых имеет ступенчатую форму. Каждый импульс — это единичный сигнал. В общем случае данные в двоичной форме при передаче кодируются таким образом, чтобы один бит данных можно было отобразить несколькими единичными сигналами. В простейшем случае это соответствие имеет однозначный характер: один бит должен соответствовать одному единичному сигналу. В примерах, приведенных ранее, как раз рассматривался именно этот простейший случай, когда двоичная 1 была представлена высоким потенциалом, а двоичный 0 — низким. Здесь же мы рассмотрим разные схемы кодирования данных на физическом уровне.

Если все единичные сигналы имеют одинаковую полярность (т.е. все положительную или все отрицательную), то говорят, что сигнал униполярный. В противном случае логическую единицу представляют положительным потенциалом, а логический нуль — отрицательным.

Скорость передачи данных — это количество бит информации в секунду, передаваемых с помощью сигналов. Эту скорость также называют *битовой скоростью*.

*Продолжительность (длина) бита* — это интервал времени, необходимого передатчику для передачи последовательности единичных сигналов, соответствующей одному биту. При скорости передачи данных  $R$ , бит/с, длина бита равна  $1/R$ . Напомним, что скорость модуляции, или сигнальная скорость, измеряемая в бодах, — это скорость изменения уровня сигнала. Очень многое при этом зависит от способа кодирования данных. Как уже отмечалось в подразд. 3.1.3 и 3.1.5, в зависимости от способа кодирования за одно изменение уровня сигнала можно передать несколько бит данных.

Теперь рассмотрим, какие задачи должен решать приемник при передаче данных, что хорошо иллюстрирует рис. 3.2. Прежде всего, приемник должен быть точно настроен на длину бита: он должен уметь распознавать начало и конец передачи каждого бита, а также уровень сигнала — низкий или высокий. На рис. 3.2 эти задачи решаются измерением уровня сигнала в середине длины бита и сравнением результата измерения с пороговым значением. Из-за шума на линии при этом могут возникать ошибки.

Как уже отмечалось, есть три важных фактора, влияющих на правильность передачи: уровень шума, скорость передачи данных и ширина полосы пропускания канала. Кроме того, существует еще один фактор, влияющий на правильность передачи данных, — это способ представления (кодирования) данных на физическом уровне. Рассмотрим наиболее распространенные из этих способов (рис. 3.4).

Основными критериями сравнения различных способов кодирования данных на физическом уровне являются:

- *ширина спектра сигнала.* Чем меньше высокочастотных составляющих в сигнале, тем уже полоса пропускания канала, требуемого для его передачи. Важно также отсутствие в сигнале постоянной составляющей, т.е. гармоники с постоянными не изменяющимися параметрами. Появление такой гармоники приводит к появлению постоянного тока между приемником и передатчиком, что крайне нежелательно. Наконец, как уже отмечалось, ширина спектра влияет на искажение формы сигнала. Чем шире спектр, тем сильнее искажение;

- *наличие синхронизации между приемником и передатчиком.* Ранее уже отмечалась необходимость для приемника точно определять начало и конец битового интервала. На небольших расстояниях, например внутри компьютера или между компьютером и его периферийными устройствами, для этих целей используется дополнительная линия синхронизации. По этой линии специальная такти-

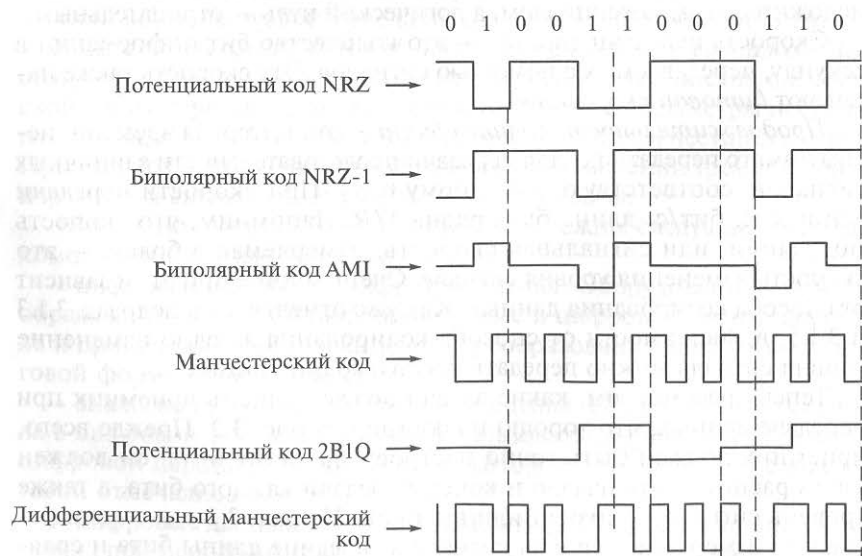


Рис. 3.4. Примеры наиболее распространенных кодов

рующая схема (часы) через строго определенные промежутки времени выдает синхроимпульсы. Приход такого импульса для приемника означает начало битового интервала.

В сетях на больших расстояниях такое решение проблемы не годится по многим причинам. Решение проблемы в этом случае состоит в создании так называемых самосинхронизирующихся кодов. Например, наличие перепада в уровне сигнала (фронта) может служить признаком для приемника о начале битового интервала. Отсутствие фронта между битовыми интервалами существенно усложняет решение проблемы синхронизации, в случае если в соседних битовых последовательностях требуется передать биты с одинаковыми значениями;

- *возможность обнаружения ошибок.* Хотя методы обнаружения и исправления ошибок располагаются на канальном уровне, который находится над физическим уровнем, тем не менее и на физическом уровне весьма полезно иметь такие возможности;

- *чувствительность к шуму.* За счет надлежащих ухищрений в схеме кодирования можно добиться высокой стойкости при передаче данных даже при наличии очень высокого уровня шума;

- *стоимость и скорость.* Несмотря на постоянное снижение стоимости цифровой аппаратуры, общая тенденция увеличения сигнальной скорости в целях увеличения битовой скорости ведет к подорожанию аппаратуры.

Все схемы кодирования подразделяются на потенциальные и импульсные. В потенциальных кодах значение бита передается удержанием потенциала сигнала на определенном уровне в течение битового интервала. В импульсных кодах значение бита передается перепадом (фронтом) уровня сигнала. Направление этого перепада с низкого на высокий или с высокого на низкий уровень определяет значение бита.

### Потенциальный NRZ-код

В схеме кодирования NRZ (Non return to zero — без возврата к нулю на битовом интервале) логическому 0 и логической 1 сопоставлены два устойчиво различаемых потенциала. К достоинствам этого кода следует отнести простоту реализации, устойчивость к ошибкам и достаточно узкий частотный спектр сигнала.

Основным недостатком этого кода является отсутствие синхронизации. На длинных последовательностях нулей или единиц, т.е. когда потенциал на линии не изменяется, может произойти рассинхронизация между приемником и передатчиком, что приведет к ошибкам. Однако если исключить возможность появления длинных последовательностей нулей или единиц, то этот метод может быть весьма эффективен. Обеспечивают отсутствие таких последовательностей специальные устройства, называемые *скремблерами*.

Модификацией NRZ-кода и хорошим примером дифференциального кодирования является код NRZ-I. Идея дифференциальных кодов состоит в том, чтобы кодировать не абсолютное значение текущего бита, а разницу значений между предыдущим битом и текущим. В случае использования кода NRZ-I, если текущий бит — 0, то он кодируется тем же потенциалом, что и предыдущий бит, если же текущий бит — 1, то он кодируется потенциалом, отличающимся от предыдущего потенциала. За счет этого код NRZ-I по сравнению с NRZ-кодом является более устойчивым к шуму.

### Биполярный код AMI

Другим примером потенциального кода является биполярный код с альтернативной инверсией (Bipolar Alternate Mark Inversion — AMI). В этом коде используются не два уровня сигналов, как в NRZ-кодах, а три: положительный, нуль и отрицательный. Значению 0 здесь соответствует нулевой потенциал на линии, а значению 1 — либо положительный, либо отрицательный потенциал. Причем потенциал каждой последующей единицы противоположен потенциалу предыдущей.

У этого кода есть несколько существенных преимуществ по сравнению с NRZ-кодами.

*Во-первых*, в случае длинной последовательности единиц не происходит рассинхронизации. Поскольку каждая единица здесь сопровождается изменением потенциала, устойчиво распознаваемым приемником, не возникнет постоянной составляющей. Однако длинная последовательность нулей в этом коде остается проблемой, и требуется принятие дополнительных мер, позволяющих избежать ее появления.

*Во-вторых*, для различных комбинаций бит на линии использование кода AMI обеспечивает более узкий спектр сигнала, чем в коде NRZ, а значит, и более высокую пропускную способность линии.

*В-третьих*, свойство чередования уровней позволяет обнаруживать единичные ошибки.

При использовании надлежащей техники скремблирования биполярные коды обладают лучшими характеристиками, чем NRZ-коды. Однако это превосходство не бесплатное: каждый единичный сигнал здесь может иметь один из трех уровней, а поэтому он может нести  $\log_2 3 = 1,58$  бит информации, из которых используется только один бит, т.е. информационная эффективность этого кода ниже. Кроме того, передатчик и приемник, необходимые для биполярного кода AMI, сложнее, чем применяемые для NRZ-кодов.

### Биполярные импульсные коды

Существует другая группа методов кодирования, известных как биполярное импульсное кодирование. Рассмотрим широко распространенные из этой группы манчестерский и дифференциальный манчестерский коды.

В манчестерском коде (см. рис. 3.4) данные кодируются фронтами сигналов в середине битового интервала. Этим достигаются две цели: синхронизация приемника и передатчика и передача данных (фронт перехода от низкого потенциала к высокому соответствует единице, а фронт перехода от высокого потенциала к низкому — нулю).

В дифференциальном манчестерском коде сигнал может изменять свой уровень дважды в течение битового интервала. В середине интервала обязательно происходит изменение уровня сигнала, и этот перепад используется для синхронизации. При передаче нуля в начале битового интервала также происходит перепад уровней сигнала, а при передаче единицы такой перепад отсутствует.

Во всех биполярных импульсных кодах происходит от одного до двух перепадов уровня сигнала за один битовый интервал, поэтому их сигнальная скорость в два раза выше, чем у потенциальных кодов. Это означает, что они требуют более широкой полосы пропускания, чем потенциальные коды. Однако они имеют несколько существенных преимуществ:

- самосинхронизация;
- отсутствие постоянной составляющей;
- возможность обнаружения единичных ошибок.

Манчестерский и дифференциальный манчестерский коды используются, например, в широко распространенном стандарте локальных сетей Ethernet. Далее будут более подробно рассмотрены реализация данных кодов для стандарта IEEE 802.3 и коды, используемые для высокоскоростных локальных сетей Fast Ethernet и Gigabit Ethernet.

### Потенциальный код 2B1Q

В этом методе кодирования каждые два последовательных бита (2B) информации передаются за один битовый интервал сигнала, который может иметь четыре состояния (1Q). Здесь 00 соответствует потенциал  $-2,5$  В; 01 — потенциал  $-0,833$  В; 11 — потенциал  $+0,833$  В; 10 — потенциал  $+2,5$  В.

В этом методе кодирования сигнальная скорость в два раза ниже, чем в кодах NRZ и AMI, а спектр сигнала в два раза уже, следовательно, с помощью кода 2B1Q можно по одной и той же линии передавать данные в два раза быстрее. Однако реализация этого метода требует наличия более мощного передатчика и более сложного приемника, который должен различать не два уровня сигнала, как у рассмотренных ранее биполярных методов, а четыре.

### Сигнальная скорость

Рассмотрим, как метод кодирования влияет на скорость передачи данных (битовую скорость) и сигнальную скорость.

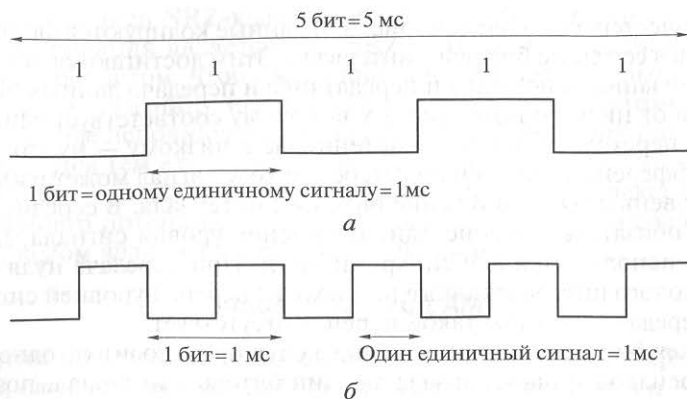


Рис. 3.5. Соотношение сигнальных скоростей при разных методах кодирования:

а — код NRZ-1; б — манчестерский код

Как уже отмечалось, битовая скорость равна  $1/t_b$ , где  $t_b$  — длина бита. Сигнальная скорость показывает скорость изменения уровня сигнала.

Возьмем для примера манчестерский код. Минимальный размер единичного сигнала в нем равен половине битового интервала. Для последовательности из нулей или единиц будет генерироваться последовательность таких единичных сигналов, поэтому сигнальная скорость манчестерского кода равна  $2/t_b$ . На рис. 3.5 показано соотношение сигнальных скоростей при разных методах кодирования последовательности из единиц при битовой скорости, равной 1 Мбит/с.

В общем случае сигнальная скорость  $D = R/b$ , где  $R$  — битовая скорость, бит/с;  $b$  — число битов в единичном сигнале.

### 3.2.3. Цифровые данные — аналоговый сигнал

Теперь рассмотрим передачу данных в цифровой форме с помощью аналоговых сигналов. Например, широко известно использование телефонных сетей для передачи цифровых данных. Телефонные сети (см. подразд. 4.2) были созданы для передачи и коммутации аналоговых сигналов в голосовом диапазоне частот от 300 до 3400 Гц. Этот диапазон не совсем подходит для передачи цифровых данных, поэтому подключить источник таких данных напрямую в телефонную сеть нельзя. Для его подключения используют специальное устройство — модем (МОдулятор — ДЕМОдулятор — см. рис. 3.3, б), который преобразует цифровой сигнал в аналоговый в надлежащем диапазоне частот, и наоборот, аналоговый в цифровой.

Рассмотрим основные принципы такого преобразования.

Как уже отмечалось, аналоговая модуляция заключается в управляемом изменении одного или нескольких основных параметров несущего сигнала: амплитуды, частоты и фазы. Существует три основных метода модуляции, обеспечивающих преобразование цифровых данных в аналоговую форму (рис. 3.6):

- амплитудная модуляция;
- частотная модуляция;
- фазовая модуляция.

Во всех этих методах спектр гармоник получаемого сигнала сконцентрирован в области частоты несущего сигнала.

При *амплитудной модуляции* двоичные 0 и 1 представляют аналоговым сигналом с несущей частотой, но с разной амплитудой. Обычно нулю здесь соответствует сигнал с нулевой амплитудой. Таким образом, при амплитудной модуляции сигнал  $s(t)$  (см. рис. 3.2) имеет следующий вид:

$$s(t) = \begin{cases} A \cos(2\pi f_c t) & \text{двоичная 1;} \\ 0 & \text{двоичный 0,} \end{cases}$$

где  $A \cos(2\pi f_c t)$  — несущий сигнал с амплитудой  $A$ .

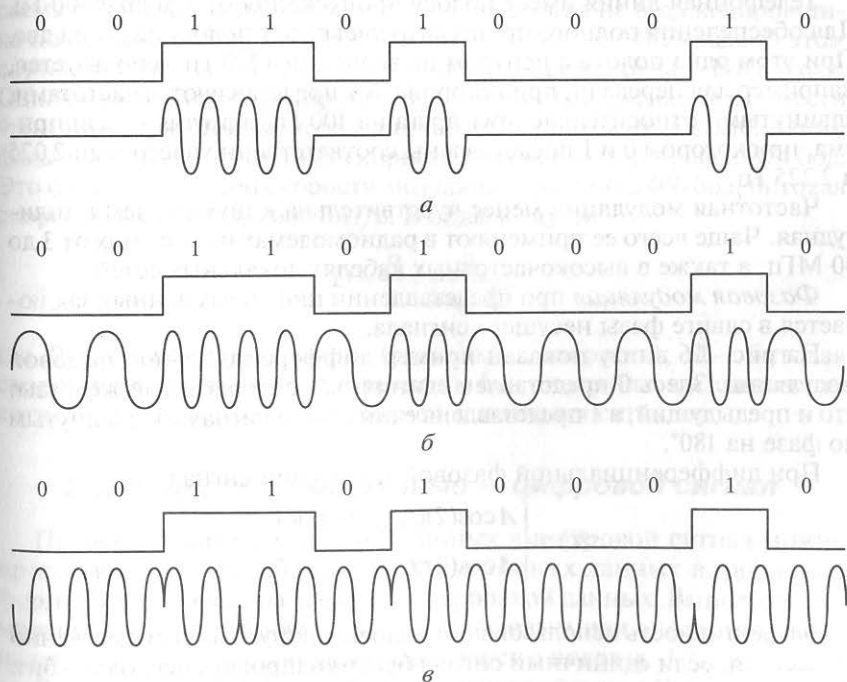


Рис. 3.6. Основные методы модуляции:

$a$  — амплитудная;  $b$  — частотная;  $v$  — фазовая

Метод амплитудной модуляции не очень эффективен по сравнению с другими методами, так как он очень чувствителен к шумам. Чаще всего этот метод используется в сочетании с другими видами модуляции. В чистом виде он применяется в телефонных линиях на скоростях передачи до 1 200 бит/с, а также для передачи сигналов по оптоволоконным каналам.

При *частотной модуляции* двоичные 0 и 1 представляют сигналами разной частоты, сдвинутой, как правило, по отношению к частоте несущей на одинаковое значение, но в противоположном направлении:

$$s(t) = \begin{cases} A \cos(2\pi f_1 t) & \text{для } 1; \\ A \cos(2\pi f_2 t) & \text{для } 0, \end{cases}$$

где  $f_1 - \Delta = f_2 + \Delta = f_c$ ;  $\Delta$  — сдвиг по частоте.

Частотную модуляцию можно использовать для организации дуплексной связи. Напомним, что дуплексной называется связь, при которой данные можно передавать по каналу одновременно в оба направления.

Телефонная линия имеет полосу пропускания от 300 до 3 400 Гц. Для обеспечения полного процесса дуплекса эту полосу делят на две. При этом одна полоса с центром на значении 1 170 Гц используется, например для передачи, при которой 0 и 1 представляются частотами, сдвинутыми относительно друг друга на 100 Гц, а другая — для приема, при котором 0 и 1 представлены соответственно частотами 2 025 и 2 225 Гц.

Частотная модуляция менее чувствительна к шумам, чем амплитудная. Чаще всего ее применяют в радиомодемах на частотах от 3 до 30 МГц, а также в высокочастотных кабелях локальных сетей.

*Фазовая модуляция* при представлении цифровых данных заключается в сдвиге фазы несущего сигнала.

На рис. 3.6 внизу показан пример дифференциальной фазовой модуляции. Здесь 0 представлен единичным сигналом той же фазы, что и предыдущий, а 1 представлена единичным сигналом, сдвинутым по фазе на  $180^\circ$ .

При дифференциальной фазовой модуляции сигнал

$$s(t) = \begin{cases} A \cos(2\pi f_c t + \pi) & \text{для } 1; \\ A \cos(2\pi f_c t) & \text{для } 0. \end{cases}$$

Эффективность использования полосы пропускания существенно повысится, если единичный сигнал будет кодировать несколько бит. Например, сдвигая фазу единичного сигнала на  $90^\circ$ , можно предложить метод кодирования цифровых данных, известный как квадратичная фазовая модуляция. В этом случае сигнал

$$s(t) = \begin{cases} A \cos\left(2\pi f_c t + \frac{\pi}{4}\right) & \text{для 11;} \\ A \cos\left(2\pi f_c t + \frac{3\pi}{4}\right) & \text{для 10;} \\ A \cos\left(2\pi f_c t + \frac{5\pi}{4}\right) & \text{для 00;} \\ A \cos\left(2\pi f_c t + \frac{7\pi}{4}\right) & \text{для 01.} \end{cases}$$

Эту схему можно усовершенствовать для передачи сразу трех битов, используя восемь фазовых углов. Мы еще вернемся (см. подразд. 5.2.3) к использованию этого метода модуляции, когда будем рассматривать применение модема для передачи данных в телефонных сетях, где используется 12 фазовых углов, четыре из которых имеют по две амплитуды.

Приведенный пример хорошо иллюстрирует различие битовой скорости  $R$ , бит/с, и скорости модуляции  $D$ , бод. Предположим, что схема с 12 фазовыми углами применяется, когда на вход кодировщика подаются данные, закодированные с помощью NRZ-кода. В этом случае битовая скорость  $R = 1/t_b$ , где  $t_b$  — длина бита в NRZ-коде. Однако на выходе закодированный единичный сигнал будет нести 4 бита информации, используя при этом 16 различных комбинаций фазы и амплитуды, поэтому скорость модуляции будет равна  $R/4$  бод. Это означает, что при скорости модуляции, равной 2 400 бод, битовая скорость составляет 9 600 бит/с. В общем случае

$$D = \frac{R}{b} = \frac{R}{\log_2 L},$$

где  $D$  — скорость модуляции (сигнальная скорость);  $R$  — битовая скорость (скорость передачи данных);  $b$  — число битов в единичном сигнале;  $L$  — число разных уровней единичных сигналов.

### 3.2.4. Аналоговые данные — цифровой сигнал

Преобразование аналоговых данных в цифровой сигнал можно представить как преобразование аналоговых данных в цифровую форму. Этот процесс называется оцифровкой данных. Выполнив его, можно передать цифровые данные цифровым или аналоговым сигналом. Как это делается, рассматривалось в подразд. 3.2.2 и 3.2.3.

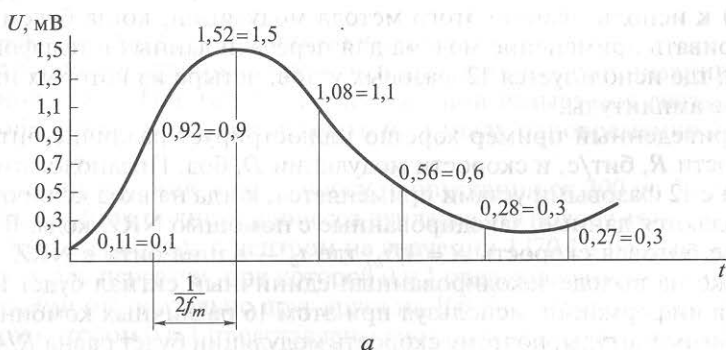
Для преобразования используют два устройства: АЦП (аналогово-цифровой преобразователь) и ЦАП (цифроаналоговый преобразователь). АЦП превращает аналоговые данные в цифровую форму, а ЦАП

выполняет обратную процедуру. Устройство, объединяющее в себе функции и АЦП, и ЦАП, называется кодеком (КОдер-ДЕКОдер).

Рассмотрим два основных метода преобразования аналогового сигнала в цифровую форму: импульсно-кодovou модуляцию и дельта-модуляцию.

### Импульсно-коддовая модуляция

Импульсно-коддовая модуляция (ИКМ) основывается на теореме Котельникова, которая утверждает, что если измерять параметры сигнала  $f(t)$  через регулярные интервалы времени с частотой не меньшей, чем удвоенная частота самой высокочастотной составляющей сигнала, то полученная серия измерений будет содержать всю инфор-



№ уровня	Двоичный эквивалент	ИКМ-сигнал
0	0000	—————
1	0001	—————
2	0010	—————
3	0011	—————
4	0100	—————
5	0101	—————
6	0110	—————
7	0111	—————
8	1000	—————
9	1001	—————
10	1010	—————
11	1011	—————
12	1100	—————
13	1101	—————
14	1110	—————
15	1111	—————

б

Рис. 3.7. Пример импульсно-коддовой модуляции:

а — вид исходного сигнала и его разбиение на уровни; б — вид ИКМ-сигнала

мацию об исходном сигнале и этот сигнал может быть восстановлен полностью.

Например, для линий передачи с полосой пропускания 4 000 Гц достаточно проводить замеры с частотой 8 000 Гц, чтобы полностью восстановить сигнал. Однако следует помнить, что это замеры амплитуды аналогового сигнала. Чтобы преобразовать результаты замеров в цифровой код, поступают следующим образом. Весь диапазон возможных амплитуд сигналов сначала разбивают, например на 16 уровней. Каждый уровень сопоставляется с двоичным кодом, соответствующим двоичному представлению номера этого уровня. В примере, изображенном на рис. 3.7, требуется четыре разряда для представления каждого замера.

Важно иметь в виду, что точное восстановление исходного сигнала невозможно, так как каждый из 16 уровней является лишь приближением реального значения амплитуды сигнала. Можно увеличить число уровней до 256, для чего потребуется восемь разрядов (при передаче голоса это будет сравнимо по качеству с аналоговой передачей). Однако заметим, что в этом случае придется передавать результаты более 8 000 замеров по восемь разрядов каждый в секунду, т. е. битовая скорость должна быть не ниже 64 Кбит/с.

На стороне приемника по полученному цифровому коду восстанавливают аналоговый сигнал. Однако, как уже отмечалась, вследствие «округления» точное восстановление сигнала невозможно. Такой эффект называется ошибкой квантования, или шумом квантования. Существуют методы понижения этого шума за счет использования нелинейных методов квантования.

### Дельта-модуляция

Альтернативой ИКМ является дельта-модуляция (рис. 3.8). В этом методе модуляции на исходную непрерывную функцию, представляющую собой аналоговый сигнал, накладывают ступенчатую функцию. Значения этой ступенчатой функции изменяются на каждом шаге квантования по времени  $T_s$  на значение шага  $\delta$ . Замена исходной функции на эту дискретную, ступенчатую функцию интересна тем, что поведение последней при этом носит двоичный характер. На каждом шаге значение ступенчатой функции либо увеличивается на шаг  $\delta$ , и этот случай представляет 1, либо уменьшается на шаг  $\delta$ , и этот случай представляет 0. Оцифрованный вид этой функции также показан на рис. 3.8. Мы вернемся еще к этому методу, когда будем рассматривать работу телефонной системы (см. подразд. 5.2).

Процесс передачи при использовании дельта-модуляции организуется следующим образом. В момент очередного замера текущее значение исходной функции сравнивается со значением ступенчатой функции на предыдущем шаге. Если значение исходной функции

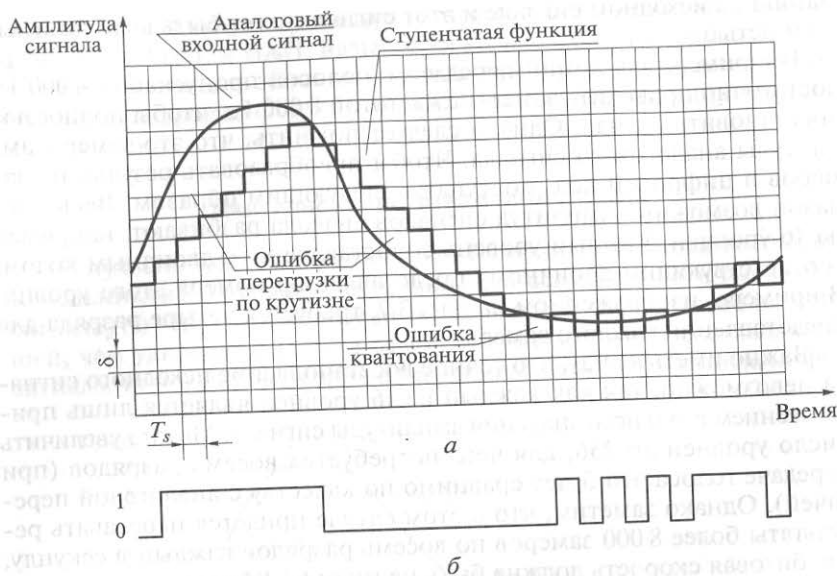


Рис. 3.8. Пример дельта-модуляции:  
*a* — кодируемые данные; *б* — результирующий сигнал

больше, то передается 1. В противном случае передается 0. Таким образом, ступенчатая функция всегда изменяет свое значение.

Метод дельта-модуляции характеризуется двумя параметрами: шагом  $\delta$  и частотой замеров, или шагом квантования,  $T_s$ . Выбор шага  $\delta$  — это установление баланса между ошибкой квантования и ошибкой перегрузки по крутизне характеристики (см. рис. 3.8). Когда исходный сигнал изменяется достаточно медленно, то возникает только ошибка квантования, и чем больше  $\delta$ , тем больше эта ошибка. Если же сигнал изменяется резко, то скорость роста ступенчатой функции может отставать. Ошибка этого вида, называемая ошибкой перегрузки по крутизне, растет с уменьшением  $\delta$ .

Эту ошибку можно снизить, увеличив частоту замеров, однако это увеличит битовую скорость на линии.

### 3.2.5. Аналоговые данные — аналоговый сигнал

Анализ этого вида преобразования начнем с того, что выясним, где может возникнуть потребность в нем. Аналоговая модуляция цифровых данных применяется там, где нет цифровых каналов. Цифровое кодирование аналоговых данных используется там, где есть

цифровые каналы. Когда же возникает потребность передавать аналоговые данные с помощью аналоговых сигналов?

Прежде всего, такая потребность возникает при использовании радиоканалов. Если передавать аудиоинформацию в голосовом диапазоне частот (300... 3000 Гц), то потребуется антенна очень большого размера. Дело в том, что размер антенны и  $\lambda$  — длина волны прямо пропорциональны. Из соотношения  $\lambda f = c$ , где  $c$  — скорость света в вакууме, ясно что при использовании низкочастотных сигналов необходимый размер антенны может достигать нескольких километров. Модуляция, т.е. объединение исходного сигнала  $m(t)$  и несущей частоты  $f_c$ , позволяет соответственно изменять параметры исходного сигнала и тем самым упростить решение ряда технических проблем. Кроме того, модуляция позволяет использовать методы мультиплексирования, или уплотнения (см. подразд. 5.2.5). Использование для передачи электромагнитных волн рассмотрено в подразд. 3.3.

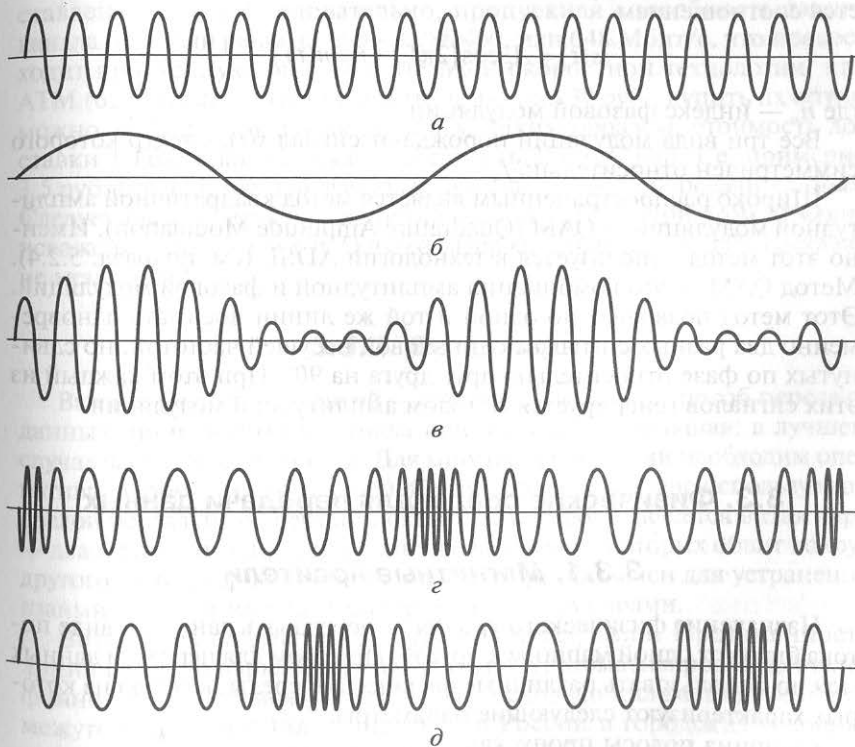


Рис. 3.9. Иллюстрация трех способов передачи аналоговых данных в аналоговой форме:

*a* — несущий сигнал; *б* — модулирующий синусоидальный сигнал; *в*... *д* — соответственно амплитудная, фазовая и частотная модуляции при передаче аналоговых данных

Три способа модуляции для передачи аналоговых данных в аналоговой форме (амплитудная, частотная и фазовая) показаны на рис. 3.9.

При амплитудной модуляции форма результирующего сигнала определяется формулой

$$s(t) = [1 + n_a x(t)] \cos 2\pi f_c t,$$

где  $n_a$  — индекс модуляции, который определяется как отношение амплитуды исходного сигнала к амплитуде несущего сигнала;  $f_c$  — частота несущей.

Форма результирующего сигнала при частотной модуляции определяется следующим выражением:

$$s(t) = A_c \cos(2\pi f_c t + n_f m(t)),$$

где  $n_f$  — индекс частотной модуляции;  $m(t) = 1 + n_a x(t)$ .

Сигнал, получаемый с помощью фазовой модуляции, определяется соотношением

$$s(t) = A_c \cos(2\pi f_c t + n_p m(t)),$$

где  $n_p$  — индекс фазовой модуляции.

Все три вида модуляции порождают сигнал  $s(t)$ , спектр которого симметричен относительно  $f_c$ .

Широко распространенным является метод квадратичной амплитудной модуляции — QAM (Quadrature Amplitude Modulation). Именно этот метод используется в технологии ADSL (см. подразд. 5.2.4). Метод QAM — это комбинация амплитудной и фазовой модуляций. Этот метод позволяет по одной и той же линии посылать одновременно два разных сигнала с одинаковой несущей частотой, но сдвинутых по фазе относительно друг друга на  $90^\circ$ . При этом каждый из этих сигналов генерируется методом амплитудной модуляции.

### 3.3. Физические среды для передачи данных

#### 3.3.1. Магнитные носители

Назначение физического уровня — передавать данные в виде потока битов от одной машины к другой. При этом для передачи данных можно использовать различные физические среды, каждую из которых характеризуют следующие параметры:

- ширина полосы пропускания;
- пропускная способность;
- задержка сигнала;
- стоимость;
- сложность прокладки;

- сложность обслуживания.

Кроме перечисленных, физическую среду характеризуют и другие параметры, например:

- достоверность передачи;
- затухание;
- помехоустойчивость.

Магнитная лента или магнитный диск в сочетании с обычным транспортным средством (автомобином, железной дорогой и т. п.) могут быть прекрасной физической средой для передачи данных. Это так, особенно в случае, если высокая пропускная способность и низкая стоимость передачи в расчете на один бит являются ключевыми факторами.

Например, обычная видеолента формата VHS может хранить до 7 Гбайт данных. В коробке размером 50 × 50 × 50 см может поместиться до 1 000 таких лент, т. е. 7 000 Гбайт данных, или 7 Тбайт (терабайт). В любой город на территории России эта коробка может быть доставлена за 24 ч. Следовательно, пропускная способность такого канала передачи равна  $(7\,000 \times 8) / 86\,400$ , или 648 Мбит/с, что превосходит пропускную способность такой скоростной технологии, как АТМ (622 Мбит/с.). Цена кассеты примерно 30 руб., купить их оптом можно за 25 руб., включая доставку. Таким образом, стоимость доставки 1 Гбайт данных будет составлять 25 000 / 7 000, т. е. примерно 3,5 руб. Вряд ли мы найдем более дешевый способ передачи данных. Следует также учесть надежность такой передачи. При этом никаких искажений, ошибок и т. п. Однако задержка сигнала в канале составит не менее 24 ч!

### **3.3.2. Витая пара**

Вагон с магнитной лентой — это очень дешевый способ передачи данных, но и задержка сигнала при этом очень большая: в лучшем случае часы, а обычно сутки. Для многих приложений необходим оперативный обмен информацией. Самой старой и все еще используемой средой передачи со времени появления телефона является витая пара — два медных изолированных провода, один из которых обвит вокруг другого. Этот второй вьющийся провод предназначен для устранения взаимного влияния между соседними витыми парами.

Витая пара широко используется в телефонии. Протяженность линии из витой пары между абонентами и автоматизированной телефонной станцией может составлять несколько километров без промежуточного усиления. Например, в России в городских условиях средняя длина абонентской линии около 3,5 км.

Витая пара может быть использована для передачи как цифровых, так и аналоговых сигналов. Ее пропускная способность зависит от толщины используемых проводов и длины линии. Скорость в несколько мегабит в секунду вполне достижима с помощью соответ-

Характеристики затухания сигнала для разных видов витой пары

Частота, МГц	Затухание на каждые 100 м, дБ		
	Пара категории 3	Пара категории 5	Экранированная пара ( $R = 150 \text{ Ом}$ )
1	2,6	2,0	1,1
4	5,6	4,1	2,2
16	13,1	8,2	4,4
25	—	10,4	6,2
100	—	22,0	12,3
300	—	—	21,4

ствующих методов передачи. На коротких расстояниях (до сотни метров) может достигаться скорость до 1 Гбит/с, на больших расстояниях (несколько километров) скорость передачи не превышает 4 Мбит/с. Сказанное, а также низкая стоимость обуславливают использование витой пары при создании ЛВС и скорее всего эта тенденция сохранится.

Витые пары объединяются в многопарные кабели. Кабель категории 3 содержит четыре витые пары с невысокой плотностью навивки и имеет ширину полосы пропускания до 16 МГц. Наиболее часто используются кабели категории 5, который тоже состоит из четырех пар, но имеет более плотную навивку, что позволяет достигать более высоких скоростей передачи и ширину полосы пропускания 100 МГц.

В табл. 3.1 приведены характеристики затухания сигнала для витых пар категорий 3 и 5, а также для экранированной витой пары.

### 3.3.3. Коаксиальные кабели

Как и у витой пары, у коаксиального кабеля есть два проводника. Однако устроены они иначе, что позволяет существенно увеличить ширину полосы пропускания. Центральный проводник представляет собой толстый медный провод, окруженный изолятором. Эта конструкция помещается внутри второго цилиндрического проводника, который обычно представляет собой плетеную плотную металлическую сетку. Все это закрывается плотным защитным слоем пластика. Обычно толщина коаксиального кабеля составляет от 1 до 2,5 см, поэтому монтировать и прокладывать его сложнее, чем витую пару. Однако у такого кабеля шире полоса пропускания и характеристики по затуханию сигнала (рис. 3.10) лучше, чем у витой пары. Из рис. 3.10 видно, что коаксиальные кабели работают на частотах от 1 до 500 МГц, поэтому их применяют на больших расстояниях и по ним

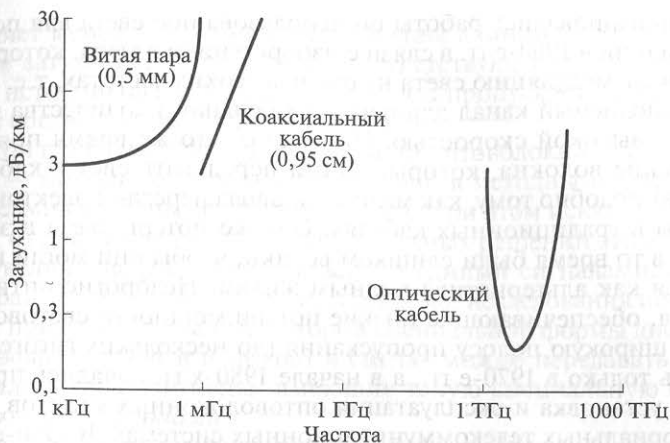


Рис. 3.10. Характеристики затухания сигнала для разных видов кабелей

могут передаваться одновременно несколько потоков данных от разных компьютеров.

Коаксиальные кабели находят самое широкое применение, например:

- передача телевизионных сигналов, включая системы кабельного телевидения;
- передача нескольких телефонных разговоров одновременно на большие расстояния между телефонными станциями, построение ЛВС;
- подключение компьютерных периферийных устройств на небольших расстояниях.

Коаксиальные кабели используют для передачи как аналоговых, так и цифровых сигналов. Из рис. 3.10 видно, что коаксиальные кабели превосходят по своим характеристикам витую пару. У них шире полоса пропускания, а следовательно, выше скорость передачи данных. Основными ограничителями скорости и расстояния при передаче без усиления в этих кабелях являются затухание сигнала, тепловой и интермодуляционный шум. Когда всю полосу пропускания кабеля разбивают на более узкие полосы и каждую такую полосу используют как отдельный канал, на границах таких каналов возникает интермодуляционный шум.

### 3.3.4. Оптоволокно

Попытки применения света в качестве носителя информации предпринимались очень давно. Еще в 1880 г. Александр Белл запатентовал устройство, которое передавало речь на расстояние до 200 м с помощью зеркала, вибрирующего синхронно со звуковыми волнами и модулирующего отраженный свет.

Активизировались работы по использованию света для передачи информации в 1960-е гг. в связи с изобретением лазера, который мог обеспечить модуляцию света на очень высоких частотах, т. е. создать широкополосный канал для передачи большого количества информации с высокой скоростью. Примерно в то же время появились оптические волокна, которые могли передавать свет в кабельных системах подобно тому, как медные провода передают электрические сигналы в традиционных кабелях. Однако потери света в этих волокнах в то время были слишком велики, чтобы они могли использоваться как альтернатива медным жилам. Недорогие оптические волокна, обеспечивающие низкие потери мощности светового сигнала и широкую полосу пропускания (до нескольких гигагерц) появились только в 1970-е гг., а в начале 1980-х гг. начались промышленная установка и эксплуатация оптоволоконных каналов связи в территориальных телекоммуникационных системах. В 1980-е гг. начались также работы по созданию стандартных технологий и устройств для использования оптоволоконных каналов в локальных сетях.

Для создания оптической связи требуется источник света с постоянной длиной волны, светопроводящая среда и детектор, преобразующий световой поток в электрический. На одном конце оптоволоконной линии имеется передатчик — источник света, световой импульс от которого проходит по светопроводящему волокну и попадает на детектор, расположенный на другом конце этой линии и преобразующий этот импульс в электрический.

Одна из основных проблем при создании оптоволоконных систем состояла в том, чтобы не дать световому пучку рассеяться через боковую поверхность силиконового шнура. Количество рассеиваемой энергии зависит от угла падения светового луча на стенки шнура. При углах больше некоторого критического угла, называемого углом полного внутреннего отражения, вся энергия луча отражается обратно внутрь.

Оказалось, что силиконовый шнур, имеющий толщину, близкую к длине волны источника света, работает как провод для тока, т. е. без потерь на внутреннее отражение. По такому *одномодовому* шнуру можно передавать данные со скоростью несколько гигабит в секунду на сотню километров без промежуточного усиления.

Поскольку можно испускать несколько лучей разной длины волны так, чтобы они попадали на границы шнура под углом больше, чем угол полного внутреннего отражения, следовательно, по одному шнуру можно пускать несколько лучей. При этом каждый луч, как говорят, имеет свою моду. Так получается *многомодовый* шнур.

Оптоволоконно изготавливают из стеклоподобного материала. Затухание оптического сигнала в стекле зависит от длины волны источника света. На практике для передачи сигнала используются три полосы для волн длиной 0,85, 1,30 и 1,55 мкм. Волны длиной 1,30 и 1,55 мкм обладают тем замечательным свойством, что их затухание

составляет менее 5 % на километр. Волны длиной 0,85 мкм имеют большее затухание, но они лучше соответствуют возможностям лазерных источников света. Ширина полосы пропускания во всех трех случаях составляет от 25 000 до 30 000 ГГц.

Другой проблемой при использовании оптоволокна является дисперсия — потеря по мере распространения исходными световыми импульсами начальных форм и размеров. При этом искажения также зависят от длины волны. Одно из возможных решений этой проблемы — увеличение расстояния между соседними сигналами. Однако это сокращает скорость передачи. К счастью, исследования показали, что при придании сигналу некоторой специальной формы дисперсионные эффекты почти исчезают и сигнал можно передавать на тысячи километров. Сигналы, имеющие такую специальную форму, называются *силитонами*.

Оптоволоконный кабель имеет сердечник, состоящий из сверхпрозрачного оптоволокна и изоляционного покрытия. В одномодовом кабеле толщина сердечника составляет 8...10 мкм, а в многомодовом — 50...100 мкм. Сердечник имеет оптическое покрытие из стекловолокна с низким коэффициентом рефракции, сокращающего потери света через его границы, и защитное покрытие из пластика.

Такой кабель прокладывают и под землей, где он нередко становится жертвой экскаваторов и другой землеройной техники, и под водой, где он становится добычей тралов и акул. Соединяют его с помощью специальных коннекторов, механически прижимая один край к другому, либо сваркой. При этом в точке соединения теряется от 5 до 20 % мощности сигнала.

Для передачи используются два вида источников света: светодиод (LED) и полупроводниковый лазер, которые обладают разными свойствами (табл. 3.2). С помощью специальных интерферометров эти источники света можно настроить на требуемую длину волны. На принимающем конце устанавливается фотодиод, время срабатывания которого 1 нс, что ограничивает максимальную скорость передачи значением 1 Гбит/с.

С помощью оптоволокна можно строить как локальные сети, так и сети большего масштаба. При этом подключение к оптоволоконной линии более сложное, чем к Ethernet-линии. Чтобы понять, как решается проблема построения сети из оптоволокна, необходимо осознать, что сеть типа кольца представляет собой цепочку соединений типа точка — точка (рис. 3.11).

Соединения типа точка — точка могут быть двух видов: пассивные и активные. В пассивном соединении имеются светодиод или лазер и фотодиод. Приняв сигнал через фотодиод, это соединение передает электрический сигнал на компьютер или транслирует его дальше с помощью светодиода или лазера. Это абсолютно надежное соединение. Выход из строя любого из компонентов не нарушает связи по кольцу, а лишь блокирует работу отдельного компьютера.

Сравнение свойств светодиода и полупроводникового лазера

Свойство	Светодиод	Полупроводниковый лазер
Скорость передачи	Низкая	Высокая
Дальность передачи	Низкая	Высокая
Модовость	Мультимодовый	Мультимодовый или одномодовый
Срок службы	Короткий	Долгий
Чувствительность к температурным контрастам	Низкая	Значительная
Стоимость	Низкая	Высокая

Активное подключение (см. справа на рис. 3.11) содержит промежуточный усилитель электрического сигнала. Фотодиод преобразует оптический сигнал в электрический, который усиливается и передается компьютеру либо транслируется дальше с помощью лазера или светодиода.

Подробно организация сетей на основе оптоволоконна по стандарту FDDI (Fiber Distributed Data Interface) будет рассмотрена в гл. 5.

В заключение сравним возможности медного кабеля и оптоволоконна.

1. Ширина полосы пропускания у оптоволоконна несравнимо больше, чем у медного кабеля, что позволяет достигать скоростей передачи в сотни гигабит в секунду на расстояниях в десятки километров. Напомним, что коаксиальный кабель обеспечивает скорость передачи максимум в несколько сотен мегабит в секунду примерно на 1 км, а витая пара — несколько мегабит в секунду на 1 км и до 1 Гбит/с на расстоянии до 100 м.

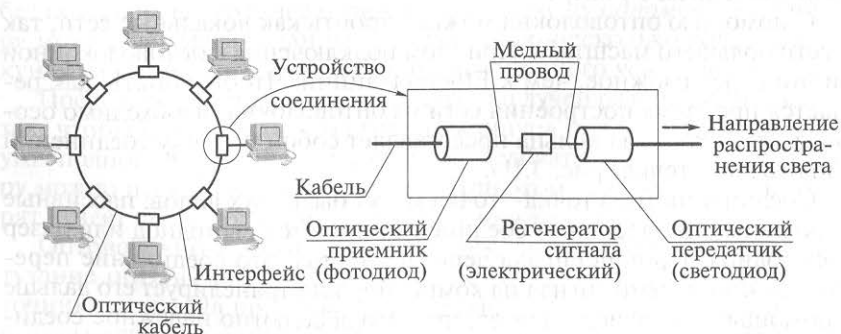


Рис. 3.11. Схема оптоволоконного кольца

**Основные характеристики витой пары, коаксиального кабеля  
и оптоволоконна**

Носитель информации	Диапазон частот	Стандартное затухание, дБ/км	Стандартная задержка, мс/км	Расстояние между репитерами, км
Витая пара	0...3,5 кГц	0,2 дБ (при частоте 1 кГц)	50	2
Многопарный кабель	0...1 МГц	3 дБ/км (при частоте 1 кГц)	5	2
Коаксиальный кабель	0...500 МГц	7 дБ/км	5	1...9
Оптический кабель	180...370 ТГц	0,2...0,5	5	40

2. Оптоволоконно компактнее и имеет меньшую массу. При одинаковой пропускной способности коаксиальный кабель и кабель из витых пар существенно тяжелее оптоволоконна. Это существенный фактор, определяющий стоимость и требования к опорным конструкциям. Например, 1 км 1000-парника имеет массу 8 т, а оптоволоконно с такой же пропускной способностью — 100 кг.

3. Затухание сигнала в оптоволоконне существенно меньше, чем в коаксиальном кабеле и витой паре, и остается постоянным для широкого диапазона частот.

4. Оптоволоконно не восприимчиво к внешним электромагнитным излучениям. Следовательно, ему не страшны интерференция, импульсные шумы и взаимные наводки. Оптоволоконно не излучает энергию, поэтому не влияет на работу другого оборудования. Его трудно обнаружить, а следовательно, трудно найти и повредить.

5. Чем меньше используется репитеров, тем дешевле система передачи и меньше источников ошибок. С этой позиции оптоволоконные системы достигли большего совершенства. Среднее расстояние между репитерами у них в разы больше, чем у коаксиального кабеля и витой пары.

В табл. 3.3 для сравнения приведены основные характеристики витой пары, коаксиального кабеля и оптоволоконна.

### **3.3.5. Физический уровень в сетях IEEE 802.3**

В качестве примера использования для передачи различных физических сред рассмотрим физический уровень стандарта IEEE 802.3

(Ethernet и его производные), который наиболее широко используется на сегодняшний день при построении локальных вычислительных сетей.

Стандарт IEEE 802.3 имеет очень интересную историю. Начало его созданию положила система ALOHA (см. подразд. 4.3). Потом компания XEROX построила канал на 2,94 Мбит/с, объединивший 100 персональных компьютеров на 1 км кабеля. Эта система была названа Ethernet (сетевой эфир) по аналогии с люминофорным эфиром, который был той средой, которая согласно представлениям XVIII в. передавала свет.

Система Ethernet фирмы Хероx имела такой большой успех, что компании Хероx, DEC и Intel, объединив свои усилия, создали систему Ethernet с пропускной способностью 10 Мбит/с. Эта разработка и составила основу стандарта IEEE 802.3.

### Кабели в стандарте IEEE 802.3

Всего по стандарту IEEE 802.3 допускается использование четырех типов кабелей (табл. 3.4).

Исторически первым появился так называемый толстый Ethernet (10Base5). Это коаксиальный кабель желтого цвета с отметками через каждые 2,5 м, указывающими, где можно производить подключение. Подключение выполняется через специальные розетки, которые монтируются прямо на кабеле. В эти розетки встраивался специальный прибор — трансивер, отвечающий за обнаружение несущей частоты и коллизий. (Подробнее протокол IEEE 802.3 и коллизии рассмотрены в гл. 4.) Когда трансивер обнаруживает коллизию, т. е. когда сразу несколько станций пытаются вести передачу, он посылает специальный сигнал по кабелю, гарантирующий, что другие трансиверы услышат эту коллизию. Обозначение 10Base5 говорит о том, что кабель обеспечивает пропускную способность 10 Мбит/с, а максимальная длина его сегмента равна 500 м.

Исторически вторым появился тонкий Ethernet (10Base2). Это более простой в употреблении коаксиальный кабель с простым подключением через BNC-коннектор, представляющий собой T-образное соединение коаксиальных кабелей. Тонкий Ethernet дешевле, однако его сегмент не должен превышать 200 м и он не должен объединять более 30 машин.

Решение проблемы поиска обрыва, частичного повреждения кабеля или плохого контакта в коннекторе привели к созданию совершенно иной кабельной конфигурации на основе витой пары. В этом случае каждая машина соединяется витой парой со специальным устройством — хабом (hub). Такой способ подключения обозначается 10Base-T.

Рассмотренные способы подключения показаны на рис. 3.12. При этом следует отметить, что первые два способа в настоящее время прак-

Наиболее распространенные средства передачи данных стандарта IEEE 802

Обозначение кабеля	Тип кабеля	Максимальная длина сегмента, м	Число узлов на сегмент	Преимущества
10Base5	Толстый коаксиальный кабель	500	100	Может использоваться для магистралей
10Base2	Тонкий коаксиальный кабель	200	30	Самый дешевый
10Base-T	Витая пара	100	1024	Проста в обслуживании
10Base-F	Оптоволокно	2 000	1024	Идеально для соединения зданий

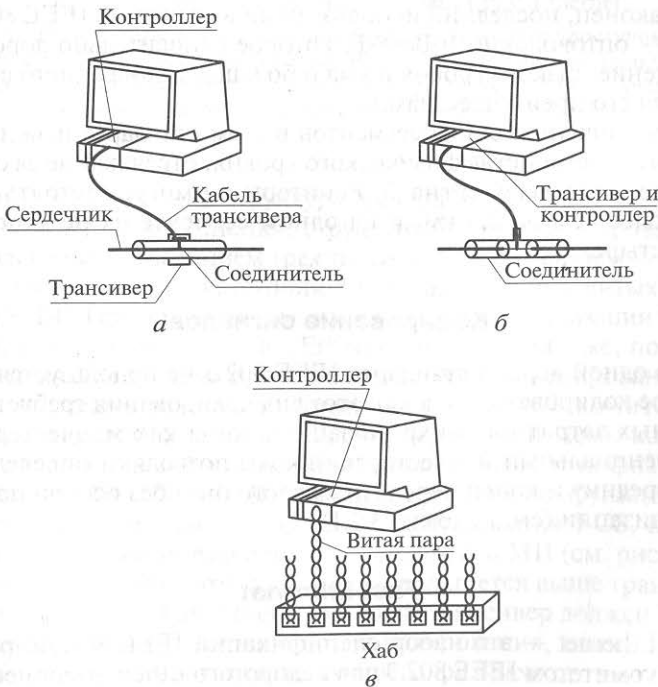


Рис. 3.12. Способы подключения по стандарту IEEE 802:

*а* — 10Base5; *б* — 10Base2; *в* — 10Base-T

тически не используются. Как уже было сказано, в 10Base5 (рис. 3.12, а) трансивер размещается прямо на кабеле и соединяется с компьютером трансиверным кабелем, длина которого не может превышать 50 м. Трансиверный кабель состоит из пяти витых пар. Две из них используются для передачи данных к компьютеру и от компьютера, две служат для передачи управляющей информации в обе стороны, а пятая — для подачи питания на трансивер. Некоторые трансиверы обеспечивают возможность подключать до восьми машин.

Трансиверный кабель подключается к контроллеру в компьютере через интерфейс AUI. В контроллере имеется специальная микросхема, отвечающая за прием кадров и их отправку, проверку и формирование контрольной суммы. В некоторых случаях эта микросхема отвечает и за управление буферами на канальном уровне, очередью буферов на отправку и обеспечивает прямой доступ к памяти машины, а также решает другие вопросы доступа к сети.

В 10Base2 трансивер располагается на контроллере, и каждая машина должна иметь свой индивидуальный трансивер (рис. 3.12, б).

В 10Base-T трансивера нет вовсе (рис. 3.12, в). Машина соединяется с хабом витой парой, длина которой не должна превышать 100 м. Вся электроника сосредоточена в хабе.

И, наконец, последний используемый в стандарте IEEE 802.3 тип кабеля — оптоволокно 10Base-F, которое относительно дорогое, но обеспечение низкого уровня шума и большая длина одного сегмента являются его преимуществами.

Для увеличения длины сегментов в этом стандарте используются репитеры — устройства физического уровня, отвечающие за очистку, усиление и передачу сигнала. Репитеры не могут отстоять друг от друга более чем на 2,5 км, и на одном сегменте их не может быть более четырех.

## Кодирование сигналов

Ни в одной версии стандарта IEEE 802.3 не используется потенциальное кодирование, так как этот вид кодирования требует дополнительных затрат на синхронизацию, тогда как манчестерский и дифференциальный манчестерский коды позволяют определять начало, середину и конец передачи каждого бита без особой побитной синхронизации (см. подразд. 3.2.1).

## Fast Ethernet

Fast Ethernet — это набор спецификаций IEEE 802.3u, разработанных комитетом IEEE 802.3 для недорогого Ethernet-совместимого стандарта, способного обеспечить работу СПД в ЛВС со скоростью 100 Мбит/с. Большая часть изменений в стандарте IEEE 802.3 при переходе к Fast Ethernet касается физического уровня.

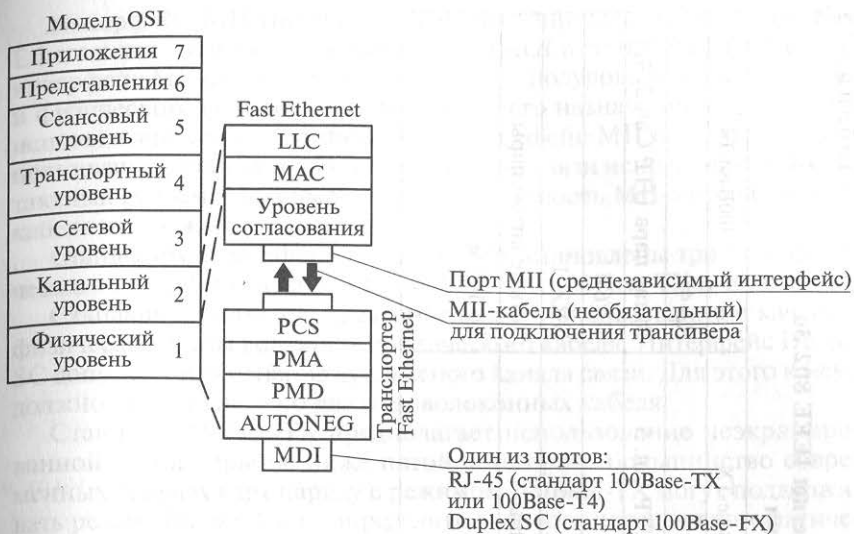


Рис. 3.13. Структура уровней стандарта Fast Ethernet:

LLC — управление логическим каналом; MAC — управление доступом к среде; PCS — уровень физического кодирования; PMA — уровень физического подключения; PMD — уровень, зависящий от физической среды; AUTONEG — уровень автоопределения; MDI — интерфейс, зависящий от среды

На рис. 3.13 показана структура уровней стандарта Fast Ethernet. Более сложная, чем в Ethernet, структура физического уровня здесь обусловлена использованием трех типов кабельных систем — оптоволокна), двух витых пар категории 5 (TX) или четырех витых пар категории 3 (T4). Причем по сравнению с вариантами реализации Ethernet отличия каждого варианта Fast Ethernet от других глубже, поскольку здесь изменяется и число проводников, и методы кодирования.

Еще на стадии разработки стандарта 100Base-T комитет IEEE 802.3u определил, что не существует универсальной схемы кодирования сигнала, которая была бы идеальной для всех трех физических интерфейсов (TX, FX, T4). В стандарте Fast Ethernet функция кодирования располагается на подуровне кодирования PCS, который находится ниже среднезависимого интерфейса МII (см. рис. 3.13), в то время как в Ethernet этот уровень располагается выше трансивера. В результате этого в Fast Ethernet каждый трансивер должен использовать свой собственный набор схем кодирования, наилучшим образом подходящий для соответствующего физического интерфейса, например для интерфейса 100Base-FX набор для кодирования по схеме 4В/5В (которую рассмотрим далее) и набор схем для кодирования NRZ-1.

**Физические интерфейсы стандарта Fast Ethernet IEEE 802.3u  
и их основные характеристики**

Физический интерфейс	100Base-FX	100Base-TX	100Base-T4
Порт устройства	Duplex SC	RJ-45	RJ-45
Среда передачи	Оптическое волокно	Витая пара UTP Cat. 5	Витая пара UTP Cat. 3, 4, 5
Сигнальная схема	4B/5B	4B/5B	8B/6T
Битовое кодирование	NRZ-1	MLT-3	NRZ-1
Число витых пар (волокон)	Два волокна	Две витые пары	Четыре витые пары
Протяженность сегмента	До 412 м (mm)*; до 2 км (mm); до 100 км (sm)*	До 100 м	До 100 м

Здесь mm — многомодовое волокно; sm — одномодовое волокно.

\* Достигаются только при дуплексном режиме связи.

Интерфейс МП (medium independent interface) в стандарте Fast Ethernet является аналогом интерфейса АUI в стандарте Ethernet, т. е. интерфейс МП обеспечивает связь между подуровнями согласования и физического кодирования. Основное его назначение — упростить использование разных типов сред. Интерфейс МП предполагает использование трансивера Fast Ethernet. Для связи используется 40-контактный разъем. Максимальная протяженность МП-интерфейсного кабеля не должна превышать 0,5 м.

Стандартом Fast Ethernet IEEE 802.3u установлены три типа физического интерфейса (табл. 3.5): 100Base-FX, 100Base-TX и 100Base-T4.

Стандарт 100Base-FX предусматривает использование в качестве физической среды волоконно-оптического кабеля. Интерфейс Duplex SC допускает применение дуплексного канала связи. Для этого к нему должно быть подведено два оптоволоконных кабеля.

Стандарт 100Base-TX предполагает использование неэкранированной витой пары не ниже пятой категории. Большинство современных сетевых карт наряду с режимом 100Base-TX могут поддерживать режим 10Base-T или определять скорость передачи автоматически. Кроме того, они могут работать в дуплексном режиме.

В версии Ethernet на 10 Мбит/с используют манчестерское кодирование для представления данных при передаче по кабелю. Метод кодирования 4В/5В каждые четыре бита данных (называемых символами) представляет пятью битами. Применение избыточного бита позволяет использовать потенциальные схемы кодирования данных. Как уже отмечалось, потенциальные коды обладают по сравнению с манчестерскими кодами более узкой полосой спектра сигнала, а следовательно, в них предъявляются меньшие требования к полосе пропускания кабеля. Однако прямое использование потенциальных кодов для передачи исходных данных без избыточного бита невозможно из-за плохой самосинхронизации приемника и источника данных: при передаче длинной последовательности единиц или нулей в течение долгого времени сигнал не изменяется, и приемник не может определить момент считывания очередного бита.

При использовании пяти бит для кодирования шестнадцати 4-битовых комбинаций строится такая таблица кодирования, в которой любой исходный 4-битовый код представляется 5-битовым кодом с чередующимися нулями и единицами. Таким образом обеспечивается синхронизация приемника с передатчиком. Так как исходные биты MAC-подуровня должны передаваться со скоростью 100 Мбит/с, то наличие одного избыточного бита вынуждает передавать биты результирующего кода 4В/5В со скоростью 125 Мбит/с. Поскольку для кодирования передаваемых данных из 32 возможных 5-битовых комбинаций требуется только 16, то остальные 16 комбинаций в коде 4В/5В используются в служебных целях.

Интерфейс 100Base-T4 позволяет обеспечить полудуплексный канал связи с использованием витой пары UTP категории 3 и выше.

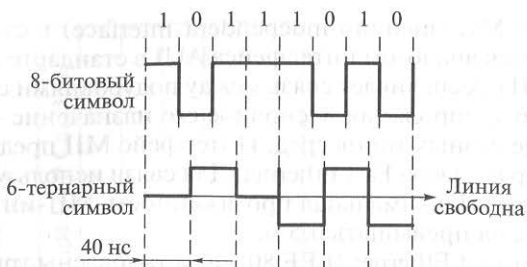


Рис. 3.14. Пример использования кода 8В/6Т

Именно возможность перехода со стандарта Ethernet на стандарт Fast Ethernet без радикальной замены существующей кабельной системы на основе UTP категории 3 следует считать главным преимуществом этого стандарта.

В табл. 3.5 указано, что для интерфейса 100Base-4T используется сигнальная схема 8В/6Т, суть работы которой состоит в следующем. Если бы для четырех витых пар категории 3 и выше использовалось манчестерское кодирование, то битовая скорость в расчете на одну витую пару была бы 33,33 Мбит/с (собственно для передачи можно использовать только три из четырех витых пар), что превышало бы установленный предел 30 МГц для таких кабелей. Эффективное уменьшение частоты модуляции достигается, если вместо прямого (2-уровневого) бинарного кода используется 3-уровневый (ternary) код. Этот код, известный как 8В/6Т, предполагает, что прежде чем происходит передача, каждый набор из 8 бит (символ) сначала преобразуется в соответствии с определенными правилами в шести тернарных (3-уровневых) символов.

Пример, приведенный на рис. 3.14, иллюстрирует определение скорости передачи трехуровневого символьного сигнала, значение которой не превышает предел, установленный для таких сред:  $(100 \times 6/8)/3 = 25$  МГц.

Интерфейс 100Base-T4 имеет один существенный недостаток: в нем принципиально невозможна поддержка дуплексного режима передачи. Поэтому данный интерфейс не получил столь большого распространения, как 100Base-TX и 100Base-FX.

В Fast Ethernet применяются такие же, как и в Ethernet, основные устройства: трансиверы, конвертеры, сетевые карты (для установки на рабочие станции-серверы), повторители, коммутаторы.

## Gigabit Ethernet

Интерес к технологиям для локальных сетей с гигабитными скоростями определяется двумя обстоятельствами: успехом развития

сравнительно недорогих (по сравнению с волоконно-оптическими) технологий Fast Ethernet и слишком большими трудностями прохождения технологии ATM к конечному пользователю (см. гл. 5).

В марте 1996 г. комитет IEEE 802.3 одобрил проект стандартизации Gigabit Ethernet 802.3z, и 11 ведущих производителей средств вычислительной техники создали альянс по развитию этого стандарта. Альянс, объединивший усилия большого числа ведущих производителей сетевого оборудования в целях выработки единого стандарта и выпуска совместимых продуктов Gigabit Ethernet, решал следующие задачи:

- поддержка расширения технологий Ethernet и Fast Ethernet, обеспечивающие более высокие скорости передачи;
- разработка технических предложений для включения в стандарт;
- выработка процедур и методов тестирования продуктов, поступающих от различных поставщиков.

К началу 1998 г. альянс объединял уже более 100 компаний. Через него обеспечивалась обратная связь между техническим комитетом по стандартизации IEEE 802.3 и индустриальными производителями сетевого оборудования, что увеличило эффективность работы комитета и способствовало более быстрому одобрению спецификаций стандартов Gigabit Ethernet IEEE 802.3z и IEEE 802.3ab. Наибольшие трудности вызывал физический уровень, а именно, адаптация много-

#### Модель OSI

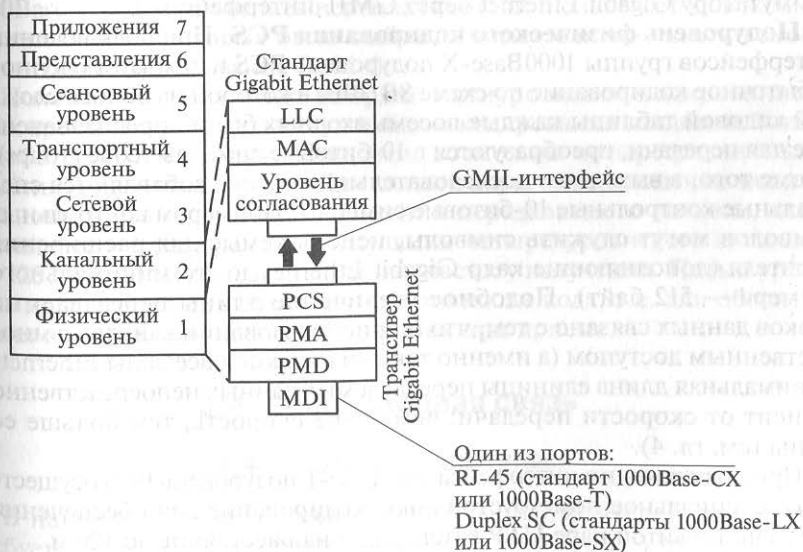


Рис. 3.15. Структура уровней стандарта Gigabit Ethernet

модового оптического волокна и витой пары. Стандарт IEEE 802.3z был принят 29 июня 1998 г., т. е. с задержкой примерно на полгода от первоначально запланированного графика.

На рис. 3.15 показана структура уровней стандарта Gigabit Ethernet. Как и в стандарте Fast Ethernet, в Gigabit Ethernet не существует универсальной схемы кодирования сигнала, которая была бы идеальной для всех физических интерфейсов: для стандартов 1000Base-LX/SX/CX используется сигнальная схема 8В/10В, а для стандарта 1000Base-T — специальный расширенный линейный код TX/T2. Функцию кодирования выполняет подуровень кодирования PCS, размещенный, как и в Fast Ethernet, ниже среднезависимого интерфейса GMII.

**GMII-интерфейс.** Среднезависимый интерфейс GMII (gigabit media independent interface) обеспечивает взаимодействие между уровнем MAC (см. гл. 4) и физическим уровнем. GMII-интерфейс является расширением интерфейса MII и может поддерживать скорости передачи 10, 100 и 1 000 Мбит/с. Также, имея отдельные 8-битовые приемник и передатчик, он может поддерживать полудуплексный и дуплексный режимы. Кроме того, GMII-интерфейс несет один сигнал, обеспечивающий синхронизацию (clock signal), и два сигнала состояния линии: один из них (в состоянии ON) указывает наличие несущей, а второй (в состоянии ON) — говорит об отсутствии коллизий. Также GMII-интерфейс обеспечивает еще несколько сигнальных каналов и питание. Его трансиверный модуль, охватывающий физический уровень и обеспечивающий один из физических средозависимых интерфейсов, может подключаться, например к коммутатору Gigabit Ethernet через GMII-интерфейс.

**Подуровень физического кодирования PCS.** При подключении интерфейсов группы 1000Base-X подуровень PCS использует блочное избыточное кодирование по схеме 8В/10В, в которой на основе сложной кодовой таблицы каждые восемь входных битов, предназначенные для передачи, преобразуются в 10-битовые символы (code groups). Кроме того, в выходном последовательном потоке добавляются специальные контрольные 10-битовые символы. Примером контрольных символов могут служить символы, используемые для расширения носителя (дополняющие кадр Gigabit Ethernet до его минимального размера — 512 байт). Подобное увеличение длины передаваемых блоков данных связано с тем, что при использовании каналов с множественным доступом (а именно такими являются все виды Ethernet) минимальная длина единицы передаваемых данных непосредственно зависит от скорости передачи: чем выше скорость, тем больше ее длина (см. гл. 4).

При подключении интерфейса 1000Base-T подуровень PCS осуществляет специальное помехоустойчивое кодирование для обеспечения передачи по витой паре UTP категории 5 на расстояние до 100 м.

На физическом уровне Gigabit Ethernet используется несколько интерфейсов, включая традиционную витую пару категории 5, а так-

же многомодовое и одномодовое оптическое волокно. Всего, как уже говорилось, определены четыре различных типа физических интерфейсов среды, которые определены в спецификациях стандартов 802.3z (1000Base-X) и 802.3ab (1000Base-T).

Интерфейс 1000Base-X основан на стандарте физического уровня Fibre Channel, который мы рассматривать не будем. Отметим только, что Fibre Channel — это СПД, обеспечивающая высокоскоростной обмен большими объемами данных для рабочих станций, суперкомпьютеров, устройств хранения и периферийных устройств. Fibre Channel имеет четырехуровневую архитектуру, два нижних уровня которой FC-0 (интерфейсы и среда) и FC-1 (кодирование-декодирование) перенесены в Gigabit Ethernet. Поскольку Fibre Channel является одобренной технологией, то такое перенесение сильно сократило время на разработку оригинального стандарта Gigabit Ethernet.

Интерфейс 1000Base-T является стандартным интерфейсом стандарта Gigabit Ethernet, служащим для передачи данных по неэкранированной витой паре категории 5 и выше на расстоянии до 100 м. Для такой передачи используются все четыре пары медного кабеля, при этом скорость передачи по одной паре кабеля составляет 250 Мбит/с. Данный стандарт обеспечивает дуплексную передачу данных, причем по каждой паре сразу в двух направлениях (двойной дуплекс).

Технически реализовать дуплексную передачу со скоростью 1 Гбит/с по витой паре УТР категории 5 оказалось значительно сложнее, чем в стандарте 100Base-TX. Для использования в стандарте 1000Base-T рассматривались первоначально несколько методов кодирования, среди которых было выбрано пятиуровневое импульсно-амплитудное кодирование PAM-5.

Поясним, почему было выбрано пятиуровневое кодирование. В распространенном четырехуровневом кодировании входящие биты обрабатываются парами. При этом возможны четыре различные комбинации — 00, 01, 10, 11. Для каждой пары бит передатчик может установить свой уровень напряжения передаваемого сигнала, что уменьшает в 2 раза частоту модуляции четырехуровневого сигнала (со 125 до 250 МГц), а следовательно, частоту излучения. Пятый уровень добавляется для создания избыточности кода, т.е. для обеспечения возможности коррекции ошибок при приеме.

### **3.4. Беспроводная связь**

#### **3.4.1. Общие сведения**

В наше время существуют категории пользователей, которым требуется постоянно находиться на связи, получать электронную почту, иметь доступ к данным и т.п. Как уже отмечалось во введении, сегодня управление сложными техническими объектами осуществля-

ется посредством распределенных вычислительных комплексов, часть вычислительных ресурсов которых располагается на самом объекте, а часть вне его. При этом управляемый объект не всегда имеет наземное базирование и может быть мобильным. В таких случаях витая пара, коаксиальный кабель и оптоволокно не могут обеспечить передачу данных между компонентами управляющего вычислительного комплекса.

Тенденции в области приложений, которые также отмечались во введении, позволяют утверждать, что будущее за беспроводными соединениями и оптоволокном. Все мобильные средства коммуникации и обработки информации будут беспроводными.

Беспроводная связь востребована не только для мобильных вычислительных средств, но и там, где прокладка любого кабеля затруднительна либо невозможна (горы, старые здания), либо если требуется быстрое создание коммуникации. Это особенно актуально для нашей страны, где почти 2/3 территории приходится на зону вечной мерзлоты и горы.

### 3.4.2. Электромагнитный спектр

Напомним, что в вакууме электромагнитная волна распространяется со скоростью света ( $c = 3 \cdot 10^8$  м/с). В медном проводнике эта скорость составляет 2/3 от скорости в вакууме. Обозначим  $f$  — частоту,  $\lambda$  — длину волны. Фундаментальное соотношение между  $f$ ,  $c$  и  $\lambda$  имеет вид

$$f\lambda = c. \quad (3.2)$$

Поскольку скорость света — это константа, зная  $f$ , мы знаем  $\lambda$ , и наоборот. Например, волны при частоте в 1 МГц согласно соотношению (3.2) имеют длину 300 м, а волны длиной 1 см имеют частоту 30 ГГц. Напомним, что длина волны определяет размер и геометрию антенны. Длина антенны как у приемника, так и у передатчика, и длина излучаемой-принимаемой ею волны связаны определенными соотношениями.

При определенных условиях, которые будут рассмотрены далее, волны распространяются в строго определенном направлении. В этом случае антенна приемника должна быть должным образом ориентирована в пространстве по отношению к антенне передатчика, чтобы принимать сигналы. При других условиях антенна передатчика распространяет электромагнитные волны во всех направлениях.

Для передачи информации из всего спектра частот, представленных на рис. 3.16, используют только следующие диапазоны: радиодиапазон, микроволновый, инфракрасный, видимый и частично ультрафиолетовый. Диапазоны рентгеновского излучения, гамма-

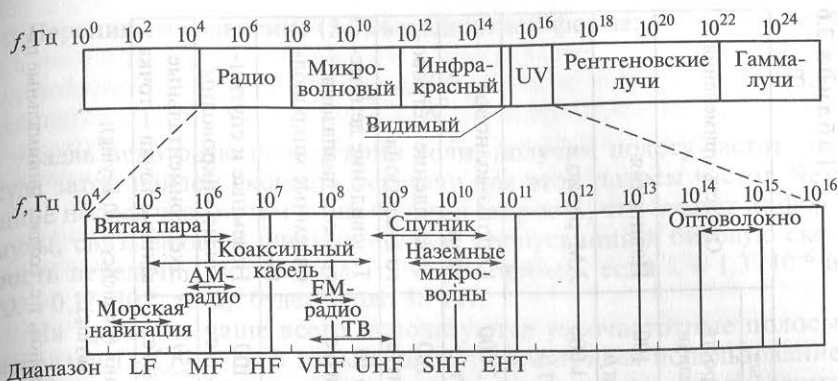


Рис. 3.16. Использование электромагнитного спектра для передачи данных

излучения и большая часть ультрафиолетового, включающие в себя большие частоты, а следовательно, предпочтительные для передачи, требуют, однако, использования сложной аппаратуры для генерации и модуляции, сигналы в них плохо преодолевают препятствия и, что самое главное, они опасны для живой материи.

В нижней части рис. 3.16 диапазоны, используемые для передачи информации, перечислены в соответствии с их официальными названиями МСЭ (ITU): LF-диапазон, т.е. диапазон длинных волн содержит волны длиной от 1 до 10 км (примерно от 30 до 300 кГц). Аббревиатуры LF, MF, HF, соответствующие отечественным аббревиатурам ДВ, СВ, КВ (т.е. длинные волны, средние и короткие), появились, когда еще никто и не думал об использовании частот больше 10 МГц. Позднее появились аббревиатуры VHF, UHF (очень высокие, ультравысокие частоты) и т.д.

Количество данных, передаваемых электромагнитной волной, определяется ее шириной, т.е. спектром частот гармоник, составляющих эту волну. При определенных условиях на низких частотах можно закодировать несколько бит данных на 1 Гц, но на высоких частотах это число можно довести до 40 бит. Следовательно, по кабелю с полосой пропускания 500 МГц можно передавать данные со скоростью несколько гигабит в секунду. Учитывая широкую полосу пропускания оптоволоконного кабеля, становится ясно, почему оптоволоконно столь привлекательно для сетей ЭВМ.

В табл. 3.6 представлены характеристики различных частотных диапазонов.

Решив уравнение (3.2) относительно  $f$  и продифференцировав по  $\lambda$ , получим выражение

$$\frac{df}{d\lambda} = -\frac{c}{\lambda^2}. \quad (3.3)$$

Характеристики частотных диапазонов

Диапазон частот	Название диапазона	Аналоговые данные		Цифровые данные		Область применения
		Модуляция	Полоса пропускания	Модуляция	Скорость передачи	
30 ... 300 кГц	LF (low frequency — низкие частоты)	Обычно не используется		ASK, FSK, MSK	0,1 ... 100 бит/с	Навигация
300 ... 3 000 кГц	MF (medium frequency — средние частоты)	AM	До 4 кГц	ASK, FSK, MSK	10 ... 1 000 бит/с	АМ-радио
3 ... 30 МГц	HF (high frequency — высокие частоты)	AM, SSB	До 4 кГц	ASK, FSK, MSK	10 ... 3 000 бит/с	Коротковолновое радио
30 ... 300 МГц	VHF (very high frequency — очень высокие частоты)	AM, SSB, FM	5 кГц... 5 МГц	FSK, PSK	До 100 кбит/с	Телевидение метрового диапазона
300 ... 3 000 МГц	UHF (ultrahigh frequency — ультравысокие частоты)	FM, SSB	До 20 МГц	PSK	До 10 Мбит/с	Телевидение десятиметрового диапазона, наземные микроволны
3 ... 30 ГГц	SHF (superhigh frequency — сверхвысокие частоты)	FM	До 500 МГц	PSK	До 100 Мбит/с	Наземные и спутниковые микроволны
30 ... 300 ГГц	EHF (superhigh frequency — супервысокие частоты)	FM	До 1 ГГц	PSK	До 750 Мбит/с	Экспериментальные каналы точка — точка

Здесь ASK — амплитудно-фазовая модуляция (amplitude shift keying); FSK — частотная модуляция (frequency shift keying); PSK — фазовая модуляция (phase shift keying); MSK — минимальная модуляция (minimum shift keying).

\* Этот вид модуляции характеризуется минимальными излучениями на границах частотных диапазонов, т. е. создает минимальные помехи в смежных частотных полосах.

Перепишем уравнение (3.3) в разностной форме:

$$\Delta f = \frac{c\Delta\lambda}{\lambda^2}. \quad (3.4)$$

Задав некоторую полосу длин волн, получим полосу частот, откуда затем найдем скорость передачи для этой полосы частот. Чем шире полоса частот, тем выше битовая скорость, что следует из формулы, связывающей ширину полосы пропускания и битовую скорость передачи (см. подразд. 3.1.4). Например, если  $\lambda = 1,3 \cdot 10^{-6}$  и  $\Delta\lambda = 0,17 \cdot 10^{-6}$ , то  $\Delta f$  будет около 30 ТГц.

На практике чаще всего используются узкополосные полосы передачи ( $\Delta f/f \ll 1$ ). В дальнейшем, рассматривая использование приведенных частей электромагнитного спектра, будем предполагать именно узкополосную передачу.

При широкополосной передаче, используемой в основном военными и спецслужбами, частота несущей волны изменяется по определенному закону в диапазоне полосы. Перехватить такую передачу можно только в случае, если известен закон изменения частоты несущей.

### 3.4.3. Радиопередача

Радиоволны распространяются на большие расстояния, легко преодолевая преграды. Техника их генерации и приема хорошо изучена, имеется множество соответствующих специалистов, поэтому радиоволны широко используются для связи как вне, так и внутри помещений. Поскольку радиоволны распространяются во всех направлениях, то принимающая и передающая антенны не требуют дополнительной настройки и регулирования взаимного расположения.

Свойства радиоволн зависят от их частоты. На низких частотах, т.е. длинных волнах, они прекрасно преодолевают препятствия, но мощность сигнала падает пропорционально  $1/r^3$ , где  $r$  — расстояние до источника. На высоких частотах радиоволны распространяются по прямой, но хуже преодолевают препятствия. Для некоторых частот помехой становится даже дождь.

На любых частотах радиоволны чувствительны к помехам от электрических устройств. В силу перечисленных причин лицензирование, т.е. право использования частот в радиодиапазоне, находится под жестким контролем государства.

Как известно, длинные и средние волны могут огибать поверхность Земли и распространяться на большие расстояния. Короткие волны хотя и поглощаются земной поверхностью, но за счет отражения от ионосферы также могут распространяться на большие расстояния.

### 3.4.4. Микроволновая передача

Частоты свыше 10 МГц (см. рис. 3.16) представляют собой область микроволнового диапазона. Волны в этом диапазоне распространяются в строго определенном направлении и могут быть сфокусированы с помощью параболической антенны, имеющей вид телевизионной тарелки. Однако приемная и передающая антенны при этом должны быть тщательно ориентированы в пространстве по отношению друг к другу. Такая направленность позволяет, построив цепочку ретрансляторов, передавать сигнал на большие расстояния.

До появления оптоволоконна радиорелейная связь составляла основу телефонных систем на больших расстояниях, где с определенным интервалом устанавливались башни с ретрансляторами. Высота этих башен зависела от расстояния и мощности передатчика. Обычно 100-метровой башни хватает для передачи сигнала на расстояние в 80 км.

Микроволны не проходят сквозь здания так же хорошо, как низкочастотные волны. Кроме того, из-за рефракции в нижних слоях атмосферы они могут отклоняться от прямого направления. При этом увеличивается задержка сигнала и нарушается передача. Помимо того передача на этих частотах зависит и от погоды: при повышении влажности (дождь, туман и т.п.) ширина полосы пропускания резко сужается, растет шум, сигнал рассеивается. Обычно операторы держат определенный частотный резерв (около 10 % каналов) на случай подобных нарушений и при необходимости переключаются на резервные частоты, чтобы обойти зону осадков.

Стремление увеличить пропускную способность канала заставляет использовать все более и более высокие частоты. Сегодня использование частоты 10 ГГц — обычное дело. Однако здесь возникает серьезная проблема: начиная с частоты 8 ГГц, волны поглощаются водой и, в частности, дождем. Единственный выход из положения в этом случае — изменить маршрут передачи и обойти область дождя.

В настоящее время микроволновый диапазон широко используется в телефонии, сотовой телефонии, телевидении и других приложениях. Одно из главных достоинств микроволнового диапазона — не требуется прокладка никакой линии. Достаточно получить права на небольшие площадки земли (в сотню квадратных метров) для установки башен-ретрансляторов через каждые 50 км. Такая технология особенно оправдана в условиях гор и других труднопроходимых участков местности, где прокладка кабеля затруднена, а также в городе, где земля дорогая, а коммуникации прокладывать очень сложно.

Несколько частотных полос в диапазоне 2 400... 2 484 ГГц, например инфракрасные волны, можно использовать свободно без специального разрешения. В этих диапазонах работают микроволновые печи, радиотелефоны, радиоуправляемые двери и т.д. Эти частоты

также используются для сетевых целей на небольших расстояниях. Однако в разных странах могут использоваться и другие дополнительные диапазоны, например в США помимо указанного диапазона используются диапазоны 902...928 МГц и 5 725...5 850 ГГц.

### **3.4.5. Инфракрасные и миллиметровые волны**

Инфракрасное излучение и излучение в миллиметровом диапазоне используются на небольших расстояниях в блоках дистанционного управления. Основной недостаток таких излучений — они не проходят через преграды. Например, для инфракрасного излучения лист бумаги — непреодолимое препятствие.

Однако этот недостаток одновременно является и преимуществом, поскольку такое излучение в одной комнате не интерферирует с подобным излучением в другой комнате. На использование этих частот не надо также получать разрешение, т.е. это прекрасный канал для передачи данных внутри помещений на небольших расстояниях.

### **3.4.6. Видимое излучение**

Видимый диапазон также используется для передачи сигналов. Обычно источником света в этом случае является лазер. Монохромное когерентное излучение легко фокусируется. Однако смог, загрязнение атмосферы, дождь или туман портят дело. Передачу такого излучения способны нарушить даже конвекционные потоки воздуха на крыше, возникающие в жаркий день, которые вызывают дрожание луча вокруг приемника, ухудшая качество передачи.

### **3.4.7. Стандарт беспроводных локальных сетей IEEE 802.11**

Рассмотрим один из активно развивающихся стандартов беспроводной связи для локальных сетей, так называемый стандарт WiFi (Wireless Fidelity). Как и для кабельных сетей, стандартизацией беспроводных протоколов в настоящее время занимается в основном организация IEEE (см. подразд. 2.6.7). Семейство стандартов, определяющих функционирование беспроводных локальных сетей, описаны в секции 11 семейства стандартов IEEE 802.

Первой и ключевой технологией стандарта 802.11 является технология расширения спектра передачи методом прямой последовательности (Direct Sequence Spread Spectrum — DSSS). Использование DSSS позволяет беспроводным интерфейсам передавать данные со скоростью от 1 до 2 Мбит/с.

Идея этого метода состоит в следующем. Пусть имеется широкий канал, т.е. канал с широкой полосой пропускания. Разобьем его на

полосы. Каждому значению бита сопоставим определенный код с длиной, равной числу полос, на которые разбили канал. Теперь будем передавать каждый бит, параллельно передавая его код, причем каждый элемент кода в своей полосе. Элементы кода называются *чипами*. Такой способ передачи позволяет эффективнее использовать полосу пропускания канала, и он более надежен по сравнению с традиционным способом передачи.

Рассмотрим пример. Пусть бинарную единицу представляет набор чипов вида 00110011011, а бинарный 0 — набор чипов вида 11001100100. Обратим внимание, что если эти последовательности рассматривать как векторы и взять их скалярное произведение, то получим 0, т. е. можно сказать, что эти последовательности ортогональны друг другу.

Далее все чипы одного набора передают в эфир параллельно.

Пусть вследствие искажений получена последовательность вида 01111011011. Сравнив ее с эталонными последовательностями, видим следующее: отличие от эталона бинарной единицы составляет 2 бита, а отличие от эталона бинарного нуля — 9 бит. Значит, перед нами единица. Это так называемый код с исправлением ошибок. (Подробно построение таких кодов рассматривается в подразд. 4.1).

Метод кодирования сигнала при передаче отдельного чипа в полосу может быть разным. Например, BPSK (Binary Phase Shift Keying) — кодирование бинарным фазовым сдвигом. Сдвиг фаз здесь может иметь два значения — 0 и  $\pi$ . Скорость передачи данных таким способом составляет в разрешенных диапазонах (шириной в 22 МГц) 1 Мбит/с.

Для получения скорости передачи 2 Мбит/с используется метод QPSK (Quadrature Phase Shift Keying) — кодирование квадратурно-фазовым сдвигом. Сдвиг фаз здесь может иметь четыре значения 0,  $\pi/2$ ,  $\pi$ ,  $3\pi/2$ . Соответственно скорость этого метода в два раза выше, чем при использовании метода BPSK.

Для обеспечения скоростей передачи 5,5 и 11 Мбит/с используется метод CCK (Complimentary Code Keying) — кодирование комплиментарными кодами, смысл которого поясним на примере комплексных чисел. Пусть разрешено использовать только те комплексные числа, модуль которых принадлежит множеству  $\{1, -1, i, -i\}$ . Таких чисел восемь, т. е. можно сформировать восемь одинаковых по модулю, но не одинаковых по фазе комплексных чисел. При этом комплексная последовательность чипов может принимать следующие значения:  $1, -1, i, -i, 1+i, 1-i, -1-i, -1+i$ , а каждый элемент 8-чиповой последовательности может иметь восемь значений фазы. Тогда число вариантов составит 8 в степени 8. Конечно, не все значения в этом случае будут комплиментарны, но истинно комплиментарных значений хватит для того, что бы передавать сразу до восьми бит.

Если продолжать бездумно двигаться по этому пути, можно еще больше увеличить скорость передачи, но здесь начинает сказываться

эффект интерференции множества сигналов с разными амплитудами и разным временем прибытия к приемнику. Этот эффект, который может вызывать даже отражение части сигнала от потолков, стен и прочих поверхностей, получил название MultiPath Distortion — искажения, вызванные множественностью путей прохождения сигнала.

Для борьбы с этим эффектом, а также для обеспечения возможности увеличения скорости передачи данных был разработан метод OFDM (Orthogonal Frequency Division Multiplexing) — мультиплексирование с ортогональным частотным разделением каналов. Его идея заключается в том, что сигнал поляризуют в ортогональной по отношению к соседним полосам плоскости. Кроме того, между передаваемыми символами вставляется охранный интервал длительностью 0,8 мкс. Для ликвидации взаимного влияния соседей по частотному диапазону по его краям имеются также защитные подканалы.

Кодирование сигнала осуществляется с помощью описанных ранее методов, а также с помощью технологии QAM (Quadrature Amplitude Modulation) — квадратурно-амплитудной модуляции. Этот метод подразумевает кодирование сигнала не только за счет изменения фазы, но и за счет изменения амплитуды сигнала, что позволяет использовать 16 или даже 64 состояния этого сигнала. При этом скорости передачи увеличиваются следующим образом: 24, 36, 48 и 54 Мбит/с.

Разброс скоростей при передаче данных по беспроводным сетям Wi-Fi довольно велик: от 1 до 54 Мбит/с. При этом возникает вполне закономерный вопрос, зачем вообще нужны «медленные» скорости и почему нельзя использовать только самую «быструю» скорость 54 Мбит/с?

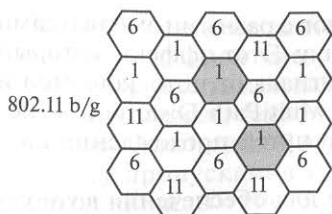
Представим себе преподавателя, который старается сообщить студентам, сидящим в аудитории, как можно больше информации. Для этого он старается говорить как можно быстрее. На первых рядах аудитории его речь вполне разборчива, однако на задних рядах слышна лишь какая-то скороговорка, которую понять невозможно, и студенты вынуждены засыпать. Чтобы речь успешно распространялась как можно дальше, необходимо говорить медленно разборчиво

Таблица 3.7

### Варианты стандарта IEEE 802.11

Модификации стандарта	Частота, ГГц	Максимальная скорость передачи, Мбит/с
802.11b	2,4	11
802.11a	5	54
802.11g	2,4	54
802.11n	2,4...5,0	600 (разрабатывается)

Рис. 3.17. Конфликт частотных диапазонов



и громко. (Попробуйте говорить быстро и громко.) В нашем случае передача данных беспроводного соединения возможна со скоростью 2 Мбит/с на расстояние 40 км. Со скоростью 54 Мбит/с такая передача без ретрансляторов невозможна.

В табл. 3.7 перечислены в порядке появления на рынке стандарты, используемые в настоящее время.

Оборудование, работающее по разным стандартам, но на одинаковых частотах, как правило, обратно совместимо друг с другом. Так, например, имея сетевую карту стандарта 802.11b, можно подключиться к точке доступа стандарта 802.11g.

Указанные в табл. 3.7 частоты несколько условны. Дело в том, что частотная сетка во многих странах разбивается с шагом 5 МГц, т. е. 2,412 ГГц (1-й канал), 2,417 ГГц (2-й канал) и т. д. Для подобных сетей правительства некоторых стран выделяют часть радиодиапазона, указывая номера каналов. Например, в США доступны каналы с 1-го по 11-й, а в Европе — с 1-го по 13-й, что, однако, не означает, что при установке 11 или 13 беспроводных устройств они не будут мешать друг другу. Из ранее сказанного известно, что ширина канала в стандартах 802.11b и 802.11g составляет 22 МГц, откуда следует, что выбрав в качестве стартовой частоты 2,412 ГГц (1-й канал), мы также захватим и каналы со 2-го по 5-й. Таким образом, доступных частот остается всего три — это 1, 6 и 11-й каналы. Однако это не является трагедией, ведь беспроводные устройства можно разместить в шахматном порядке, но помнить об этом необходимо (рис. 3.17).

В стандарте 802.11a ширина канала составляет 20 МГц и имеется 12 неперекрывающихся частот, что существенно упрощает его внедрение. Следует также помнить, что частотная политика может отличаться в разных странах. Например, есть государства (Аргентина, Бразилия и др.), где стандарт 802.11a полностью запрещен.

## КАНАЛЬНЫЙ УРОВЕНЬ

### 4.1. Основы передачи данных на канальном уровне

#### 4.1.1. Сервис, предоставляемый сетевому уровню

Теперь, когда мы знаем, как биты могут трансформироваться в электромагнитные сигналы, передаваться через разные физические среды, а затем снова трансформироваться в биты, рассмотрим, как эти биты надо обрабатывать, чтобы передача данных между двумя соседними машинами была надежной и эффективной.

Под словами «соседние машины» будем понимать две машины, соединенные физической линией, например проводом. Будем предполагать, что для этой линии справедливо, что биты поступают получателю точно в той последовательности, в какой их послал отправитель. Эта простая, на первый взгляд, задача при детальном рассмотрении оказывается весьма сложной, если учесть, что при передаче по каналу могут возникать ошибки, задержки, вызывающие дублирование данных, и т. д.

На уровне канала данных решается ряд проблем, присущих только этому уровню: реализация сервиса для сетевого уровня; объединение битов, поступающих с физического уровня, в кадры; формирование кадра и передача его на физический уровень; обнаружение и исправление ошибок передачи, управление потоком кадров и др.

Основная задача канального уровня — обеспечить сервис сетевому уровню по передаче и приему данных. Назначением сервиса является передача данных от процесса на сетевом уровне одной машины процессу на сетевом уровне другой машины. Как это происходит показано на рис. 4.1, а. Фактический процесс передачи данных сложнее, чем показано на рис. 4.1, б. Однако для простоты изложения будем придерживаться этой схемы.

Существуют разные виды сервиса на канальном уровне:

- без уведомления и без соединения;
- с уведомлением и без соединения;
- с уведомлением и с соединением.

Сервис без уведомления и без соединения не предполагает установки соединения до начала передачи, которое после передачи необходимо разорвать, а также подтверждения специальным сообщением факта приема переданного кадра. Если в результате помех на

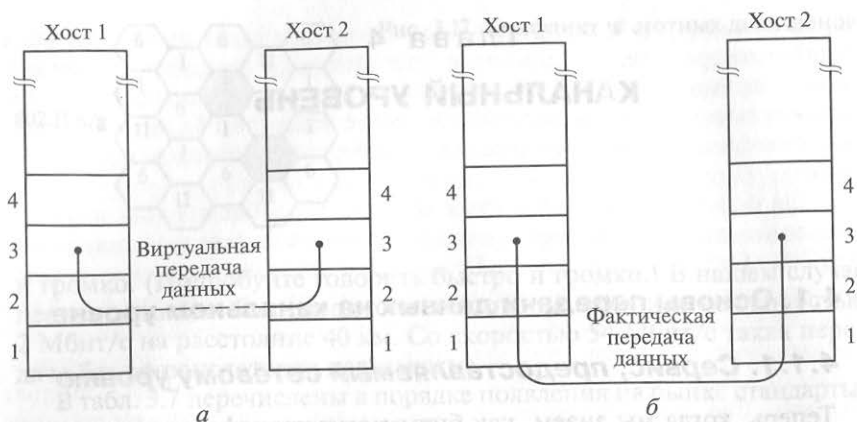


Рис. 4.1. Схемы виртуальной (а) и фактической (б) передач данных

физическом уровне кадр будет потерян, то на канальном уровне никаких попыток его восстановить не будет. Этот вид сервиса используется там, где физический уровень обеспечивает настолько высокую надежность при передаче, что потеря кадров происходит редко и восстановление при потере кадров можно переложить на верхние уровни. Также этот вид сервиса применяется при передаче данных в реальном времени там, где лучше потерять часть данных, чем увеличить задержку при их доставке. Например, передача речи, видеоизображения, управление техническими объектами. В большинстве ЛВС используется этот вид сервиса на канальном уровне.

Сервис с уведомлением без соединения предполагает подтверждение получения каждого посланного кадра. Если подтверждение не пришло в течение определенного промежутка времени, считается, что кадр не принят и должен быть послан снова. Этот вид сервиса используется в ненадежной физической среде передачи, например беспроводной. Можно было бы, конечно, подтверждать не кадры, а все сообщение целиком на сетевом уровне, однако это становится невыгодным при передаче больших сообщений. Например, если при передаче больших сообщений разрушится 10...20 % кадров, то повторная их передача займет больше времени, чем передача отдельных фрагментов. Поэтому подтверждение, выполняемое на канальном уровне, следует рассматривать как минимизацию затрат на передачу данных, а не необходимость.

Наиболее сложный вид сервиса на канальном уровне — это сервис с соединением и уведомлением, который предполагает, что до начала передачи между машинами устанавливается соединение и данные передаются по этому соединению. При этом каждый передаваемый кадр нумеруется, и канальный уровень гарантирует, что он будет обязательно получен, причем только один раз, а также что все кадры

будут получены в надлежащей последовательности. При сервисе без соединения этого гарантировать нельзя, поскольку потеря подтверждения получения кадра приведет к его повторной пересылке, что, в свою очередь, может привести к появлению нескольких идентичных кадров. Использование сервиса с соединением особенно полезно в том случае, когда канал формирует СПД. В СПД может быть достаточно сложная организация канала передачи, при которой коммутация потоков данных происходит самыми разными способами.

В гл. 5 рассматриваются различные типы сервиса в разных СПД, а также показывается, как за счет использования поля номера кадра переменной длины можно повысить эффективность применения канала для различных видов сервиса и оптимизировать затраты на поддержку соединения.

При использовании сервиса с соединением и уведомлением передача данных разбивается на три этапа. На первом этапе устанавливается соединение: на обеих машинах иницируются переменные и счетчики, отслеживающие то, с какими номерами кадры были приняты, а с какими нет. На втором этапе передаются требуемые кадры, а на третьем этапе соединение разрывается: переменные, счетчики, буферы и другие ресурсы, использованные для поддержки соединения, освобождаются.

#### **4.1.2. Разбиение на кадры**

Сервис, создаваемый канальным уровнем для сетевого уровня, опирается на сервис, создаваемый физическим уровнем. На физическом уровне принимаются и передаются потоки битов. Нельзя предполагать, что число отправленных битов должно быть равно числу принятых битов, а значение посланного бита также не обязательно должно быть равно значению принятого бита. Следовательно, на канальном уровне необходимы специальные действия для обнаружения и исправления таких ошибок.

Типовой подход к решению подобных проблем — это разбиение пакета сетевого уровня на кадры, подсчет контрольной суммы символов для каждого кадра и передача этой суммы вместе с кадром. При приеме контрольная сумма вычисляется для каждого кадра заново и сравнивается с той суммой, которая пришла с кадром. Различие этих сумм является признаком ошибки передачи. На канальном уровне необходимо принять меры по исправлению ошибки, например сбросить плохой кадр и послать сообщение об ошибке тому, кто прислал этот кадр.

Также на канальном уровне решается задача разбиения потока битов на кадры при приеме, например делая паузу между битами разных кадров. Однако в сети, где нет единого таймера, нет и гарантии, что эта пауза всегда будет одинаковой или, наоборот, что не появится новая пауза там, где ее не должно было быть.

Поскольку методы, использующие временные задержки, ненадежны, необходимо рассмотреть другие методы разбиения:

- использование счетчиков символов;
- вставка специальных стартовых и конечных символов;
- вставка стартовых и конечных битов;
- нарушение кодировки на физическом уровне.

Идея первого метода заключается в том, что в начале каждого кадра указывают, сколько символов в кадре. При приеме кадра подсчитывают число принятых символов. Если число полученных символов отличается от числа, указанного в начале кадра, то этот факт воспринимается как ошибка. Однако этот метод разбиения имеет существенный недостаток: счетчик символов может быть искажен при передаче и тогда принимающая сторона не сможет обнаружить границы кадра. Даже обнаружив несовпадение контрольных сумм, принимающая сторона не сможет сообщить передающей стороне, какой кадр следует переслать и сколько символов пропало, поэтому данный метод сейчас используется редко.

Следующий метод разбиения на кадры основан на вставке специальных символов. Обычно в этом случае для начала кадра используется последовательность символов DLE STX, а для конца кадра — DLE ETX.

DLE (Data Link Escape), STX (Start TeXt), ETX (End TeXt) — это специальные символы, имеющие специальную кодировку. При использовании этого метода, если даже была потеряна граница текущего кадра, требуется просто найти ближайший специальный символ DLE STX или DLE ETX. Однако здесь имеется одна опасность: при передаче чисел или программы в объектном коде такие последовательности могут уже содержаться в передаваемых данных. Для решения этой проблемы используют прием экранирования: каждая последовательность DLE STX просто дублируется в передаваемых данных. Следовательно, если при приеме получены две последовательности DLE, то одну из них удаляют.

Основным недостатком рассмотренного метода является его жесткая связь с размером байта и конкретным методом кодировки символов — ASCII, которая по мере развития сетей становилась все более и более обременительной. Кроме того, на стороне отправителя в этом случае необходимо просматривать кадр, чтобы обнаружить недопустимые байтовые последовательности.

Идея другого предложенного приема, позволяющего использовать любое число битов на символ и любую кодировку, состоит в том, что каждый кадр начинается и заканчивается специальной последовательностью битов (флагом) 01111110. Чтобы избежать появления аналогичной последовательности внутри кадра, поступают следующим образом. Посылающая сторона, встретив последовательность из пяти единиц, обязательно вставит нуль. Принимающая сторона, приняв последовательность из пяти единиц, обязательно удалит следующий

за ней нуль. Таким образом, если в передаваемых данных встретится конфигурация флага, то она будет преобразована в конфигурацию 01111010.

Кадр легко распознается по флагу, и если граница очередного кадра по какой-то причине была потеряна, то все что следует сделать — это «поймать» ближайший флаг.

Последний метод разбиения — нарушение кодировки — используется там, где применяется специальная кодировка битов на физическом уровне. Пусть для передачи одного бита используются два единичных сигнала, например как в манчестерском коде, где единица кодируется как переход высокое — низкое, а нуль — как переход низкое — высокое. Сочетания низкое — низкое или высокое — высокое не используются для передачи данных, поэтому их и применяют для обозначения границ кадра.

На практике для разбиения на кадры используют, как правило, комбинацию рассмотренных методов, например счетчик символов комбинируют с одним из перечисленных методов. Тогда если число символов в кадре совпадает с кодировкой его границы, кадр считается переданным правильно.

#### **4.1.3. Сохранение последовательности кадров**

Решив проблему разбиения на кадры, приходим к необходимости решения следующей проблемы: обеспечение попадания на сетевой уровень всех кадров в надлежащей последовательности. Для решения этой проблемы устанавливают обратную связь между отправителем и получателем в виде кадра подтверждения. Если кадр-подтверждение несет положительную информацию, то считается, что переданные кадры прошли нормально, если же в нем имеется сообщение об ошибке, то все или часть переданных кадров надо передавать заново.

Однако возможны ситуации, когда из-за ошибок в канале кадр может исчезнуть целиком. В этом случае получатель не будет никак реагировать, а отправитель может сколь угодно долго ждать подтверждения. Для решения этой проблемы на канальном уровне используются таймеры, т.е. сразу после передачи очередного кадра устанавливают таймер на определенное время, которого должно хватать на то, чтобы получатель получил кадр и отправил уведомление, а отправитель получил его. Заметим, что определить это время не так-то просто и его значение может изменяться в течение передачи.

При этом если отправитель не получит уведомление раньше, чем истечет время, установленное на таймере, то он будет считать, что кадр потерян и отправит его еще раз.

Однако если был утерян кадр-подтверждение, то вполне возможно, что один и тот же кадр получатель получит дважды. Для решения

этой проблемы каждому кадру присваивается порядковый номер, с помощью которого получатель может обнаружить дубли.

Итак, таймеры и нумерация кадров — это основные средства на канальном уровне, обеспечивающие доставку каждого кадра в единственном экземпляре и в требуемом порядке.

#### **4.1.4. Управление потоком**

Другая важная проблема, которую необходимо решать на канальном уровне, — управление потоком. Может случиться так, что отправитель будет посылать кадры столь часто, что получатель не будет успевать их обрабатывать. Это возможно, например, если машина-отправитель более мощная или загружена слабее, чем машина-получатель.

Для борьбы с такими ситуациями вводится специальный механизм управления потоком. Этот механизм предполагает наличие обратной связи между отправителем и получателем, которая позволит им регулировать темп передачи.

Существует много схем управления потоком, но все они в основе своей используют следующий сценарий. Прежде чем начать передачу отправитель спрашивает у получателя, сколько кадров тот может принять. Получатель сообщает ему эти данные. Отправитель после передачи указанного ему числа кадров должен приостановить передачу и запросить у получателя еще раз, сколько кадров тот может принять в этот раз, и т. д. Далее на примерах мы познакомимся с конкретными механизмами управления потоком.

#### **4.1.5. Обнаружение и исправление ошибок**

При рассмотрении физической среды отмечалось, что в беспроводных и аналоговых каналах достаточно высок уровень ошибок, т. е. ошибки при передаче на физическом уровне — это реальность, которую надо обязательно учитывать.

В разных средах характер ошибок разный. Ошибки могут быть одиночными, а могут возникать группами. Групповые ошибки\* имеют, если можно так сказать, свои достоинства и недостатки.

Их достоинство заключается в следующем. Пусть данные передаются блоками по 1 000 бит, а частота ошибок  $10^{-3}$  на 1 бит, т. е. одна ошибка на каждые 1 000 бит. Если ошибки одиночные, т. е. изолированные и независимые, то практически каждый блок данных в среднем будет содержать ошибку. Если же ошибки возникают группами по 100 сразу, то в среднем они будут содержаться в одном-двух

---

\* В отечественной литературе также используется термин «пакетные ошибки». Однако чтобы избежать каких-либо ассоциаций с пакетами данных, мы будем использовать термин «групповые ошибки».

блоках из каждых 100. Недостатком групповых ошибок является то, что их труднее обнаруживать и исправлять, чем одиночные.

#### 4.1.6. Коды с исправлением ошибок

К надежной передаче битов были предложены два основных подхода. Первый — внести избыточность в передаваемый блок данных в форме дополнительных битов таким образом, чтобы, анализируя полученный блок, можно было бы указать, где возникли искажения. Это так называемые *коды с исправлением ошибок* [30]. Второй — внести избыточность, но лишь настолько, чтобы, анализируя полученные данные, можно было сказать, есть в переданном блоке ошибки или нет. Это так называемые *коды с обнаружением ошибок* [1, 16, 19, 23, 31].

Пусть данные занимают  $m$  разрядов, и к ним добавляется  $r$  избыточных контрольных разрядов. При этом необходимо передать слово длиной  $n = m + r$ , называемое  $n$ -битовым *кодословом*. *Расстояние Хемминга* между двумя кодословами — это число разных разрядов в этих кодословах. Например, пусть имеется два кодослова — 10001001 и 10110001. Расстояние Хемминга между ними равно трем, так как число различных разрядов в них — три. Следовательно, если два кодослова находятся на расстоянии  $d$  по Хеммингу, это означает, что для преобразования одного кодослова в другое необходимо преобразовать ровно  $d$  разрядов.

Поскольку избыточные контрольные разряды могут принимать только вполне определенные значения, то при длине  $n$  не все  $2^n$  кодовых слов возможны. Зная алгоритм установки контрольных разрядов, можно вычислить минимальное расстояние Хемминга между двумя правильными кодословами.

Способность кода исправлять ошибки или только обнаруживать их зависит от расстояния между кодословами по Хеммингу. Если мы хотим обнаружить  $d$  ошибок, то необходимо, чтобы правильные кодослова отстояли друг от друга на расстояние  $d + 1$ . Тогда, если минимальное расстояние принятого кода от правильных кодослов  $k < d$ , то принятое кодослово содержит  $k$  ошибок. Если мы хотим исправить  $d$  ошибок, то необходимо, чтобы кодослова отстояли друг от друга на расстояние  $2d + 1$ . В этом случае, даже если переданное кодослово содержит  $d$  ошибок, оно все равно расположено ближе только к одному кодослову, чем к другим. Это кодослово и считается правильным, и таким образом можно определить исходное слово.

Простым примером кода с обнаружением одной ошибки является код с битом четности, конструкция которого следующая: к исходному кодослову добавляется бит четности. Если число единиц в исходном кодослове четное, то значение этого бита ноль, а если нечетное, то — единица. В случае единичных ошибок у кодослов с битом четности расстояние Хемминга равно двум, так как любая ошибка в

одном бите порождает ошибку четности. Однако при возможности двойных ошибок бит четности проблему не решает.

В качестве примера кода с исправлением ошибки рассмотрим код, в котором есть только четыре правильных кодослова: 000000000, 000001111, 111100000, 111111111. Расстояние Хемминга в этом коде равно пяти, следовательно, он может исправлять двойные ошибки. Если получатель примет слово 0000000111, будет ясно, что исходное слово имело вид 000001111. Однако, если допустимы тройные ошибки, то полученное слово 0000000111 может означать, что исходным было слово 000000000.

Оценим минимальное количество контрольных разрядов, необходимое для исправления одиночных ошибок. Пусть имеется код из  $m$  бит сообщения и  $r$  контрольных битов. В этом случае каждое из  $2^m$  правильных сообщений содержит  $n$  неправильных кодослов на расстоянии Хемминга, равном единице, где  $n = m + r$ . Таким образом, с каждым из  $2^m$  кодослов связано  $n + 1$  кодослов:  $n$  неправильных и одно правильное. Так как общее число кодослов  $2^n$ , то  $(n + 1)2^m \leq 2^n$ . Учитывая, что  $n = m + r$ , получим отношение

$$(m + r + 1) \leq 2^r.$$

Для заданного  $m$  это отношение задает минимальное число контрольных разрядов, необходимых для исправления одиночных ошибок. Такой теоретический предел достигим при использовании метода, предложенного Хеммингом, идея которого заключается в следующем:

- разряды кодослова нумеруются слева направо, начиная с 1;
- все биты, номера которых являются степенью 2 (т.е. 1, 2, 4, 8, 16 и т.д.) — контрольные, остальные — биты сообщения;
- каждый контрольный бит отвечает за четность группы битов, включая себя. Чтобы определить группу битов, за четность которой отвечает определенный контрольный бит, следует представить номер позиции каждого бита по степеням двойки. Те биты, в номера которых входит степень двойки, равная номеру контрольного бита, и есть искомая группа. Например,  $11 = 1 + 2 + 8$ ,  $39 = 1 + 2 + 4 + 32$ . Таким образом, бит в позиции 11 и бит в позиции 39 входят в группу, контролируруемую битом в позиции 2.

Приняв кодослово, получатель устанавливает специальный счетчик в нуль, а затем проверяет каждый контрольный бит на предмет правильности четности группы битов, контролируемой этим контрольным битом. Если четность нарушена, то порядковый номер этого бита заносится в счетчик. Если после такой проверки счетчик остается на нуле, то все в порядке. Если нет, то он содержит номер неправильного разряда. Например, если 1, 2, 8 — ошибочные контрольные разряды, то ошибка содержится в 11-м разряде, так как только он связан одновременно с этими контрольными разрядами.

Символ    ASCII-код    Контрольные биты

Н	1001000	00110010000
а	1100001	10111001001
м	1101101	11101010101
м	1101101	11101010101
і	1101001	01101011001
п	1101110	01101010110
g	1100111	11111001111
	0100000	10011000000
с	1100011	11111000011
о	1101111	00101011111
d	1100100	11111001100
е	1100101	00111000101

Порядок передачи битов

Рис. 4.2. Использование кода Хемминга для исправления ошибок передачи

На рис. 4.2 показаны 7-разрядный ASCII-код и соответствующий ему 11-разрядный код Хемминга. В этом коде Хемминга разряды 1, 2, 4, 8 — контрольные, 3-й разряд соответствует 1-му разряду исходного кода, а разряды 5, 6, 7, 9, 10, 11 — разрядам 2, 3, 4, 5, 6, 7. В коде Хемминга 1-й разряд контролирует группу, в которую входят разряды с номерами 3, 5, 7, 9, 11, что соответствует разрядам 1, 2, 4, 5, 7 в исходном коде. Так как единица в этих разрядах исходного кода четная, то 1-й разряд в коде Хемминга равен нулю. Аналогично определяется значение остальных контрольных разрядов.

Код Хемминга может исправлять только одиночные ошибки. Однако существует прием, который позволяет распространить идеи Хемминга на случай групповых ошибок. Пусть требуется передать  $k$  кослов. Расположим их в виде матрицы: одно слово — строка. Обычно передают слово за словом, но мы поступим иначе: передадим слово длиной  $k$  сначала из первых разрядов всех слов, затем — из вторых и так далее, т. е. по столбцам. После приема всех слов матрица восстанавливается. Если необходимо обнаруживать групповые ошибки размером  $k$ , то в каждой строке восстановленной матрицы будет не более одной ошибки, а с одиночными ошибками код Хемминга справится.

#### 4.1.7. Коды с обнаружением ошибок

Рассмотрение кодов с обнаружением ошибок начнем с небольшого примера. Пусть имеется канал передачи, в котором одиночные ошибки появляются с частотой  $10^{-6}$  на один бит. В случае необходимости исправление единичных ошибок при передаче блока данных размером в 1 000 бит потребуются 10 контрольных битов  $((m + r + 1) \leq 2^r$ , где  $m = 1\,000$ , т. е.  $(1001 + r) \leq 2^r$ , следовательно,  $r = 10$ ).

При передаче 1 Мбит данных требуется потратить 10 000 контрольных битов. В то же время для обнаружения единичной ошибки до-

статочно одного бита четности. Следовательно, при использовании техники повторной передачи на передачу 1 000 блоков по 1 000 бит в каждом требуется потратить 1 001 бит четности или с повторной передачей 2 002 бит вместо 10 000 бит в случае применения кода с исправлением ошибки.

Прямое применение техники четности в случае наличия групповых ошибок не дает необходимого результата, поэтому ее следует скорректировать. Пусть требуется передать  $n$  слов по  $k$  бит. Расположим их в виде матрицы  $n \times k$ . Для каждого столбца установим бит четности и разместим его в дополнительной строке, после чего передадим матрицу по строкам. При получении матрица восстанавливается, и если хоть один бит нарушен, то весь блок передается повторно. Этот метод позволяет обнаружить групповые ошибки длиной  $n$ , однако против групповых ошибок длиной  $n + 1$  он бессилён.

На практике применяют другую технику, которая называется *циклическим избыточным кодом* (Cyclic Redundancy Code — CRC) [46]. CRC-коды построены на основе представления битовой строки как строки коэффициентов полинома. При этом битовую строку длиной  $k$  рассматривают как коэффициенты полинома степени  $k - 1$ , а самый левый бит строки — как коэффициент при старшей степени. Например, строка 110001 представляет собой полином вида  $x^5 + x^4 + x^0$ .

Использование полиномиальных кодов при передаче заключается в следующем. Отправитель и получатель заранее договариваются о некотором определенном полиноме  $G(x)$ , в котором коэффициенты при старшем и младшем членах должны быть равны 1 и который называется образующим. Идея данного метода состоит в добавлении контрольной суммы к передаваемому блоку, рассматриваемому как полином  $M(x)$ , таким образом, чтобы передаваемый блок с контрольной суммой был кратен полиному  $G(x)$ . Когда к получателю приходит блок данных с контрольной суммой, он делит его на  $G(x)$ \*. Наличие при этом остатка свидетельствует об ошибках при передаче. Пусть степень  $G(x)$  равна  $r$ . При вычислении контрольной суммы блока из  $m$  бит должно выполняться условие  $r < m$ . Арифметические операции с полиномами выполняются по модулю 2. При делении сложение и вычитание происходят без переноса разрядов, т. е. по модулю 2, и, следовательно, эти операции становятся эквивалентными операции EXCLUSIVE OR.

Алгоритм вычисления контрольной суммы, где  $r$  — степень  $G(x)$ , следующий:

1) добавить  $r$  нулей в конец передаваемого блока таким образом, чтобы он содержал  $m + r$  разрядов и соответствовал полиному  $x^r M(x)$ ;

2) разделить по модулю 2 полином  $x^r M(x)$  на  $G(x)$ ;

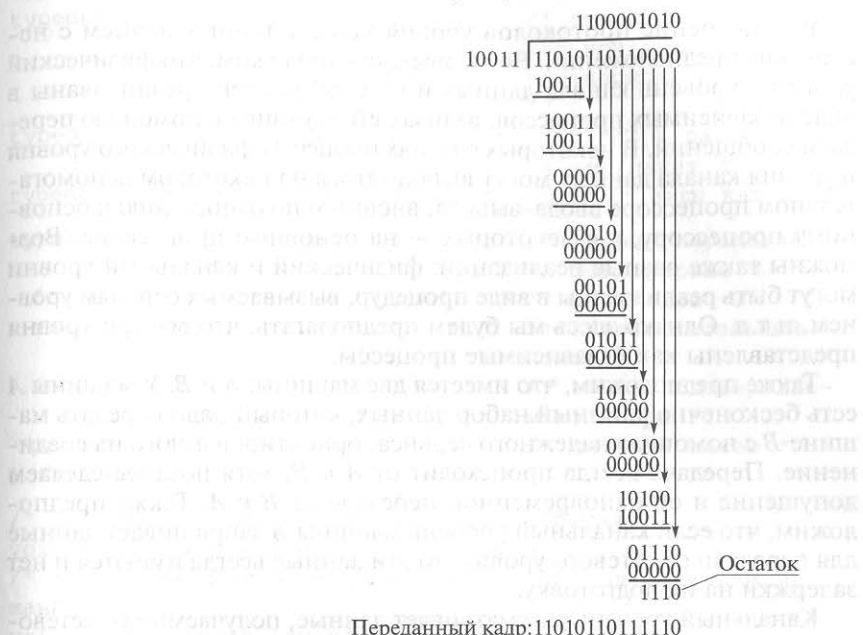
---

\* Поскольку операция деления на вычислительных машинах сводится к операции сдвига, то она может быть реализована эффективно.

Кадр: 1101011011

Генератор: 10011

Сообщение после прибавления четырех нулей: 11010110000



Переданный кадр: 11010110111110

Рис. 4.3. Расчет контрольной суммы для полиномиального кода

3) вычесть остаток (длина которого всегда не более  $r$  разрядов) из строки, соответствующей полиному  $x^r M(x)$  по модулю 2. Полученный результат и является блоком с контрольной суммой (назовем его  $T(x)$ ).

Рис. 4.3 [40] показывает, как этот алгоритм работает для блока 1101011011 и  $G(x) = x^4 + x + 1$ .

Данный метод позволяет обнаруживать одиночные ошибки, групповые ошибки длиной не более  $r$  и нечетное число отдельных ошибок.

Существует три международных стандарта на вид полинома  $G(x)$ :

- CRC-12 —  $x^{12} + x^{11} + x^3 + x^2 + x + 1$ ;
- CRC-16 —  $x^{16} + x^{15} + x^2 + 1$ ;
- CRC-CCITT —  $x^{16} + x^{12} + x^5 + 1$ .

Стандарт CRC-12 используется для передачи символов из шести разрядов, а CRC-16 и CRC-CCITT — из восьми. Стандарты CRC-16 и CRC-CCITT ловят одиночные, двойные ошибки, групповые ошибки длиной не более 16 и нечетное число изолированных ошибок. Достаточно подробно техника циклических кодов рассматривается в [40].

## 4.2. Протоколы для каналов типа точка—точка

### 4.2.1. Простейшие протоколы канала данных

Рассмотрение протоколов уровня канала данных начнем с нескольких предположений. Во-первых, предположим, что физический уровень, уровень канала данных и сетевой уровень реализованы в виде независимых процессов, взаимодействующих с помощью передачи сообщений. В некоторых случаях процессы физического уровня и уровня канала данных могут выполняться на некотором вспомогательном процессоре ввода-вывода, внешнем по отношению к основному процессору, а в некоторых — на основном процессоре. Возможны также разные реализации: физический и канальный уровни могут быть реализованы в виде процедур, вызываемых сетевым уровнем, и т.д. Однако здесь мы будем предполагать, что все три уровня представлены как независимые процессы.

Также предположим, что имеется две машины: *A* и *B*. У машины *A* есть бесконечно длинный набор данных, который надо передать машине *B* с помощью надежного сервиса, ориентированного на соединение. Передача всегда происходит от *A* к *B*, хотя позднее сделаем допущение и об одновременной передаче от *B* к *A*. Также предположим, что если канальный уровень машины *A* запрашивает данные для передачи от сетевого уровня, то эти данные всегда имеются и нет задержки на их подготовку.

Канальный уровень рассматривает данные, получаемые от сетевого уровня, как неструктурированные, несмотря на то что в них имеется хотя бы заголовок сетевого уровня. Все эти данные должны быть переданы равнозначному сетевому уровню. Когда канальный уровень получает пакет, он погружает его в кадр, добавляя признаки начала и конца кадра. Этот кадр затем передается на физическом уровне.

Допустим, что есть две библиотечные функции: *from\_physical\_layer* — для получения кадра с физического уровня, и *to\_physical\_layer* — для передачи кадра на физический уровень. Предположим также, что вычисление и добавление контрольных сумм происходит аппаратно.

Изначально получатель просто ожидает наступления какого-либо события, ничего не предпринимая. В наших примерах это отражается вызовом функции *wait\_for\_event(&event)*, где параметр *event* возвращает информацию о произошедшем событии. Ясно, что в действительности никто не будет ожидать в цикле (для этого обычно используются прерывания), но мы будем так считать для упрощения.

Когда кадр поступает к получателю, контрольная сумма вычисляется аппаратно. Если она неверна, то канальному уровню сообщается следующее: *event = cksum\_err*. Если же кадр поступил без повреждений, то канальный уровень получает сообщение: *event = frame\_arrivel*.

Приведем перечень структур и функций [40], используемых в реализации протокола канального уровня:

```

#define MAX_PKT 1024 /* размер пакета в
                      байтах */

typedef enum (false, true) boolean: /* булевский тип */
typedef unsigned int seq_nr: /* тип для последовательной нумерации или подтверждения получения */

typedef struct {unsigned char data [MAX_PKT]} packet: /* тип/пакет */
typedef enum (data, ack, nak) frame_kind: /* виды кадров */
typedef struct: /* кадры, передаваемые на этом уровне */
    frame_kind kind: /* вид кадра */
    seq_nr seq: /* последовательный номер */
    seq_nr ask: /* номер подтверждаемого кадра */
    packet info: /* сетевой пакет */
} frame:

/* ожидание события возвращает тип события */
void wait_for_event(event_type*event);
/* получение пакета от сетевого уровня для передачи на канальный */
void from_network_layer(packet *p);
/* доставка информации из полученного кадра на сетевой уровень */
void to_network_layer (packet *p);
/* получение кадра с физического уровня и копирование его в r */
void from_physical_layer(frame *r);
/* передача кадра на физический уровень для отправки */
void to_physical_layer(frame *s);
/* включение таймера и ожидание события timeout */
void start_timer (seq_nr k);
/* остановка таймера и отмена ожидания события timeout */
void stop_timer(seq_nr k);
/* запуск вспомогательного таймера и разрешение события ack_timer */
void start_ack_timer(void);
/* остановка вспомогательного таймера и запрет события ack_timer */
void stop_ack_timer (void);
/* разрешение сетевому уровню генерировать событие network_layer_ready */
void enable_network_layer(void);

```

```

/* запрет сетевому уровню генерировать событие network_
layer_ready */
void disable_network_layer(void).

```

Как уже отмечалось, для обеспечения возможности обнаружения потери кадров уровень канала, отправляя кадр, должен устанавливать таймер. Если подтверждение не приходит до истечения времени, установленного таймером, считается, что кадр не дошел. В этом случае получают сообщение *event = timeout*. Процедуры *start\_timer* и *stop\_timer* используются соответственно для запуска и остановки таймера, причем процедуру запуска таймера можно вызывать, не ожидая окончания предыдущего запуска. Подобное обращение означает перезапуск таймера на новый интервал.

Процедуры *start\_act\_timer* и *stop\_act\_timer* используются для управления дополнительным таймером, используемым в определенных случаях для уведомления.

#### 4.2.2. Симплекс-протокол без ограничений

Рассмотрим простейший симплексный протокол канального уровня:

```

/* Протокол 1 позволяет передавать данные от передатчика
к получателю. Предполагается, что канал передачи
свободен от ошибок и получатель способен обрабатывать
входные данные сколь угодно быстро. */

```

```

typedef enum (frame_arrival)event_type;
#include "protocol.h"

void sender1(void)
{
    frame s; /* буфер для входного
              кадра */
    packet buffer; /* буфер для входного
                   пакета */

    while (true) {
        from_network_layer(&buffer); /* получаем то, что
                                       будем отправлять */
        s.info=buffer; /* копируем в s для
                       передачи */
        to_physical_layer(&s); /* отсылаем */
    } /* и снова, и снова,
        и снова */
}

void receiver1 (void)

```

```

}
frame r;
event_type event;                               /* заполняется при ожида-
                                                    нии, но здесь не исполь-
                                                    зуется */

while (true) {
    wait_for_event(&event);                       /* единственно возможное
                                                    событие —
                                                    / frame- frame_arrival */
    from_physical_layer(&r):                       /* получаем входной кадр */
    to_network_layer(&r.info):                   /* передаем данные
                                                    на сетевой уровень */
}
}

```

Этот протокол передает данные только в одном направлении. При этом считается, что получатель и отправитель всегда готовы к отправке и получению данных. Время обработки данных игнорируется. Предполагается также, что буфер имеет неограниченные размеры, а данные в канале не теряются и не искажаются.

### 4.2.3. Симплексный старт-стопный протокол

Теперь снимем одно из ограничений предыдущего протокола — способность сетевого уровня обрабатывать поступающие данные сколь угодно быстро. Все остальные предположения остаются в силе: канал абсолютно надежный, трафик однонаправленный.

Основная проблема — предотвращение ситуации, когда отправитель «заваливает» данными получателя. Если получателю требуется время  $\Delta t$  для исполнения функции *from\_physical\_layer* плюс *to\_network\_layer*, то отправитель должен передавать данные со средней скоростью один кадр за время  $\Delta t$ .

Решением этой проблемы может быть введение коротких специальных служебных сообщений. В этом случае получатель, получив один или несколько кадров, отправляет отправителю короткий специальный кадр, означающий, что отправитель может передавать следующий кадр. Приведем этот так называемый старт-стопный протокол капитального уровня:

```

/* Протокол 2 служит для однонаправленной передачи данных
от передатчика к приемнику. Канал, как и в Протоколе
1, предполагается свободным от ошибок. Однако на этот
раз у приемника буфер конечного объема и скорость
обработки поступающих данных конечны. Таким образом,
протокол должен явно препятствовать передатчику пере-
гружать приемник данными, передавая их быстрее, чем
тот способен их обработать */

```

```

typedef enum (frame_arrival) event_type;
#include "protocol.h"

void sender2(void)
{
    frame s; /* буфер для выходного кадра */
    packet buffer; /* буфер для выходного пакета */
    event_type event; /* единственно возможное событие — frame_arrival */

    while (true) {
        from_network_layer(&buffer); /* получаем для отправки */
        s.info = buffer; /* копируем в s для передачи */
        to_physical_layer(&s); /* Счастливого пути! */
        wait_for_event(&event); /* ждем наступления события */
    }
}

void receiver2(void)
{
    frame r.s; /* буфера для кадров */
    event_type event; /* единственно возможное событие frame_arrival */

    while (true) {
        wait_for_event(&event); /* ожидаем единственно возможное событие — frame_arrival */
        from_physical_layer(&r); /*получаем входной кадр */
        to_network_layer (&r.info); /* посылаем данные на сетевой уровень */
        to_physical_layer(&s); /* посылаем пустой кадр для того, чтобы «разбудить» приемник */
    }
}

```

#### 4.2.4. Симплексный протокол для канала с шумом

Основная проблема при передаче по каналу с шумом состоит в том, что кадр с подтверждением о получении может быть потерян целиком. Как отличить кадр, переданный первый раз, от кадра, переданного повторно?

Одно из очевидных решений — нумерация передаваемых кадров. Однако сколько места отводить под эту нумерацию? Поскольку эта проблема возникает только для последовательных кадров  $m$  и  $m + 1$ , то достаточно одного разряда: 0 — для только что посланного кадра и 1 — для следующего ожидаемого\*. Все кадры, не содержащие корректной нумерации, просто сбрасываются при приеме.

Приведем программу протокола с подтверждением и восстановлением:

```

/* Протокол 3 для однонаправленной передачи данных через
ненадежный канал */

#define MAX_SEQ 1 /* должно быть равно
                  1, для Протокола 3 */
typedef enum {frame_arrival, cksum_err; timeout}event_type,
#include "protocol.h"

void sender3(void)
{
seq_nr next_frame_to_send; /* последовательный
                             номер для следующего
                             отправляемого кадра */
frame s; /* переменная для
           кадра */
packet buffer; /*буфер для отправляе-
               мого пакета */
event_type event;
next_frame_to_send = 0; /* первое значение для
                          последовательных но-
                          меров отправляемых
                          кадров */
from_network_layer(&buffer); /* получение первого
                               пакета */

while (true) {
s.info = buffer /* формирование кад-
                 ра для передачи */
s.seq = next_frame_to_send; /* установка после-
                              довательного номера
                              в кадре */
to_physical_layer(&s); /* пересылка кадра */
start_timer(s.seq); /*запуск таймера,
                    ожидание одного из
                    следующих событий */
wait_for_event(&event); /* frame_arrival,
                          chssum_err, timeout */
}

```

\* Попробуйте доказать справедливость этого утверждения.

```

if (event == frame_arival) {
    from_physical_layer(&s); /* получение кадра */
    if (s_ask == next_frame_to_send); /* проверка подтвержде-
        ние */
        from_network_layer(&buffer); /* получение следую-
            щего пакета для пе-
            редачи */
            inc (next_frame_to_send); /* увеличение после-
                довательного номера
                для следующего */
        }
    }
}

void receiver3(vod)
{
    seq_nr frame_expected;
    frame r, s;
    event_type event;
    frame_expected = 0;
    while (true) {
        wait_for_event(&event); /* возможны события:
            frame_arnival,
            ckcsun.err */

        if (event == frame_arrival) { /* получен коррект-
            ный кадр */
                from_physical_layer(&r); /* получен очередной
                    прибывший кадр */
                    if (r.seq == frame_expected); /* вот это то, что мы
                        ждали */
                            to_network_layer(&r.info); /* передаем данные
                                на сетевой уровень
                                */
                                    inc (frame_expected); /* в следующий раз
                                        ожидает другой после-
                                        довательный номер */
                                            }
                                                s_ask = 1 - frame_expected; /* показывает полу-
                                                    чение какого кадра
                                                    подтверждается */
                                                        to_physical_layer(&s); /* ни одно из полей
                                                            не используется */
                                                                }
                                                                    }
}

```

#### 4.2.5. Протоколы скользящего окна

В рассмотренных протоколах канального уровня кадры передавались только в одном направлении. Для обеспечения передачи в обоих направлениях на физическом уровне требуется два симплексных канала: один для передачи кадров, другой — для передачи подтверждений. Однако использование канала только для подтверждений — довольно дорогое удовольствие. Можно смешивать кадры с данными и кадры с подтверждениями на одном канале. Это, конечно, решение проблемы, но по-прежнему на подтверждения будет тратиться полезная пропускная способность канала.

Можно также для подтверждения использовать полезные кадры с данными, движущимися в попутном направлении. В этом случае получатель не сразу отправляет подтверждение, а ожидает от сетевого уровня очередного пакета. Как только такой пакет возникает, канальный уровень помещает в кадр с пакетом в специальное поле *ack* уведомление о получении. Такой прием позволяет полнее использовать имеющуюся пропускную способность канала. Меньше кадров — меньше прерываний на канальном уровне на их обработку и меньше затрат на буферизацию.

Однако реализация этой идеи усложняет протокол, поскольку непонятно, что делать, если тайм-аут у отправителя на получение подтверждения заканчивается, а с сетевого уровня получателя не поступает запрос на передачу пакета. Поэтому на канальном уровне должен быть фиксированный интервал времени, в течение которого он будет ожидать от сетевого канала попутный кадр. Если до истечения этого времени пакет с сетевого уровня не поступил, то канальный уровень отправляет подтверждение отдельным кадром.

Теперь подробно рассмотрим класс протоколов скользящего окна. Протоколы этого класса выполняют следующее: получатель сообщает отправителю значение определенной константы  $n$  (числа кадров), которое тот может послать, не ожидая подтверждения для каждого кадра получателем. Отправленные кадры отправитель сохраняет у себя в буфере до тех пор, пока не получит подтверждение об их получении. По мере получения подтверждений отправленные кадры сбрасываются из буфера отправителя, и буфер пополняется новыми кадрами.

Мы уже сталкивались с подобными протоколами. Например, это старт-стопный протокол, в котором  $n$  было равно 1. Обычно же в таких протоколах  $n = 2^k - 1$ . У получателя и отправителя в этом случае имеется набор последовательных чисел — номеров кадров, которые отправитель может отправить, не ожидая подтверждения каждого из них. Эти кадры образуют окно отправки. Аналогично у получателя имеется буфер для получения и временного хранения получаемых кадров — окно получения.

Хотя в этих условиях отправителю обеспечивается определенная свобода в порядке отправления кадров, мы по-прежнему будем счи-

тать, что кадры отправляются в соответствии с порядковыми номерами. Окна отправки и получения имеют верхнюю и нижнюю границы. Порядковые номера кадров в окне отправки показывают кадры отправленные, но не подтвержденные. Как только от сетевого уровня поступает еще один пакет, ему присваивается первый свободный наибольший номер, и верхняя граница окна отправителя поднимается. Как только приходит подтверждение получения, нижняя граница окна также поднимается. Таким образом, в окне все время находятся неподтвержденные кадры.

Рассмотрим протокол скользящего окна, имеющего максимальный размер 1 бит. Такой протокол использует старт-стопный режим и, послав один кадр, не шлет другой, пока не придет подтверждение на первый.

Приведем текст протокола скользящего окна размером 1 бит [40]:

```

/* Протокол 4 является двунаправленным и более полным,
чем Протокол 3 */
#define MAX_SEQ1 /*должно быть равно 1 для протокола 4
*/
typedef enum {frame_arrival, cksum_err, timeout) event_
type;
#include "protocol.h"
void protocol4 (void)
{
    seq_nr next_frame_to_send; /*0 или 1 */
    seq_nr frame_expected; /*0 или 1 */
    frame r, s; /*переменные для кадров */
    packer buffer; /*буфер для пакета, который
был послан */
    event_type event.
    next_frame_to_send = 0; /* следующий кадр в опрвляемом
потоке */
    frame_expected = 0; /* номер кадра, ожидаемого к
поступлению */
    from_network_layer (&buffer); /* получаем пакет с сетевого
уровня */
    s.info = buffer; /* подготовка к отправке
первого кадра */
    s.seq = next_frame_to_send; /* вставляем последовательный
номер в кадр */
    s.ask = 1 - frame_expected; /* подтверждение с попутным
кадром */
    to_physical_laylr (&s); /* передаем кадр */
    start_timer (s.seq); /* включаем таймер */

```

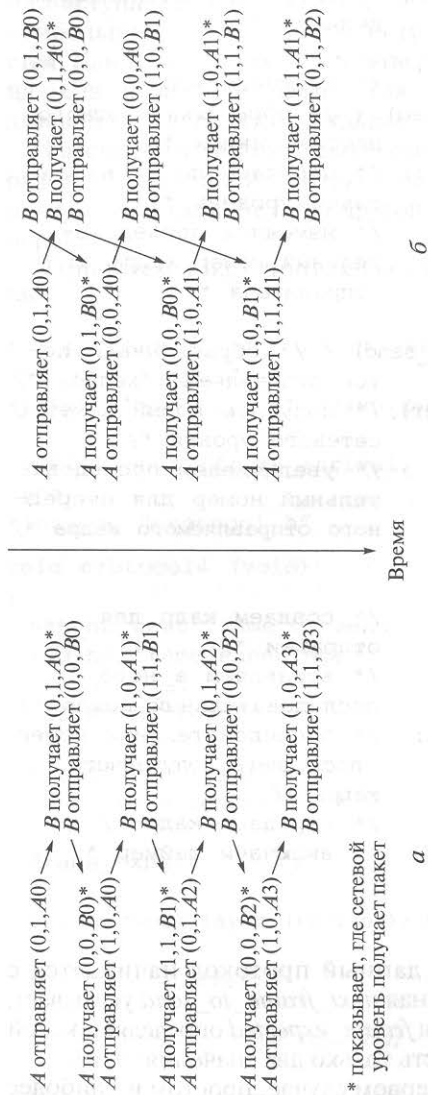
```

while (true) {
    wait_for_event(&event);
    if (event == frame_arrival)
    {
        from_physical_layer (&r);
        if (r.seq == frame_expected) {
            to_network_layer (&r.info);
            inc(frame_expected);
        }
        if (r.ask == next_frame_to_send) {
            from_network_layer (&buffer);
            inc(next_frame_to_send);
        }
    }
    s.info = buffer;
    s.seq = next_frame_to_send;
    s.ask = 1 - frame_expected;
    to_physical_layer (&s);
    start_timer (s.seq);
}

```

Как и все другие протоколы, данный протокол начинается с определения переменных. Переменная *next\_frame\_to\_send* указывает, какой кадр посылается. Переменная *frame\_expected* определяет, какой кадр получатель ожидает, и у нее есть только два значения: 0 и 1.

Здесь возможны два случая. В первом случае, простом и наиболее удобном, один из канальных уровней первым начинает передачу. В этом случае вне тела основного цикла одной из программ канального уровня имеются обращения к процедурам *to\_physical\_layer* и *start\_timer*.



б

Рис. 4.4. Два сценария (а, б) для протокола скользящего окна в 1 бит

\* показывает, где сетевой уровень получает пакеты

Машина, иницирующая обмен, берет пакет от сетевого уровня, формирует кадр и посылает его. Когда этот кадр (или любой другой) поступает, канальный уровень-получатель проверяет, не является ли этот кадр дубликатом. Если поступивший кадр тот, который ожидался, то он передается на сетевой уровень и окно получателя сдвигается вверх.

Поле уведомления содержит номер последнего кадра, полученного без ошибок. Если этот номер согласуется с номером кадра, который стараются послать, то уровень-отправитель считает, что кадр, хранящийся в буфере, послан и сбрасывает его оттуда, забирая при этом новый кадр с сетевого уровня. Если же указанные номера не согласуются, то отправитель старается послать тот же кадр еще раз. При этом в любом случае, после получения кадра отправляется новый кадр.

На рис. 4.4 показана схема работы протокола скользящего окна в 1 бит. Если у машины *A* очень короткий тайм-аут, то все дубликаты кадра пойдут с одним и тем же значением полей *seq* и *ack*. Поэтому, получив исправный кадр, машина *B* установит значение переменной *frame\_expected*, равное 1, и pošлет подтверждение. Все последующие дубликаты будут отвергнуты машиной *B*, так как она ожидает кадр с единицей, а не с нулем.

Случай, когда оба канальных уровня начинают передачу одновременно, рассматривается в [40].

#### **4.2.6. Протокол с возвратом на *n* кадров и протокол с выборочным повтором**

До сих пор мы предполагали, что время доставки кадра и время доставки подтверждения пренебрежимо мало. В некоторых случаях это предположение очевидно не работает, т. е. оно может приводить к серьезным бесполезным тратам пропускной способности канала. Рассмотрим канал со скоростью передачи 50 Кбит/с и общей задержкой 500 мс, например спутниковый канал. Попробуем использовать протокол скользящего окна для передачи кадров размером 1 000 бит по этому каналу. В момент времени  $t = 0$  отправитель отправляет первый кадр. В момент времени  $t = 20$  мс кадр полностью отправлен, в момент времени  $t = 270$  мс он принят и в момент времени  $t = 520$  мс отправитель получил подтверждение. Эти цифры говорят о том, что отправитель был блокирован в течение 96 % времени работы (500/520), а это потеря пропускной способности канала.

Рассматриваемая проблема является следствием правила, по которому отправитель прежде чем послать следующий кадр ждет подтверждения о получении предыдущего кадра. Это требование можно ослабить, т. е. разрешить отправителю отправлять  $w$  кадров, не дожидаясь их подтверждения. Надлежащим образом выбрав значение  $w$ , отправитель может заполнить все время, необходимое на отправ-

ку кадра и получение его подтверждения. В приведенном примере  $w$  должно быть равно по крайней мере 26. Это число кадров, какое отправитель успеет отправить за 520 мс, т.е. прежде чем придет подтверждение на кадр 0. Таким образом, неподтвержденными будут 25 из 26 кадров, а размер окна отправителя будет равным 26 кадрам.

При использовании этой техники, известной как конвейер, в случае применения ненадежного канала необходимо решить несколько проблем. Во-первых, что делать, если в середине потока пропадет или попадет поврежденный кадр? Ведь получатель уже получит большое количество кадров к тому моменту, когда отправитель обнаружит, что что-то произошло. В то же время, когда получатель получил поврежденный кадр, он его должен сбросить, поэтому необходимо решить вопрос, что делать с последующими кадрами. Помните, что канальный уровень обязан передавать пакеты на сетевой уровень в том порядке, в каком их отправлял отправитель.

Имеется два метода решения этих проблем: *откат* и *выборочный повтор*. При откате все кадры, поступившие после поврежденного кадра, сбрасываются и не подтверждаются. Отправитель по тайм-ауту повторно отправляет все кадры, начиная с первого неподтвержденного кадра. При выборочном повторе у получателя длина окна такая же, как и у отправителя. Отправитель отмечает неподтвержденные кадры и посылает их еще раз. Получатель вставляет повторно посланные кадры туда, где требуется, и не передает на сетевой уровень пакет, если в нем есть разрывы.

#### 4.2.7. Протокол HDLC

До сих пор мы рассматривали схемы решений основных проблем, с которыми приходится иметь дело на канальном уровне. Теперь познакомимся с группой давно известных, но по-прежнему широко используемых на практике протоколов. Все они имеют одного предшественника — SDLC (Synchronous Data Link Control) — протокол управления синхронным каналом, предложенный фирмой IBM. Этот протокол был модифицирован ISO и выпущен под названием HDLC (High level Data Link Control). Протокол HDLC был модифицирован МСЭ для X.25 и выпущен под названием LAP (Link Access Procedure), который позднее был модифицирован как LAPB.

Все эти протоколы для обособления кадров используют технику вставки специальных последовательностей битов и являются бит-

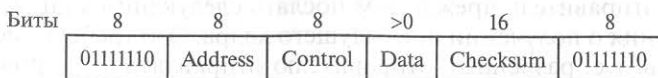


Рис. 4.5. Типовая структура кадра протокола HDLC

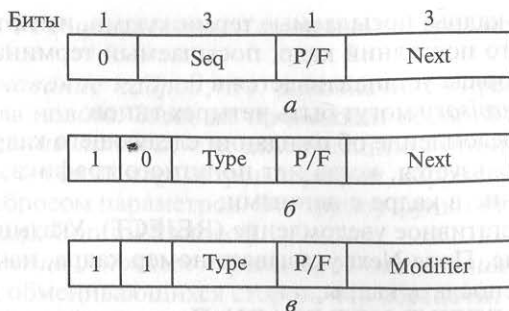


Рис. 4.6. Поле Control для кадров Information (а), Supervisory (б) и Unnumbered (в)

ориентированными протоколами. Различия между ними незначительные.

На рис. 4.5 показана типовая структура кадра протокола HDLC:

- поле Address используется для адресации, если на линии имеется несколько абонентов. Для линий точка — точка это поле используется для того, чтобы отличать команду от ответа;
- поле Control используется для последовательных номеров кадров, подтверждений и других нужд;
- поле Data, которое может быть сколь угодно большим, используется для передачи данных. Надо только иметь в виду, что чем длиннее это поле, тем больше вероятность повреждения кадра на линии;
- поле Checksum используется для формирования контрольной суммы с помощью CRC-кода.

Флаговые последовательности 01111110 используются для разделения кадров и постоянно передаются по незанятой линии в ожидании кадра. Именно это свойство протокола HDLC и определяет слово «синхронный». Этот протокол использует три вида кадров: *Information*, *Supervisory*, *Unnumbered*.

Организация поля Control для этих трех видов кадров показана на рис. 4.6.

Для кадров *Information* структура поля показана для случая трех-битового поля Seq — номера кадра, поэтому в окне отправителя может находиться до семи неподтвержденных кадров. Заметим, что в протоколе LAPB в стандарте X.25 это поле может состоять из 7 и 15 бит. Поле Next используется для отправки подтверждения вместе с передаваемым кадром. Подтверждение может быть в форме номера последнего правильно переданного кадра, а может быть в форме первого, еще не переданного кадра. Какой вариант будет использован — зависит от параметров протокола.

Разряд P/F используется при работе с группой терминалов. Когда компьютер приглашает терминал к передаче, он устанавливает этот

разряд в 1 (все кадры, посылаемые терминалами, имеют здесь значение 1). Если это последний кадр, посылаемый терминалом, то значение этого разряда устанавливается в 0.

Кадры *Supervisory* могут быть четырех типов:

- тип 0 — уведомление об ожидании следующего кадра (RECEIVE READY). Используется, когда нет попутного трафика, чтобы передать уведомление в кадре с данными;

- тип 1 — негативное уведомление (REJECT). Указывает на ошибку при передаче. Поле Next указывает номер кадра, начиная с которого надо перепослать кадры;

- тип 2 — RECEIVE NOT READY. Подтверждает все кадры кроме указанного в поле Next. Используется для сообщения источнику кадров о необходимости приостановки передачи в силу каких-то проблем у получателя. После устранения этих проблем получатель посылает кадры RECEIVE REDAY, REJECT или другой надлежащий *Supervisory* кадр;

- тип 3 — SELECTIVE REJECT. Используется при необходимости перепослать только кадр, указанный в поле Next. Протоколы LAPB и SDLC не используют кадры этого типа. При этом протокол HDLC и протоколы LAPB и SDLC используют разные механизмы для восстановления последовательности недополученных кадров.

Кадры *Unnumbered* иногда используют для целей управления, но чаще они применяются при ненадежной передаче без соединения.

Протокол HDLC использует команду *DISConnect* для сообщения о разрыве соединения, команды для установки счетчиков кадров в нуль, сброса соединения в начальное состояние, установки соподчиненности на линии, а также команды, которые информируют отправителя о ненормальных ситуациях, например о повреждении поля Control кадра (когда контрольная сумма верная, а значения полей противоречивы).

#### 4.2.8. Протокол типа точка — точка — PPP

Протокол типа точка—точка — PPP (Point-to-Point Protocol) был разработан по решению комитета IETF (Internet Engineering Task Force) для замены протокола SLIP, обладавшего многочисленными недостатками. Протокол PPP, описанный в RFC\* 1661, 1662 и 1663, обеспечивает обнаружение ошибок, работает с пакетами разных протоколов сетевого уровня, позволяет динамически выделять IP-адрес только на период соединения, выполняет аутентификацию абонентов и имеет ряд других преимуществ перед протоколом SLIP (Serial Line IP).

\* RFC (Request For Comments) — спецификации описания стандартов в Интернете выпускаемых организацией IAB (Internet Architecture Board). Подробно описываются в подразд. 1.3.2 т. 2 данного учебника.

Протокол PPP обеспечивает выполнение трех основных групп функций:

1. *Распознавание кадров*, т.е. однозначное определение конца кадра и начала нового. Здесь же происходит обнаружение ошибок.

2. *Управление линией*, т.е. активизацию линии, ее проверку, определение основных параметров передачи, корректное завершение передачи со сбросом параметров. Эту группу функций реализует протокол LCP (Link Control Protocol).

3. *Определение основных параметров соединения* между сетевыми уровнями обменивающихся сторон, что обеспечит независимость от реализации сетевого уровня. Протокол PPP предполагает наличие разных специальных протоколов NCP (Network Control Protocol) на каждом поддерживаемом сетевом уровне.

Чтобы лучше понять, как это все работает вместе, рассмотрим типичный сценарий, когда пользователь из дома по телефонной линии хочет подключить свой персональный компьютер (ПК) к Интернету. ПК через модем звонит на маршрутизатор сервис-провайдера. После того как маршрутизатор принял звонок и установил физическое соединение, ПК посылает несколько LCP-пакетов в PPP-кадрах. Маршрутизатор отвечает LCP-пакетами в PPP-кадрах. В результате такого обмена определяются параметры соединения.

После этого следует обмен NCP-пакетами для настройки сетевого уровня. В частности, здесь происходит временное присваивание ПК IP-адреса, который действует только на период соединения. Это происходит, если обе стороны хотят использовать TCP/IP-стек.

Теперь, когда ПК, получив IP-адрес, стал полноправной машиной в Интернете, он может обмениваться IP-пакетами с другими машинами. Когда пользователь закончит работу, NCP разрывает соединение с сетевым уровнем и освобождает ранее занятый IP-адрес, после чего LCP-протокол разрывает соединение на канальном уровне, и ПК говорит модему: «Положи трубку».

PPP-кадры имеют формат, очень близкий к формату HDLC-кадров. Основное их различие состоит в том, что PPP — байт-ориентированный, а HDLC — бит-ориентированный. Для HDLC возможен кадр размером в 30,25 байт, а для PPP — нет. Формат PPP-кадра показан на рис. 4.7.

Все PPP-кадры начинаются со стандартного байта 01111110. Поле Address по умолчанию равно 11111111. Поле Control по умолчанию равно 00000011, что означает Unnumbered-кадр, т.е. нумерация пере-

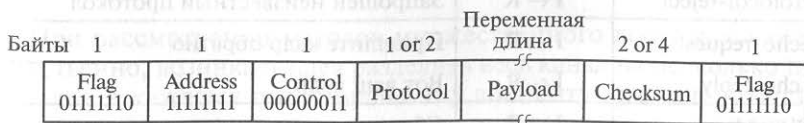


Рис. 4.7. Формат PPP-кадра

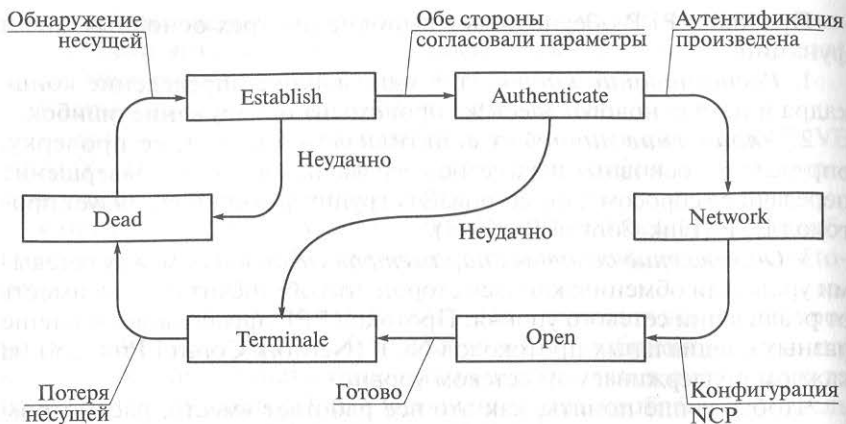


Рис. 4.8. Основные фазы установления соединения и его разрыва

даваемых кадров и подтверждений в их получении здесь не предполагается. В случае ненадежной среды передачи данных имеется вариант надежной передачи, описанный в RFC 1663.

Так как значения полей Address и Control — константы, то LCP-протокол опускает их, экономя два байта на передаче. В поле Protocol указывается, какой тип пакетов будет в поле Payload. Там допускаются

Таблица 4.1

### Типы LCP-пакетов

Название LCP-пакета	Направление передачи	Назначение
Configure-request	I → R	Предлагаемые параметры и их значения
Configure-ack	I ← R	Все параметры приняты
Configure-nak	I ← R	Некоторые параметры не приняты
Configure-reject	I ← R	Некоторые параметры недоступны
Terminate-request	I → R	Требуется закрыть соединение
Terminate-ack	I ← R	ОК, соединение закрыто
Code-reject	I ← R	Получен неизвестный запрос
Protocol-reject	I ← R	Запрошен неизвестный протокол
Echo-request	I → R	Пришлите кадр обратно
Echo-reply	I ← R	Вот ваш кадр
Discard-request	I → R	Сбросьте этот кадр (для проверки)

Здесь I — инициатор соединения; R — вызываемая сторона.

пакеты протоколов LCP, NCP, IP, IPX, Apple Talk и др. Поле Payload, предназначенное для передаваемых данных, имеет переменную длину, которая по умолчанию равна 1 600 байт.

На рис. 4.8 показаны основные фазы установления соединения и его разрыва для протокола PPP.

В табл. 4.1 приведены 11 типов LCP-пакетов, допустимых в кадрах протокола PPP по RFC 1661.

## **4.3. Протоколы множественного доступа**

### **4.3.1. Общие сведения**

Как уже говорилось, существует два вида каналов передачи данных: канал точка — точка и канал с множественным доступом. Канал точка — точка обеспечивает соединение только двух сторон: приемника и передатчика. Проблемы синхронизации доступа здесь не столь сложны. Этот вид каналов передачи характерен для WAN-сетей. В локальных сетях широко применяется другой вид каналов — каналы с множественным доступом. Характерными примерами каналов с множественным доступом являются практически все беспроводные каналы.

Для каналов с множественным доступом ключевым является следующий вопрос: как определить, кому из абонентов, запросивших канал, предоставить право пользоваться им? Для примера представим себе конференцию по телефону, т.е. когда несколько абонентов соединены по схеме каждый с каждым. Возможно, когда говорящий закончит речь, сразу несколько участников конференции захотят высказаться и начнут говорить одновременно. Как же предотвратить хаос?

Протоколы для решения этой проблемы относятся к подуровню канального уровня, который называется подуровнем доступа к среде, или подуровнем канального уровня (MAC — Medium Access Control). Протоколы MAC-подуровня регулируют доступ к каналу при наличии нескольких абонентов. Рассмотрим статическую и динамическую схемы распределения доступа, а также конкретные алгоритмы, реализующие эти схемы.

### **4.3.2. Статические методы доступа к каналу**

При рассмотрении методов множественного доступа к каналу, естественно, возникает идея разделить весь канал на несколько подканалов и каждому потенциальному абоненту предоставить свой подканал. Эта техника называется мультиплексированием, или уплотнением канала. Далее будут подробно рассмотрены вопросы мульти-

плексирования нескольких логических каналов в одном физическом канале. Немного забежав вперед, отметим, что имеется два основных подхода к мультиплексированию: использование частотного (FDM) и временно́го (TDM) разделения канала.

При частотном разделении весь диапазон частот полосы пропускания канала разбивается на поддиапазоны, которые называются подканалами. По каждому подканалу выполняется передача независимо от того, что происходит в других каналах. При временно́м разделении используется вся полоса пропускания канала для каждого абонента, но при этом время передачи делится на слоты по числу потенциальных абонентов, и каждому из них выделяется свой интервал времени (слот) для передачи. Частотное разделение хорошо работает в условиях, когда число абонентов фиксированное и каждый из них обеспечивает плотную загрузку канала. При этом каждому абоненту выделяется своя полоса частот, которую он использует независимо от других.

Однако, когда число пользователей велико, их число изменяется или трафик отдельных абонентов нерегулярный, в FDM появляются проблемы. Например если весь диапазон полосы пропускания разделить на  $N$  полос, а лишь немногим из  $N$  абонентов потребуются доступ к каналу, то бо́льшая часть пропускной способности канала не будет использована. Если число абонентов, которым необходимо передать данные, больше  $N$ , и жестко зафиксировано расписание их доступа к каналу, то часть из них получит отказ из-за недостатка пропускной способности, хотя при этом часть абонентов из тех, кому канал был предоставлен, может ничего не передавать и не принимать.

Таким образом, статическое разделение канала на подканалы является неэффективным решением проблемы доступа при предположении о постоянстве числа абонентов в среднем и нерегулярном трафике у абонентов. Напомним, что трафик в локальных сетях, как правило, носит взрывной характер (пиковые нагрузки от средних могут отличаться в 1 000 раз).

Вывод, к которому мы пришли чисто интуитивно, можно получить теоретически с использованием следующей модели [40]. Пусть необходимо оценить среднее время  $T$  задержки кадра в канале. Предположим, что имеется канал со скоростью передачи  $C$ , бит/с, в котором средняя скорость поступления кадров в секунду равна  $\lambda$ , а средняя длина кадра имеет экспоненциальное распределение со средним значением  $1/\mu$  бит/кадр. Тогда из теории массового обслуживания или, как ее еще называют, теории очередей [12], получим следующее соотношение:

$$T = \frac{1}{\mu C - \lambda}.$$

Разделив канал на  $N$  подканалов со скоростью передачи каждого  $C/N$ , бит/с, получим скорость поступления кадров в каждом из под-

каналов  $\lambda/N$ . Другими словами, что выгоднее иметь  $N$  разных очередей, каждую из которых можно обслуживать медленно, или одну очередь, которую надо обслуживать быстро? Подставив в формулу для  $T$  новые значения скоростей подканалов и поступления кадров, получаем:

$$T_{\text{FDM}} = \frac{1}{\mu(C/N) - (\lambda/N)} = \frac{N}{\mu C - \lambda} = NT.$$

Из этой формулы видно, что при частотном разделении среднее время задержки кадра в канале будет в  $N$  раз больше по сравнению с распределением кадров из единой очереди.

Те же самые рассуждения можно применить и к временному разделению. Если каждому пользователю выделить свой слот и тот его не использует, то это будет пустой тратой пропускной способности канала. Таким образом, ни один из известных статических методов не позволяет эффективно распределять нагрузку, поэтому мы сосредоточимся на динамических методах распределения доступа к каналу.

### 4.3.3. Базовая модель динамического предоставления доступа к каналу

Рассмотрим методы динамического предоставления доступа к каналу. Прежде чем перейти к их описанию сформулируем пять основных предположений, составляющих основу моделей сетей ЭВМ, в которых в качестве СПД используется канал с множественным доступом, и будем использовать эти предположения при оценке динамических методов доступа к каналу [40]:

**1. Станции.** Модель состоит из  $N$  независимых станций (компьютеров, телефонов, факс-машин и т. п.). На каждой станции работает пользователь или программа, генерирующие кадры для передачи. Вероятность появления кадра в интервале времени длиной  $\Delta t$  равна  $\lambda \Delta t$ , где  $\lambda$  — константа и  $0 < \lambda < 1$ . Предполагаем, что если кадр сгенерирован, то станция блокируется, и новый кадр не появится, пока не будет передан первый кадр. Это предположение означает, что станции независимы, и на каждой из них работает только одна программа или один пользователь, генерирующие нагрузку с постоянной скоростью.

**2. Единственность канала.** Канал один и он доступен всем станциям. Все станции равноправны. Они получают кадры и передают кадры только через этот единственный канал. Аппаратные средства всех станций для доступа к каналу одинаковые, но программно можно устанавливать станциям приоритеты.

**3. Коллизии.** Если во время передачи кадра одной станцией другая станция начала передачу своего кадра, то такой случай будем называть коллизией. Предполагаем, что любая станция может обнаружить коллизию и что кадры, разрушенные при коллизии, должны

быть посланы повторно позднее. Кроме коллизий других ошибок передачи нет.

**4. Время.** Возможны две модели времени — непрерывная и дискретная:

- *непрерывное время.* Передача кадра может начаться в любой момент. В сети нет единых часов, которые разбивают время на слоты. Другими словами, время является непрерывной функцией, отображающей интересующие нас действия в сети на множество вещественных чисел;

- *дискретное время.* Все время работы канала разбивается на одинаковые интервалы, называемые слотами. В слоте может оказаться нуль кадров, если это слот ожидания, один кадр, если в этом слоте передача кадра прошла успешно, и несколько кадров, если в этом слоте произошла коллизия.

**5. Доступ к каналу.** Возможны два способа доступа станции к каналу:

- *с обнаружением несущей.* Станция прежде чем использовать канал всегда определяет, занят он или нет с помощью несущей — сигнала определенной формы. Когда канал не занят, по нему все время передается такой сигнал, а если канал занят, то сигнал в нем отличается от несущей, и станция не начинает передачу;

- *при отсутствии несущей.* Станция ничего не знает о состоянии канала, пока не начнет использовать его. Она сразу начинает передачу и лишь в ходе передачи обнаруживает коллизию, так как сигнал, который она «увидит» в канале, будет отличаться от того сигнала, который станция передала в канал.

Существуют и другие модели сетей, которые предусматривают использование многопользовательских станций, но эти модели намного сложнее. Единый канал передачи — это краеугольное предположение, и иного способа передать кадр нет.

Говоря о динамическом доступе, подразумевают, что отсутствует какая-либо фиксированная политика предоставления доступа к каналу для передачи в отличие от статических методов доступа. При этом любая станция может запросить доступ к каналу в любой момент времени, а методы доступа лишь определяют правила удовлетворения этих запросов.

#### **4.3.4. Методы множественного доступа ALOHA**

В 1970-х гг. Н. Абрамсон со своими коллегами из университета Гавайи предложил простой способ распределения доступа к каналу. Систему, реализующую этот способ распределения канала, Н. Абрамсон назвал ALOHA, что по-гавайски означает что-то вроде «привет». Система состояла из наземных радиостанций, работающих на одной частоте и связывающих острова между собой. Идея ее конструкции заключалась в том, чтобы позволить в вещательной среде любому количеству пользователей неконтролируемо использовать один и тот же канал.

Мы здесь рассмотрим два варианта системы: чистая АЛОНА и слотированная АЛОНА, в которой время работы разбито на слоты. Первая система реализует модель с непрерывным временем, вторая — с дискретным. Основное их различие состоит в том, что в первой системе никакой синхронизации пользователей не требуется, а во второй — все пользователи начинают передачу только в определенные моменты времени.

### Чистая АЛОНА

Идея чистой АЛОНА проста: любой пользователь, желающий передать сообщение, сразу пытается это сделать. Благодаря тому, что в вещательной среде у него всегда есть обратная связь, т. е. он может определить, пытался ли кто-то еще передавать сообщение на его частоте, отправитель может установить возникновение конфликта при передаче.

Обратная связь в среде ЛВС происходит практически мгновенно, а вот, например, в системах спутниковой связи задержка сигнала составляет около 270 мс. Заметим, что отправитель при этом должен «слушать» среду передачи до тех пор, пока последний бит его сообщения не достигнет самого отдаленного получателя. Обнаружив конфликт, отправитель ожидает некоторый случайный отрезок времени, после чего повторяет попытку передачи. Интервал времени на ожидание должен быть случайным, иначе конкуренты, повторяя попытки передачи вызовут коллизию снова. Системы, в которых пользователи конкурируют за получение доступа к общему каналу, называются *системами с состязаниями*.

Неважно, когда произошел конфликт, когда первый бит одного кадра «наехал» на последний бит другого кадра или в какой-то иной момент, оба кадра считаются испорченными и должны быть переданы повторно. Контрольная сумма, защищающая данные в кадре, не позволяет различать разные случаи наложения кадров.

Оценим эффективность системы АЛОНА через количество кадров, переданных без коллизий. Для этого воспользуемся ранее сформулированной моделью (см. подразд. 4.3.3).

Назовем *временем кадра* время, необходимое на передачу кадра стандартной фиксированной длины. Обозначим это время  $\tau$ . Предположим, что число пользователей неограничено и все они порождают кадры по закону Пуассона со средним числом  $N$  кадров за  $\tau$ . Это означает, что вероятность события, при котором будет порождено  $n$  кадров за время  $\tau$ , можно записать в виде

$$P[n] = \frac{\lambda^n e^{-\lambda}}{n!},$$

где  $\lambda = N$ .

Поскольку при  $N > 1$  очередь на передачу будет только расти и все кадры будут страдать от коллизий, предположим, что  $0 < N < 1$ . Также предположим, что вероятность за время кадра сделать  $k$  попыток передачи, как новых, так и ранее не переданных из-за коллизий кадров, распределяется по закону Пуассона со средним значением  $G$ . Понятно, что при этом должно выполняться соотношение  $G \geq N$ , иначе очередь будет расти бесконечно. При слабой загрузке ( $N \approx 0$ ) будет мало передач, а следовательно, и коллизий, поэтому  $G \approx N$ . При высокой загрузке должно выполняться соотношение  $G > N$ . При этом пропускная способность канала ( $S$ ) будет равна числу кадров, которые надо передать, умноженному на вероятность успешной передачи. Если обозначить  $P_0$  вероятностью отсутствия коллизий при передаче кадра, то можно записать  $S = GP_0$ .

Рассмотрим внимательно, сколько времени требуется отправителю, чтобы обнаружить коллизию. Пусть он начал передачу в момент времени  $t_0$  и пусть требуется время  $t$ , чтобы кадр достиг самой отдаленной станции. Тогда, если в тот момент, когда кадр почти достиг этой отдаленной станции, она начнет передачу (ведь в системе ALOHA станция сначала передает, а потом слушает), отправитель узнает об этом только через время, равное  $t_0 + 2t$  (рис. 4.9).

Вероятность появления  $k$  кадров при передаче кадра с распределением Пуассона

$$P[k] = \frac{G^k e^{-G}}{k!},$$

поэтому вероятность, что появится 0 кадров, равна  $e^{-G}$ .

За двойное время кадра среднее число кадров равно  $2G$ , откуда

$$P_0 = e^{-2G},$$

а так как  $S = GP_0$ , то пропускная способность канала



Рис. 4.9. Определение времени, требуемого для обнаружения коллизии

$$S = Ge^{-2G}$$

Зависимость между числом попыток передачи  $G$  и пропускной способностью  $S$  чистой системы ALOHA за время кадра показана на рис. 4.10. Максимальная пропускная способность достигается при  $G = 0,5$  при  $S = 1/2e$ , что составляет примерно 18 % номинальной пропускной способности системы. Это означает, что если генерировать кадры со скоростью, большей чем 18 % пропускной способности канала, то очереди переполнятся и система «захлебнется». Результат не очень впечатляющий, но это плата за удобство: каждый передает, когда захочет.

### Слотированная ALOHA

В 1972 г. Л. Робертс (Roberts) предложил модификацию чистой ALOHA [76], в которой все время работы канала разделяется на слоты. Размер слота при этом должен быть равен максимальному времени кадра. Ясно, что такая организация работы канала требует синхронизации. Кто-то, например одна из станций, испускает сигнал начала очередного слота. Поскольку передачу теперь можно начинать не в любой момент, а только по специальному сигналу, то время на обнаружение коллизии сокращается вдвое. Откуда

$$S = Ge^{-G}$$

Как видно из рис. 4.10, максимум пропускной способности слотированной ALOHA наступает при  $G = 1$ , где  $S = 1/e$ , т.е. составляет около 37 %, что вдвое больше, чем у чистой ALOHA.

Рассмотрим, как  $G$  влияет на пропускную способность системы. Для этого подсчитаем вероятность успешной передачи кадра за  $k$  попыток. Так как  $e^{-G}$  — это вероятность отсутствия коллизии при передаче, то вероятность того, что кадр будет передан ровно за  $k$  попыток, можно записать в виде

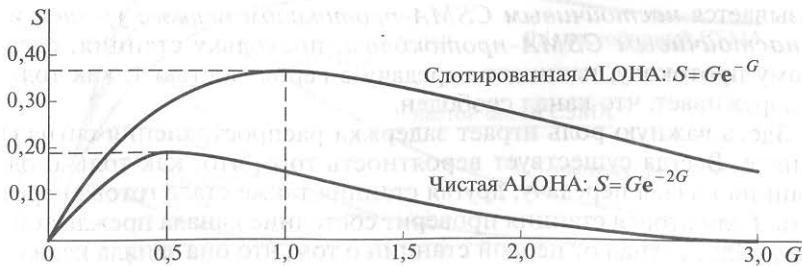


Рис. 4.10. Зависимости между нагрузкой и пропускной способностью чистой и слотированной систем ALOHA

$$P_k = e^{-G}(1 - e^{-G})^{k-1}.$$

Среднее ожидаемое число повторных передач

$$E = \sum_{k=1}^{\infty} kP_k = \sum_{k=1}^{\infty} ke^{-G}(1 - e^{-G})^{k-1} = e^G.$$

Эта экспоненциальная зависимость показывает, что с ростом  $G$  резко возрастает число повторных попыток, поэтому незначительное увеличение загрузки канала ведет к резкому падению его пропускной способности.

#### 4.3.5. Протоколы множественного доступа с обнаружением несущей

Максимальная пропускная способность, которую можно получить для системы АЛОНА, достигается при  $S = 1/e$ . Это неудивительно, так как в этих системах станция не обращает внимания на то, что делают другие, а следовательно, вероятность коллизии чрезвычайно высока. В локальных сетях имеется возможность определения того, что делают другие станции, и только после этого решать, что делать самому.

Протоколы, реализующие идею начала передачи только после определения, занят канал или нет, называются *протоколами с обнаружением несущей* — CSMA (Carrier Sensitive Multiple Access).

##### Настойчивые и ненастойчивые CSMA-протоколы

Рассмотрим протокол, согласно которому станция прежде чем что-либо передавать определяет состояние канала. Если канал занят, то она ждет, а как только он освободился, пытается сразу начать передачу. Если при этом произошла коллизия, станция ожидает случайный промежуток времени и все начинает сначала. Этот протокол называется *настойчивым CSMA-протоколом первого уровня*, или *1-настойчивым CSMA-протоколом*, поскольку станция, следуя этому протоколу, начинает передачу с вероятностью 1, как только обнаруживает, что канал свободен.

Здесь важную роль играет задержка распространения сигнала в канале. Всегда существует вероятность того, что, как только одна станция начала передачу, другая станция также стала готова передавать. Если вторая станция проверит состояние канала прежде чем до нее дойдет сигнал от первой станции о том, что она заняла канал, то вторая станция сочтет канал свободным и начнет передачу. В результате возникает коллизия. Чем больше время задержки сигнала, тем

больше вероятность такого случая и тем хуже производительность канала.

Однако даже если время задержки сигнала будет равно нулю коллизии все равно могут возникать. Например, если во время передачи готовыми к передаче оказались две станции. В этом случае они вежливо подождут, пока ранее начатая передача будет закончена, а затем будут состязаться между собой. Тем не менее этот протокол более эффективен, чем любая из систем ALOHA, так как станция учитывает состояние канала, прежде чем начать действовать.

Другим вариантом CSMA-протокола является *ненастойчивый CSMA-протокол*. Основное отличие его от предыдущего состоит в том, что готовая к передаче станция опрашивает канал. Если канал свободен, то она начинает передачу. Если же канал занят, то она не будет настойчиво его опрашивать в ожидании, когда он освободится, а будет делать это через случайные отрезки времени. Это несколько увеличивает задержку при передаче сигнала для станции, но общая эффективность протокола возрастает.

И, наконец, *настойчивый CSMA-протокол уровня  $p$* , который применяется к слотированным каналам. Когда станция готова к передаче, она опрашивает канал. Если канал он свободен, то она с вероятностью  $p$  передает свой кадр и с вероятностью  $q = 1 - p$  ждет следующего слота. Так станция действует, пока не передаст кадр. Если во время передачи происходит коллизия, станция ожидает случайный промежуток времени и опрашивает канал снова. Если при опросе он опять оказывается занятым, станция ждет начала следующего слота, и весь алгоритм повторяется.

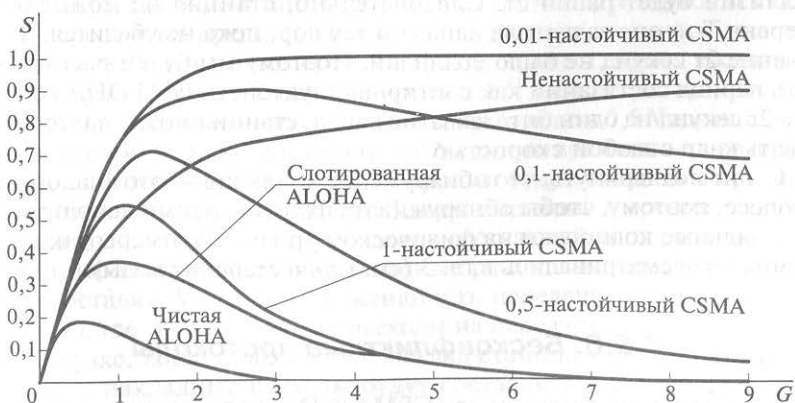


Рис. 4.11. Зависимости пропускной способности протоколов ALOHA и CSMA-протоколов различного уровня настойчивости от нагрузки

На рис. 4.11 показаны зависимости пропускной способности рассмотренных протоколов от нагрузки.

### CSMA-протокол с обнаружением коллизий

Настойчивые и ненастойчивые CSMA-протоколы — несомненное улучшение протокола ALOHA, так как они начинают передачу, только проверив состояние канала. Другое улучшение протокола ALOHA состоит в умении станций определять коллизии как можно раньше, что экономит время и пропускную способность канала. Такой класс протоколов известен как CSMA/CD (Carrier Sense Multiple Access with Collision Detection), т. е. протокол множественного доступа с контролем несущей и обнаружением коллизий.

Протоколы этого класса широко используются в локальных сетях. Модель их работы следующая. В момент времени  $t_0$  одна станция заканчивает передачу очередного кадра, а все другие станции, у которых имеется кадр для передачи, начинают передачу. Естественно, в этом случае происходят коллизии, которые быстро обнаруживаются посредством сравнения отправленного сигнала с тем сигналом, который есть на линии. Обнаружив коллизию, станция сразу прекращает передачу на случайный промежуток времени, после чего все начинается сначала. Таким образом, в работе протокола CSMA/CD можно выделить три стадии: состязания, передачи и ожидания (когда нет кадров для передачи).

Рассмотрим подробнее алгоритм состязаний. Определим, сколько времени станции, начавшей передачу, требуется, чтобы обнаружить коллизию. Обозначим  $\tau$  время распространения сигнала до самой удаленной станции на линии. Для коаксиального кабеля длиной в 1 км  $\tau = 5$  мкс. В этом случае минимальное время для определения коллизии будет равно  $2\tau$ . Следовательно, станция не может быть уверена, что она захватила канал до тех пор, пока не убедится, что в течение  $2\tau$  секунд не было коллизий. Поэтому мы будем рассматривать период состязаний как слотированную систему ALOHA со слотом  $2\tau$  секунд на один бит. Захватив канал, станция может далее передавать кадр с любой скоростью.

Стоит подчеркнуть, что обнаружение коллизий — это аналоговый процесс, поэтому, чтобы обнаруживать их, необходимо использовать специальные кодировки на физическом уровне. Примеры таких кодировок рассматривались в гл. 3 (см. манчестерские коды).

#### 4.3.6. Бесконфликтные протоколы

Хотя коллизии в протоколе CSMA/CD могут возникать только в период состязаний? тем не менее при больших  $\tau$  и коротких кадрах они съедают часть пропускной способности канала. Рассмотрим,

как можно этих коллизий избежать с помощью протоколов класса CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), т. е. протокола множественного доступа с обнаружением несущей и предупреждением коллизий.

Предположим, что имеется  $N$  станций с адресами от 0 до  $N - 1$ . Все адреса уникальны. Требуется определить, кто будет владеть каналом, когда закончится текущая передача.

### Протоколы с резервированием (bit-map protocol)

Идея метода, положенного в основу этой группы протоколов, состоит в следующем: в работе протокола выделяется специальный период состязаний, в котором число слотов равно числу станций, подключенных к каналу. Каждая станция, у которой есть кадр для передачи, проставляет 1 в своем слоте. Поскольку рассматривается канал с множественным доступом (т. е. когда все видят, что проходит в канале), то в конце состязаний все станции знают, кто будет передавать кадры и в каком порядке. Передача происходит в том порядке, в каком пронумерованы слоты. При этом, поскольку станции знают, кто будет передавать и в каком порядке, конфликтов не будет. Если станция опоздала с заявкой на передачу, она должна ждать следующего периода состязаний, который начнется по окончании передач, заявленных на предыдущем периоде состязаний. Протоколы, в которых заявки на передачу откладываются и могут быть сделаны лишь в определенные периоды времени, называются *протоколами с резервированием*.

Теперь рассмотрим производительность этого метода. Пусть  $N$  — число станций. Для удобства будем измерять время в количестве слотов состязаний, а также предположим, что передача одного кадра будет занимать ровно  $d$  таких слотов, а вероятность готовности станции к передаче распределена равномерно для всех станций. Тогда для станции с небольшим номером, например 0 или 1, время ожидания на передачу в среднем будет равняться  $1,5N$  слотов состязаний, так как она, пропустив начало состязаний, будет ждать  $0,5N$  единиц времени в первом периоде состязаний и  $N$  единиц времени — во втором периоде. Станции со старшими номерами будут ожидать в среднем  $N/2$  слотов до начала передачи. Таким образом, в среднем любая станция должна будет ждать  $N$  слотов состязаний до передачи.

При небольшой нагрузке накладные расходы на передачу одного кадра составят  $N$  бит, а эффективность передачи одного кадра —  $d/(d + N)$ , где  $N$  — накладные расходы на передачу кадра. При плотной загрузке, когда практически каждая станция каждый раз что-то посылает, накладные расходы будут составлять 1 бит на кадр, т. е.  $d/(d + 1)$ . Средняя задержка кадра будет равна средней задержке кадра внутри очереди в станции плюс  $N(d + 1)/2$  слотов ожидания, когда кадр достигнет заголовка очереди к каналу. Отсюда видно, что

с ростом  $N$ , хотя накладные расходы на передачу одного кадра падают, задержка кадра в канале существенно возрастает и эффективность падает.

Следует также отметить, что если  $d$  и  $N$  имеет сопоставимые значения, то значительная часть пропускной способности канала будет тратиться на состязания. Кроме того, следует иметь в виду что станции с большими номерами будут иметь в этой схеме преимущество и «оттеснять» станции с меньшими номерами от канала.

### **Протокол двоичного адреса**

Один из недостатков протоколов с резервированием — это затраты на слоты состязаний, составляющие 1 бит на станцию. При коротких кадрах это накладно. Повысить эффективность применения канала можно, используя двоичное представление адреса станции.

В этом методе каждая станция, готовая к передаче, на стадии состязаний выставляет свой адрес бит за битом, начиная со старшего разряда. Эти разряды подвергаются логическому сложению. Если станция выставила на очередном шаге 0, а результат логического сложения 1, то она должна ждать, т.е. в текущих состязаниях она далее участия не принимает. Эффективность использования канала в этом методе составляет  $d/(d + \ln N)$ . Если структура заголовка кадра при этом выбирается таким образом, чтобы его можно было использовать для выбора очередной станции для передачи, то эффективность использования канала достигнет 100 %, поскольку слагаемое  $\ln N$  уходит.

Этот метод, как и предыдущий, имеет один существенный недостаток — он несправедливый: чем больше номер станции, тем скорее она захватит канал. Для устранения этого недостатка была предложена модификация данного метода, в которой у станций динамически изменяется приоритет, т.е. победитель в текущих состязаниях получает наименьший приоритет, который будет увеличиваться от состязания к состязанию.

### **4.3.7. Протоколы с ограниченным числом конфликтов**

Рассмотренные в подразд. 4.3.5 и 4.3.6 протоколы показывают, что при небольшой загрузке возникающие конфликты неопасны ввиду небольшой задержки на передачу. Однако по мере роста нагрузки они снижают эффективность использования канала. Следовательно, при высокой загрузке канала арбитраж желателен и протоколы без коллизий предпочтительнее, а вот при низкой загрузке он лишь вызывает дополнительные накладные расходы.

Естественной была попытка создать протокол, объединяющий достоинства этих двух групп методов, т. е. обеспечить возможность использования состязаний при небольших нагрузках и бесконфликтных методов — при высоких. Такие протоколы были созданы, и называются они *протоколами с ограниченным числом конфликтов*. Их изучением мы и закончим рассмотрение класса протоколов с контролем несущей.

### Симметричные протоколы с ограниченным числом состязаний

До сих пор рассматривались протоколы с состязаниями только в так называемой симметричной конфигурации: все станции, пытающиеся передать кадр, получали канал с одной и той же вероятностью  $p$ . Однако оказывается, что общую производительность системы можно улучшить, если разные станции будут получать канал с разной вероятностью.

Рассмотрим производительность системы при симметричной конфигурации. Пусть имеется  $k$  станций, каждая из которых с вероятностью  $p$  готова передать кадр. В этом случае вероятность, что какая-то станция успешно передаст свой кадр, равна  $kp(1-p)^{k-1}$ , и эта вероятность достигает максимума при  $p = 1/k$ . Тогда вероятность передачи сообщения какой-либо станцией равна  $((k-1)/k)^{k-1}$ . График этой функции показан на рис. 4.12.

При небольшом числе станций шансы передать кадр достаточно велики, но с ростом числа станций эти шансы резко падают. Единственным способом увеличить шансы на передачу является сокращение числа конфликтов. Для этого в протоколах с ограниченным числом состязаний все станции разбивают на непересекающиеся группы. Каждой группе присваивается номер. За слот с номером 0 состязаются только станции из группы 0. Если передавать в этой группе нечего или была коллизия, то начинаются состязания за слот

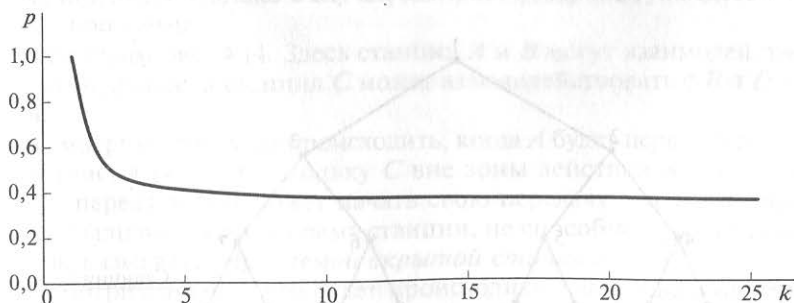


Рис. 4.12. Зависимость вероятности  $p$  успешной передачи сообщения от числа  $k$  станций в симметричной конфигурации

1 между членами группы 1 и т.д. В результате в каждом слоте конкуренция падает, что соответствует левой части кривой, показанной на рис. 4.12. Основную сложность в этом методе представляет распределение станций по группам.

### Адаптивный древовидный протокол

Данный протокол, конкретизирующий способ распределения станций по группам, устроен по принципу дихотомии и позволяет эффективно находить оптимальное число станций в группе.

Рис. 4.13 иллюстрирует этот принцип применительно к станциям (листьям). За слот 0 борются все станции. Если какая-то из них победила — хорошо, а если нет, то за слот 1 борются только станции поддерева с корнем в вершине 2. Если какая-то из них победила, то следующий слот резервируется для станций поддерева с корнем в вершине 3. Если какая-то из них победила, то за следующий слот борются станции поддерева с корнем в вершине 4, и т.д.

Когда число станций велико и все они готовы передавать, то вряд ли целесообразно начинать поиск с уровня 0 дерева. Следовательно, возникает вопрос, с какого уровня надо начинать эту процедуру при заданном числе станций? Перенумеруем уровни дерева: на уровне 0 — вершина 1, на уровне 1 — вершины 2 и 3 и т.д. Заметим, что на уровне  $i$  располагается  $2^i$  вершин, т.е. число станций, являющихся листьями в поддерева с корнем на уровне  $i$  равно  $N/2^i$ .

Пусть число станций, готовых к передаче, нормально распределено. Обозначим это число  $q$ . Тогда число станций, готовых к передаче и расположенных ниже узла уровня  $i$ , будет равно  $2^{-i}q$ . Заметим, что доля станций от общего числа станций, входящих в поддерево с корнем на уровне  $i$ , равна  $2^{-i}$ . Естественно, необходимо подобрать такое соотношение между  $i$  и  $q$ , при котором число конкурирующих станций будет равно 1, т.е. будет выполняться условие  $2^{-i}q = 1$ , или  $\log_2 q = i$ .

Рассмотренный алгоритм имеет много вариантов [59]. Мы описали лишь основную идею.

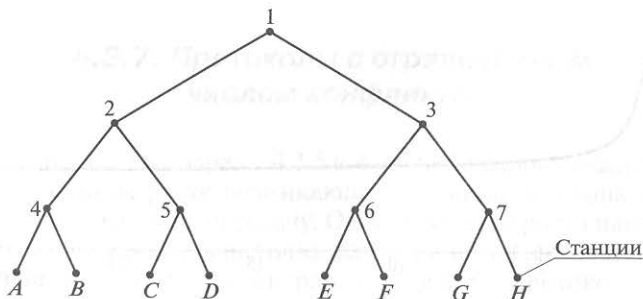


Рис. 4.13. Дерево состязаний для восьми станций

### 4.3.8. Множественный доступ к беспроводным каналам

Беспроводная связь в настоящее время активно развивается, и все чаще можно встретить локальные сети, построенные на беспроводных каналах, например WiFi. К этой же группе систем связи относятся сотовая и спутниковая связь. Так как количество абонентов этих систем достаточно велико, для управления доступом к беспроводному каналу придумано много методов, часть из которых мы и рассмотрим.

#### Методы MACA для беспроводных локальных сетей

В беспроводных локальных сетях абонентскими устройствами являются мобильные компьютеры. Чтобы быть по-настоящему мобильным, компьютер использует радиоканал для связи. Локальные сети, построенные на основе радиоканала, существенно отличаются от кабельных локальных сетей: они имеют специальный MAC-подуровень.

Обычная конфигурация таких сетей следующая: в здании размещается сеть стационарных приемопередающих станций, соединенных кабелем. Вспомним системы WiFi (см. разд. 3.4.6). Если настроить приемопередатчики станций и компьютеров на расстояние 3...4 м, то каждая комната в здании образует ячейку. В каждой ячейке действует только один канал, пропускная способность которого обычно равна 1...2 Мбит/с и которую разделяют все машины этой ячейки.

Далее предположим ради простоты изложения, что все передатчики работают на одной и той же частоте. Когда приемник оказывается в зоне действия двух активных передатчиков, то он принимает искаженный сигнал, который рассматривается как бесполезный шум.

Естественно было бы попытаться использовать протокол CSMA для радиоканала. Однако в случае беспроводного доступа здесь возникают проблемы.

Рассмотрим рис. 4.14. Здесь станции  $A$  и  $B$  могут взаимодействовать друг с другом, а станция  $C$  может взаимодействовать с  $B$  и  $D$ , но не с  $A$ .

Рассмотрим, что будет происходить, когда  $A$  будет передавать данные  $B$  (рис. 4.14, *а*). Поскольку  $C$  вне зоны действия  $A$ , то она не слышит передачи  $A$  и может начать свою передачу для  $B$ , что приведет к коллизии. Эта проблема станции, не способной увидеть конкурента, называется *проблемой скрытой станции*.

Рассмотрим теперь, что будет происходить, если  $B$  начнет передавать, например  $A$  (рис. 4.14, *б*). Тогда  $C$  услышит эту передачу и ложно заключит, что она не может передавать данные  $D$ , хотя та свободна. Эта ситуация называется *проблемой мнимой станции*.

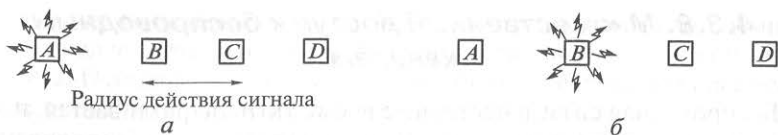


Рис. 4.14. Два случая передачи (а, б) в беспроводной локальной сети

Итак, все сводится к тому, как узнать, идет ли реальная передача тому абоненту, которому надо передать сообщение. В силу ограниченности диапазона действия каждого передатчика протокол CSMA здесь не подходит.

Первые протоколы, разработанные специально для беспроводных сетей, относились к протоколам множественного доступа с предотвращением коллизий — MACA (Multiple Access Collision Avoidance), идея которых заключалась в том, что отправитель должен принудить получателя послать короткое сообщение перед началом передачи. Тогда все станции, находящиеся в зоне действия получателя, услышав этот сигнал, не начнут передачу.

Действие протокола иллюстрирует рис. 4.15.

Рассмотрим, как станция *A* теперь передает сообщение станции *B*. Передача начинается со специального сообщения RTS (Request To Send). Это короткое сообщение (30 байт) несет информацию о настоящем сообщении (например, о его длине). Станция *B* в ответ шлет сообщение CLS (Clear To Send). В этом сообщении повторяются данные о сообщении, которое последует. Получив сообщение CTS, станция *A* начинает передачу.

Теперь рассмотрим, как другие станции реагируют на RTS- и CTS-сообщения. Станции, близко расположенные к *A*, слышат RTS-сообщение и знают, что надо хранить молчание, чтобы сообщение *A*

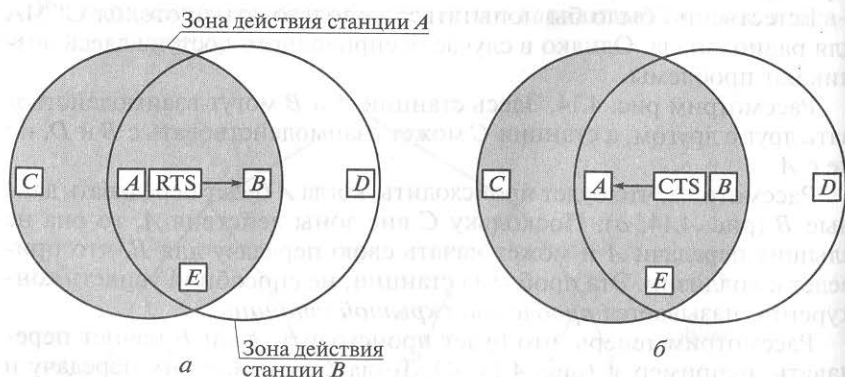


Рис. 4.15. Схема действия протокола MACA

было передано. Станции, близко расположенные к  $B$ , слышат CTS-сообщение и не станут инициировать передачу для  $B$ .

Однако, несмотря на все эти предосторожности, коллизии все-таки могут случаться. Например, если две станции в одно и то же время пошлют RTS-сообщения. Эти сообщения будут конфликтовать, поэтому никакой реакции на них не поступит. Станции переждут некоторый случайный промежуток времени и повторяют попытку. Подробно алгоритмы разрешения подобных конфликтов рассматриваются при изучении стандарта IEEE 802.3.

В подразд. 4.4.2 подробно рассматривается канальный уровень в беспроводных локальных сетях 802.11 (WiFi).

### **Метод множественного доступа на основе разделения кодов**

Для многих систем беспроводной связи характерно использование методов множественного доступа FDM, TDM, ALOHA и их комбинаций. Однако такие системы имеют существенные недостатки: ни один из пользователей этих систем не может использовать всю полосу пропускания, предоставленную системе. Если при этом принять в расчет сужение полосы пропускания из-за проблем на границе сот, падение мощности сигналов от мобильных терминалов в пограничных сотовых зонах, накладные расходы на шифрование в целях безопасности, то становится ясно, что высокую скорость передачи в такой системе получить непросто.

Метод множественного доступа на основе разделения кодов — CDMA (Code Division Multiple Access) основан на принципиально иной идее: каждый участник связи может использовать всю полосу пропускания канала в соте за счет применения метода прямого расширения спектра передачи подобно WiFi (см. подразд. 3.4.6). Если точнее, то сначала этот метод был предложен в рамках CDMA, а уже затем был использован в WiFi.

В CDMA-системе каждый бит сообщения кодируется последовательностью из  $m$  частиц (чипов). Бит со значением 0 передается инвертированной последовательностью частиц, а бит со значением 1 — прямой. Каждой мобильной станции присваивается уникальный код — последовательность частиц для 0 и для 1. Другими словами, у каждого участника этой системы свой уникальный «язык», поэтому все могут говорить сразу. Понимать друг друга будут только те, кто говорит на одном языке.

Ясно, что такая техника возможна, только если при увеличении объема передаваемой информации будет пропорционально увеличиваться ширина полосы пропускания. При использовании техники FDM канал, равный 1 МГц, можно разделить на 100 подканалов по 10 кГц каждый, и осуществлять передачу по этим подканалам со ско-

ростью 10 Кбит/с (1 бит на 1 Гц). В случае применения CDMA каждый может использовать всю полосу пропускания — 1 МГц, т.е. если использовать 10-разрядные последовательности частиц (что предполагает  $2^{10}$  разных последовательностей), можно передавать данные со скоростью 100 Кбит/с.

Кроме того, поскольку каждая станция имеет уникальную последовательность частиц, не требуется дополнительного шифрования. Из сказанного ясно преимущество CDMA-системы по сравнению с TDM- и FDM-техниками.

Идея уникальности последовательности частиц для каждой станции основана на ортогональных кодах. Суть этих кодов состоит в следующем: если рассмотреть последовательности частиц для станции как векторы  $S$  и  $T$  соответственно, то можно записать

$$(S, T) = \frac{1}{m} \sum_{i=1}^m S_i T_i = 0.$$

На рис. 4.16 приведен пример, поясняющий механизм работы ортогональных последовательностей. На рис. 4.16, *a* приведены кодовые последовательности частиц для 1 станций  $A, B, C, D$ , которые все ортогональны. На рис. 4.16, *б* показаны наборы сигналов, которые

A: 00011011	A: (-1 -1 -1 +1 +1 -1 +1 +1)
B: 00101110	B: (-1 -1 +1 -1 +1 +1 -1 -1)
C: 01011100	C: (-1 +1 -1 +1 +1 +1 -1 -1)
D: 01000010	D: (-1 +1 -1 -1 -1 -1 +1 -1)

*a*

*б*

--1- C	$S_1 = (-1 +1 -1 +1 +1 +1 -1 -1)$
-11- B+C	$S_2 = (-2 \ 0 \ 0 \ 0 +2 +2 \ 0 -2)$
10-- A+B	$S_3 = (0 \ 0 -2 +2 \ 0 -2 \ 0 +2)$
101- A+B+C	$S_4 = (-1 +1 -3 +3 -1 -1 -1 +1)$
1111 A+B+C+D	$S_5 = (-4 \ 0 -2 \ 0 +2 \ 0 +2 -2)$
1101 A+B+C+D	$S_6 = (-2 -2 \ 0 -2 \ 0 -2 +4 \ 0)$

*в*

$$\begin{aligned}
 S_1 \cdot C &= (1+1+1+1+1+1+1+1)/8=1 \\
 S_2 \cdot C &= (2+0+0+0+2+2+0+2)/8=1 \\
 S_3 \cdot C &= (0+0+2+2+0-2+0-2)/8=0 \\
 S_4 \cdot C &= (1+1+3+3+1-1+1-1)/8=1 \\
 S_5 \cdot C &= (4+0+2+0+2+0-2+2)/8=1 \\
 S_6 \cdot C &= (2-2+0-2+0-2+4+0)/8=-1
 \end{aligned}$$

*г*

Рис. 4.16. Пример, поясняющий метод ортогональных последовательностей:

*a, б* — коды для 0 и 1 соответственно станций  $A \dots D$ ; *в* — результирующий сигнал при различных комбинациях передач разных станций; *г* — сигнал, выделенный станцией  $C$  из комбинаций, показанных на рис. 4.16, *в*

ми передаются кодовые последовательности частиц. На рис. 4.16, *в* приведены результирующие наборы сигналов, возникающие при одновременной передаче станциями в разных комбинациях. На рис. 4.16, *г* показано, как приемник, знающий кодовую последовательность частиц для станции *C*, может выделить из результирующего набора сигналов, образуемого сигналами от нескольких станций, бит, передаваемый станцией *C*.

Реализация этого элегантного метода потребовала решения целого ряда сложных технических проблем: синхронизация передачи кодовых последовательностей частиц разными станциями; регулирования уровня мощности сигналов в полосе каждой частицы; определения способа, как получатель узнает последовательность частиц отправителя.

Здесь мы не будем заниматься этими вопросами, так как они уведут нас в сторону от вопросов канального уровня. Тем, кого заинтересовал этот метод, рекомендуется почитать [77].

## **4.4. Канальный уровень стандарта IEEE 802 для локальных и муниципальных сетей**

### **4.4.1. Стандарт IEEE 802.3 и Ethernet**

Перейдем от изучения абстрактных протоколов к рассмотрению конкретных стандартов, применяемых в каналах с множественным доступом. Большинство стандартов для локальных сетей сконцентрированы в документе IEEE 802, который разделен на части:

IEEE 802.1 содержит введение в стандарты и описание примитивов;

IEEE 802.2 описывает протокол LLC (Logical Link Control — управление логическим каналом), который является верхней частью канального протокола;

IEEE 802.3х описывают протоколы CSMA/CD для локальных сетей, известные как Ethernet, Fast Ethernet и Gigabit Ethernet.

К этому же семейству протоколов относятся WiFi и WiMax, а также 802.4 — шина с маркером и 802.5 — кольцо с маркером.

Стандарты 802.4 и 802.5 здесь не рассматриваются. Их описание можно посмотреть, например в [40]. Однако в подразд. 5.2 будет рассмотрена технология FDDI, построенная на стандартах, являющихся развитием IEEE802.4 и IEEE802.5.

Стандарт IEEE 802.3 относится к 1-настойчивым протоколам CSMA/CD. Напомним, что прежде чем начать передачу, станция, использующая такой протокол, опрашивает канал. Если канал занят, то станция ждет и как только он освободится, сразу начинает передачу. Если несколько станций одновременно начали передачу, то

возникает коллизия и передача тут же прекращается. Станции ожидают некоторый случайный промежуток времени, и все начинается сначала.

### Протокол IEEE 802.3 MAC-подуровня

Структура кадра в IEEE 802.3 показана на рис. 4.17. Кадр начинается с преамбулы — 7 байт вида 10101010, которая в манчестерском коде на скорости 10 МГц обеспечивает интервал времени 5,6 мкс для синхронизации приемника и передатчика. Затем следует стартовый байт 10101011, обозначающий начало передачи.

Хотя стандарт IEEE 802.3 допускает двух- и шестибайтовые адреса назначения, для 10Base используются только шестибайтовые. Ноль в старшем бите адреса получателя указывает на обычный адрес, а единица — это признак группового адреса. Групповой адрес позволяет обращаться сразу к нескольким станциям одновременно. Адрес получателя, состоящий из одних единиц, — это вещательный адрес, т. е. этот кадр должен получить все станции в сети.

Адресация обеспечивает также возможность различения локального и глобального адресов. На то, какой адрес используется, указывает 46-й бит. Если этот бит равен 1 — это локальный адрес, который устанавливает сетевой администратор, и вне данной СПД этот адрес смысла не имеет. Глобальный адрес устанавливает IEEE, гарантируя при этом, что нигде в мире нет второго такого адреса. С помощью 46 бит можно получить  $7 \cdot 10^{13}$  глобальных адресов.

Поле данных в кадре может занимать от 0 до 1 500 байт. Поле данных длиной 0 создает проблему для обнаружения коллизий, поэтому IEEE 802.3 предписывает, что кадр не может быть короче 64 байт. Если длина поля данных недостаточна, то поле *Заполнение* компенсирует нехватку длины. Этот прием называется расширением носителя.

Ограничение длины кадра связано со следующей проблемой. Если кадр короткий, то станция может закончить передачу прежде чем начало этого кадра достигнет самого отдаленного получателя. В этом случае станция может пропустить коллизию, ошибочно считая, что кадр доставлен благополучно (см. подразд. 3.3). В IEEE 802.3 (при 2,5 км и четырех репитерах) минимальное время обнаружения коллизии равно 51,2 мкс, что соответствует 64 байт. При больших скоростях передачи длина кадра должна быть еще больше. Например, при

Байты	7	1	2 или 6	2 или 6	2	0 ... 1500	0 ... 46	4
	Преамбула	Стартовый байт	Адрес назначения	Адрес источника	Длина поля данных	Данные	Заполнение	Контрольная сумма

Рис. 4.17. Структура кадра в IEEE 802.3

скорости 1 Гбит и длине сегмента 2,5 км она должна будет равна 6 400 байт.

Последнее поле в структуре кадра — это контрольная сумма, которая формируется с помощью CRC-кода (см. подразд. 3.1.7).

### Двоичный экспоненциальный алгоритм задержки

Теперь рассмотрим, как определяется случайная задержка при возникновении коллизий. На этапе состязаний время разбивается на слоты длиной, соответствующей удвоенному времени распространения сигнала до самой удаленной станции ( $2\tau$ ). В IEEE 802.3, как уже указывалось, это время равно 51,2 мкс.

При первой коллизии станции, участвовавшие в ней, случайно выбирают 0 или 1 слот для ожидания. Если они выберут одно и то же число, то коллизия возникнет снова. Тогда выбор будет происходить среди чисел  $0, 2^i, 1$ , где  $i$  — порядковый номер очередной коллизии.

После 10 коллизий число слотов достигает 1 023 и далее не увеличивается. После 16 коллизий Ethernet-контроллер фиксирует ошибку и сообщает о ней более высокому уровню стека протоколов.

Этот алгоритм, называемый *алгоритмом двоичной экспоненциальной задержки*, позволяет динамически подстраиваться под число конкурирующих станций. Если для каждой коллизии случайный интервал составлял 1 023, то вероятность повторной коллизии для двух станций была бы пренебрежимо мала, однако среднее время ожидания разрешения коллизии в этом случае равнялось бы сотням слотов. Если бы случайный интервал составлял постоянно 0 или 1, то при наличии 100 станций разрешение коллизии потребовало бы годы, так как в этом случае 99 станций должны были бы случайно выбрать, например 0, и лишь одна — 1.

### Производительность протоколов по стандарту IEEE 802.3

Рассмотрим производительность протоколов стандарта IEEE 802.3 при условии плотной и постоянной нагрузки. Пусть имеется  $k$  станций, всегда готовых к передаче. В целях упрощения анализа при коллизиях будем рассматривать не алгоритм двоичной экспоненциальной задержки, а постоянную вероятность повторной передачи в каждом слоте. Если каждая станция участвует в состязаниях в слоте с вероятностью  $p$ , то вероятность того, что некоторая станция захватит канал в этом слоте

$$A = kp(1 - p)^{k-1}.$$

Вероятность  $A$  достигает максимума при  $p = 1/k$ ;  $A \rightarrow 1/e$  при  $k \rightarrow \infty$ . Вероятность того, что период состязаний будет составлять  $j$  слотов,

равна  $A(1 - A)^{j-1}$ , откуда среднее число слотов в состязаниях определяется в виде

$$\sum_{j=0}^{\infty} jA(1 - A)^{j-1} = \frac{1}{A}.$$

Так как каждый слот имеет длительность  $2\tau$ , то средний интервал состязаний  $w = 2\tau/A$ . При  $p = 1/k$  средний интервал состязаний  $w \leq 2\tau e$ , что примерно равно  $5,4\tau$ . Если передача кадра средней длины занимает  $m$  секунд, то при условии работы большого числа станций, постоянно имеющих кадры для передачи, эффективность канала равна  $m/(m + 2\tau/A)$ .

Из этой формулы видно, что чем длиннее кабель, т.е. больше  $\tau$ , тем хуже эффективность канала, так как растет длительность периода состязаний. При  $\tau = 51,2$  мкс, что соответствует 2,5 км при четырех репитерах и скорости передачи 10 Мбит/с, минимальный размер кадра составляет 512 бит, или 64 байт. Хотя с ростом длины кадра эффективность канала растет, время задержки кадра в системе также увеличивается.

### Уровень MAC в Fast Ethernet

Как уже говорилось в гл. 3, под термином Fast Ethernet понимают набор спецификаций IEEE 802.3u для недорогого стандарта, совместимого с Ethernet IEEE 802.3 и способного обеспечить работу ЛВС со скоростью 100 Мбит/с, т.е. обеспечить:

- десятикратное увеличение пропускной способности сегментов сети;
- сохранение метода случайного доступа CSMA/CD, принятого в Ethernet 802.3;
- сохранение формата кадра, принятого в Ethernet 802.3;
- поддержка традиционных сред передачи данных — витой пары и волоконно-оптического кабеля.

Кроме того, важной функцией этого стандарта является поддержка двух скоростей передачи 10/100 Мбит/с, а также обеспечение автоматического выбора одной из функций, встраиваемых в сетевые карты и коммутаторы Fast Ethernet. Все это позволяет осуществлять плавный переход от сетей Ethernet к более скоростным сетям Fast Ethernet, обеспечивая выгодную преємственность по сравнению с другими технологиями. Еще один положительный фактор — низкая стоимость оборудования Fast Ethernet. В стандарте 802.3u изменения коснулись в основном физического уровня, а MAC-подуровень остался прежним.

### Подуровень MAC в Gigabit Ethernet

На подуровне MAC стандарта Gigabit Ethernet используется тот же самый протокол передачи CSMA/CD, что и в стандартах Ethernet и

Fast Ethernet. В стандарте Ethernet IEEE 802.3 принят минимальный размер кадра, равный 64 байт. Как уже неоднократно отмечалось, именно значение минимального размера кадра определяет максимально допустимое расстояние между самыми удаленными станциями в сегменте сети. Время, за которое станция передает такой кадр (время кадра), равно 51,2 мкс. Максимальная длина сегмента Ethernet определяется из условия разрешения коллизий, т. е. время, за которое сигнал доходит до удаленного узла и возвращается обратно, не должно превышать 51,2 мкс (без учета преамбулы).

При переходе от Ethernet к Fast Ethernet скорость передачи возрастает, а время передачи кадра длиной 64 байт соответственно сокращается до 5,12 мкс. Чтобы можно было обнаруживать все коллизии до конца передачи кадра, как и раньше, необходимо выполнить одно из следующих условий:

- сохранить прежнюю максимальную длину сегмента, но увеличить время кадра (и, следовательно, увеличить минимальную длину кадра);
- сохранить время кадра (т. е. прежний размер кадра), но уменьшить максимальную длину сегмента.

В Fast Ethernet был оставлен такой же минимальный размер кадра, как в Ethernet, в результате чего была достигнута совместимость, но значительно сократился максимальный размер сегмента.

Опять же в силу преимущественности стандарт Gigabit Ethernet должен был поддерживать те же минимальный и максимальный размеры кадра, которые приняты в Ethernet и Fast Ethernet. Однако поскольку скорость передачи возросла, то соответственно уменьшалось время передачи пакета аналогичной длины, что при сохранении прежней минимальной длины кадра привело бы к уменьшению максимальной длины сегмента сети до 20 м, что было бы мало полезным. Поэтому при разработке стандарта Gigabit Ethernet было принято решение об увеличении времени кадра, но, чтобы поддержать совместимость со

Преамбула SFD	DA	SA	L или T	Данные	FCS	Расширение носителя
7+1 байт	6 байт	6 байт	2	46 ... 1500 байт	4 байт	

Рис. 4.18. Формат кадра Gigabit Ethernet с полем расширения носителя:

SFD (Start of Frame Delimiter) — ограничитель начала кадров; DA (Destination Address) — адрес назначения; SA (Source Address) — адрес источника;  $L$  — длина поля данных (для кадра 802.3);  $T$  — тип поля данных (для кадра Ethernet в WiFi); FCS (Frame Check Sequence) — контрольная последовательность кадра

стандартами Ethernet и Fast Ethernet, минимальный размер кадра не был увеличен, а к кадру было добавлено дополнительное поле, получившее название *расширение носителя*. Содержимое этого поля обычно не несет служебной информации.

Если станции требуется передать короткий (меньше 512 байт) кадр, то при передаче к нему добавляется поле расширения носителя, дополняющее кадр до 512 байт. Поле контрольной суммы вычисляется только для оригинального кадра и не распространяется на поле расширения носителя. При приеме кадра это поле отбрасывается, поэтому уровень LLC даже и не знает о наличии такого поля. Если размер кадра равен или превосходит 512 байт, то поле расширения носителя не добавляется.

На рис. 4.18 показан формат кадра Gigabit Ethernet при использовании расширения носителя.

#### **4.4.2. Канальный уровень в сетях IEEE 802.11**

Рассмотрим уровень канала данных в сетях IEEE 802.11 (WiFi), физическая организация которых уже рассматривалась в подразд. 3.4.7.

Минимально сеть WiFi может содержать всего два устройства, например две рабочие станции или два ноутбука. В этом случае организуется *выделенная* (ad hoc) сеть, в которую входят беспроводные интерфейсы указанных устройств. Данное соединение можно сравнить с соединением типа точка—точка в проводной связи. Однако соединение WiFi имеет следующие существенные недостатки: во-первых, безопасность передачи данных в таком соединении минимальна; во-вторых, зачастую беспроводные интерфейсы разных производителей несовместимы друг с другом в режиме ad hoc.

Для решения задачи совместимости в сети устанавливается выделенный узел — точка доступа, представляющая собой устройство, которое имеет проводной интерфейс для подключения к проводной сети и доступа во внешний мир, а также антенну, образующую вокруг себя зону покрытия точки доступа. В зависимости от того, где установлена точка доступа, а также от того, каковы мощность и размер ее антенны, размер зоны покрытия может сильно различаться. Обычно радиус зоны покрытия точки доступа составляет от 90 до 150 м. Для обслуживания больших площадей устанавливают несколько точек доступа с перекрывающимися зонами покрытия. Перекрывание этих зон позволяет организовать прозрачное перемещение абонентских устройств в пределах общей зоны покрытия (по такому же принципу строятся сети сотовой связи). Размер зоны перекрывания не установлен в стандарте, но обычно он составляет 20...30 %.

Когда абонентское устройство включается внутри зоны покрытия беспроводной сети, оно начинает прослушивать эфир в поисках совместимого устройства, с которым оно могло бы взаимодействовать.

Этот этап называется *сканированием*, которое может быть активным или пассивным.

При активном сканировании генерируется широковещательный запрос от абонентского устройства, обязательно включающий в себя идентификатор сети, к которой он хочет присоединиться (Service Set Identifier — SSID). Когда запрос достигает точки доступа, имеющей запрашиваемый идентификатор сети, эта сеть генерирует ответ на запрос.

При пассивном сканировании абонентское устройство слушает эфир и ожидает появления кадров-маяков, которые периодически рассылаются точками доступа или интерфейсами других узлов, находящимися в режиме ad hoc. Когда абонентское устройство получает кадр-маяк, в котором указан идентификатор сети SSID, оно пытается присоединиться к указанной сети. Пассивное сканирование — это постоянный процесс, в котором узлы могут присоединяться к точке доступа или отсоединяться по мере изменения мощности радиосигнала.

После присоединения узла к беспроводной сети он может отправлять и принимать кадры точно так же, как в стандарте IEEE 802.3. Беспроводные стандарты семейства 802.11 используют формат кадра, отличный от Ethernet. В WiFi определены три типа кадров: контрольные, управляющие и кадры данных. Формат кадров данных здесь аналогичен формату кадра в Ethernet. Размер поля данных в WiFi, как и в стандарте 802.3, равен 1 500 байт. В то же время тогда как размер кадра в Ethernet не может превышать 1 518 байт, максимальный размер кадра в WiFi составляет 2 346 байт. Как правило, размер кадра в беспроводной сети ограничивается значением 1 518 байт для облегчения передачи кадров между сегментами проводной и беспроводной сетей.

Так как радиоканал является средой множественного доступа, в нем могут происходить коллизии, как и в проводной Ethernet. Основное отличие между ними заключается в том, что в беспроводной сети источник никак не может определить возникновение коллизии. Для разрешения коллизий в беспроводной сети используется метод множественного доступа с обнаружением несущей и предупреждением коллизий (Carrier Sense Multiple Access/Collision Avoidance — CSMA/CA, в котором узел-источник отправляет кадр, узел-получатель отвечает кадром с подтверждением (ACK). В худшем случае такой метод разрешения коллизий может занять до 50 % всей пропускной способности канала. С учетом накладных расходов на протокол предупреждения коллизий реальная скорость передачи данных в канале 802.11b с пропускной способностью 11 Мбит не превышает 5...5,5 Мбит/с.

На производительность сети влияют уровень сигнала и падение качества сигнала с увеличением расстояния, а также помехи. При ослаблении сигнала на источнике включается метод адаптивного

управления скоростью (Adaptive Rate Selection — ARS), который будет последовательно снижать скорость передачи с 11 до 5,5 Мбит/с, с 5,5 до 2 Мбит/с и с 2 до 1 Мбит/с.

## **4.5. Стандарт IEEE 802.2: управление логическим каналом**

### **4.5.1. Общие сведения**

Основное назначение протокола LLC (стандарт 802.2) — обеспечение требуемого качества услуг системы передачи данных посредством передачи своих кадров либо дейтаграммным способом, либо с помощью процедур с установлением соединения и восстановлением кадров, а также обеспечение независимости вышерасположенных уровней стека протоколов от конкретного типа физической среды канала с множественным доступом.

Рассмотрим протокол LLC, следуя [21]. Этот протокол занимает уровень между сетевыми протоколами и протоколами уровня MAC. Протоколы сетевого уровня передают через межуровневый интерфейс данные для протокола LLC: свой пакет (например, пакет IP, IPX или NetBEUI), адресную информацию об узле назначения, а также требования к качеству транспортных услуг, которое протокол LLC должен обеспечить. Протокол LLC помещает пакет протокола верхнего уровня в свой кадр, который дополняется необходимыми служебными полями. Далее через межуровневый интерфейс протокол LLC передает свой кадр вместе с адресной информацией об узле назначения соответствующему протоколу уровня MAC, который упаковывает кадр LLC в свой кадр (например, кадр Ethernet).

В основу протокола LLC положен протокол HDLC (см. подразд. 4.2.8). Спецификация IEEE 802.2 несколько отличается от стандарта HDLC. Сначала подуровень LLC в технологиях фирм-изготовителей сетевого оборудования не выделялся в самостоятельный подуровень, и его функции растворялись в общих функциях протокола канального уровня. Из-за больших различий в функциях протоколов фирменных технологий, которые можно отнести к уровню LLC, на этом уровне пришлось ввести три типа процедур. Протокол сетевого уровня может обращаться к одной из этих процедур.

### **4.5.2. Три типа процедур уровня LLC**

В соответствии со стандартом 802.2 уровень управления логическим каналом LLC предоставляет верхним уровням три типа процедур:

- LLC1 — процедура без установления соединения и без подтверждения;

- LLC2 — процедура с установлением соединения и подтверждением;
- LLC3 — процедура без установления соединения, но с подтверждением.

Этот набор процедур является общим для всех методов доступа к среде, определенных стандартами 802.3...802.5.

*Процедура без установления соединения и без подтверждения (LLC1)* позволяет пользователю передавать данные с минимальными издержками благодаря дейтаграммному режиму работы. Обычно процедуры этого типа используются, когда такие функции, как восстановление данных после ошибок и упорядочивание данных, выполняются протоколами вышерасположенных уровней, поэтому не требуется дублировать их на уровне LLC.

*Процедура с установлением соединения и подтверждением (LLC2)* обеспечивает пользователю возможность установки логического соединения перед началом передачи любого блока данных, а также, если это требуется, позволяет выполнить процедуры восстановления после ошибок и упорядочивание потока этих блоков в рамках установленного соединения. Протокол LLC2 во многом аналогичен протоколам семейства HDLC (LAP-B, LAP-D, LAP-F, которые рассматриваются в гл. 5), применяемым в глобальных сетях для обеспечения надежной передачи кадров на зашумленных линиях. Протокол LLC2 работает в режиме скользящего окна.

В некоторых случаях (например, при использовании сетей в системах реального времени управляющих промышленными объектами), когда временные издержки установления логического соединения перед отправкой данных неприемлемы, а подтверждение о корректности приема переданных данных необходимо, базовая процедура без установления соединения и без подтверждения не подходит. Для таких случаев предусмотрена дополнительная процедура, т.е. *процедура без установления соединения, но с подтверждением (LLC3)*.

Выбор одного из трех режимов работы уровня LLC зависит от стратегии разработчиков конкретного стека протоколов. Например, в стеке TCP/IP уровень LLC всегда работает в режиме LLC1, выполняя простую работу извлечения из кадра и демультимплексирования пакетов различных протоколов — IP, ARP, RARP (которые рассматриваются во втором томе данного учебника).

### **4.5.3. Структура кадров LLC. Процедура с восстановлением кадров LLC2**

Подобно протоколу HDLC все кадры уровня LLC по своему назначению подразделяются на три типа: информационные, управляющие и нenumерованные.

*Информационные кадры* (Information) предназначены для передачи информации в процедурах с установлением логического соединения LLC2 и должны обязательно содержать поле информации. В процессе передачи информационных блоков осуществляется их нумерация в режиме скользящего окна.

*Управляющие кадры* (Supervisory) предназначены для передачи команд и ответов в процедурах с установлением логического соединения LLC2, в том числе запросов на повторную передачу искаженных информационных блоков.

*Ненумерованные кадры* (Unnumbered) предназначены для передачи ненумерованных команд и ответов, выполняющих в процедурах без установления логического соединения передачу информации, идентификацию и тестирование LLC-уровня, а в процедурах с установлением логического соединения LLC2 — установление и разъединение логического соединения, а также информирование об ошибках.

Все типы кадров уровня LLC имеют единый формат (рис. 4.19)

Кадр LLC обрамляется двумя однобайтовыми полями «Флаг», имеющими значение 01111110. Флаги используются на уровне MAC для определения границ кадра LLC. В соответствии с многоуровневой структурой протоколов стандартов IEEE 802, кадр LLC вкладывается в кадр уровня MAC: в кадр Ethernet, Token Ring, FDDI и т. д. При этом флаги кадра LLC отбрасываются.

Кадр LLC содержит поле данных и заголовок, включающий в себя три поля:

- адрес точки входа службы назначения (Destination Service Access Point — DSAP);
- адрес точки входа службы источника (Source Service Access Point — SSAP);
- управляющее поле (Control).

*Поле данных* кадра LLC предназначено для передачи по сети пакетов протоколов вышерасположенных уровней, например сетевых протоколов IP, IPX, AppleTalk. Поле данных может отсутствовать в управляющих и некоторых ненумерованных кадрах.

*Адресные поля* DSAP и SSAP, занимающие по одному байту, позволяют указать, какая служба верхнего уровня пересылает данные с помощью этого кадра. Программному обеспечению узлов сети при получении кадров канального уровня необходимо распознать, какой протокол вложил свой пакет в поле данных поступившего кадра, чтобы передать извлеченный из кадра пакет соответствующему протоколу верхнего уровня для последующей обработки.

Флаг	Адрес точки входа службы назначения (DSAP)	Адрес точки входа службы источника (SSAP)	Управляющее поле (Control)	Данные (Data)	Флаг
01111110					01111110

Рис. 4.19. Формат кадров уровня LLC

Для идентификации этих протоколов вводятся так называемые адреса точки входа службы (Service Access Point — SAP). Значения адресов SAP приписываются протоколам в соответствии со стандартом 802.2. Например, для протокола IP значение SAP равно 0х6, а для протокола NetBIOS — 0хf0. Для одних служб определена только одна точка входа и соответственно только один SAP, когда адреса DSAP и SSAP совпадают, а для других — несколько. Например если в кадре LLC значения DSAP и SSAP содержат код протокола IPX, то обмен кадрами осуществляется между двумя IPX-модулями, выполняющимися в разных узлах. Однако иногда в кадре LLC указываются различающиеся DSAP и SSAP, что возможно только в тех случаях, когда служба имеет несколько адресов SAP, и это может быть использовано протоколом узла отправителя в специальных целях, например для уведомления узла получателя о переходе протокола отправителя в некоторый специфический режим работы.

*Поле управления* (1 или 2 байт) имеет сложную структуру при работе в режиме LLC2 и достаточно простую структуру при работе в режиме LLC1 (рис. 4.20).

В режиме LLC1 используется только один тип кадров — нумерованный. У кадра этого типа поле управления имеет длину 1 байт. Все подполя поля управления нумерованных кадров принимают нулевые значения, так что значимыми остаются только первые два бита поля, используемые как признак типа кадра. Так как в протоколе Ethernet при записи реализован обратный порядок битов в байте, то запись поля управления кадра LLC1, вложенного в кадр протокола Ethernet, имеет значение 0х03 (здесь и далее префикс 0х обозначает шестнадцатеричное представление).

В режиме LLC2 используются все три типа кадров, и все кадры делятся на команды и ответы на эти команды. Бит P/F (Poll/Final) имеет следующее значение: в командах он называется битом Poll и требует, чтобы на команду был дан ответ, а в ответах он называется битом Final и говорит о том, что ответ состоит из одного кадра.

Нумерованные кадры используются на начальной стадии взаимодействия двух узлов, т. е. стадии установления соединения по протоколу LLC2. Поле M нумерованных кадров определяет несколько типов команд, которыми пользуются два узла на этапе установления соединения. Приведем примеры таких команд:

		Разряды поля управления																
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	
Тип кадра	Информационный (Information)	0	N(S)								P/F	N(R)						
	Управляющий (Supervisory)	1	0	S	—	—	—										N(R)	
	Нумерованный (Unnumber)	1	1	M	P/F	M												

Рис. 4.20. Структура поля управления

ему с большой скоростью за счет механизма окна. Получение кадра RNR требует от передатчика полной приостановки передачи, до получения кадра RR. С помощью этих кадров осуществляется управление потоком данных, что особенно важно для коммутируемых сетей, в которых нет разделяемой среды, автоматически тормозящей работу передатчика за счет того, что новый кадр нельзя передать, пока приемник не закончит прием предыдущего.

Итак, можно сделать следующие выводы:

- протокол LLC обеспечивает для технологий локальных сетей требуемое качество транспортной службы, передавая свои кадры либо дейтаграммным способом, либо с помощью процедур с установлением соединения и восстановлением кадров;

- предоставляет верхним уровням три типа процедур, т.е. процедуру без установления соединения и без подтверждения, процедуру с установлением соединения и подтверждением и процедуру без установления соединения, но с подтверждением;

- обеспечивает дуплексный канал, т.е. данные могут передаваться в обоих направлениях;

- использует алгоритм скользящего окна в режиме с установлением соединения;

- может управлять потоком данных, поступающих от узлов сети с помощью управляющих кадров, что особенно важно для коммутируемых сетей, в которых нет разделяемой среды, автоматически тормозящей работу передатчика при высокой загрузке сети.

## 4.6. Мосты в ЛВС

### 4.6.1. Общие сведения

Довольно часто в организации возникает необходимость соединить между собой несколько ЛВС на канальном уровне. Почему на канальном? Потому, что чем выше мы поднимаемся по стеку протоколов вверх, тем больше затрат мы несем на обработку заголовков PDU разного уровня. Для этой цели используются специальные устройства, называемые мостами, которые функционируют на уровне канала данных. Это означает, что такое устройство не анализирует заголовки пакетов сетевого уровня и выше, а значит, может просто копировать кадры одной СПД в кадры другой СПД.

Мост является простейшим и исторически первым устройством для решения описываемой задачи. В настоящее время мосты уступили место коммутаторам, которые по сути представляют собой многопортовые мосты — устройства со множеством интерфейсов Ethernet и (или) WiFi, где каждая пара интерфейсов выполняет функции моста.

Рассмотрим типичные ситуации, в которых применяются мосты.

• *Установить сбалансированный асинхронный расширенный режим (SABME)*. Эта команда является запросом на установление соединения и одной из полного набора команд такого рода протокола HDLC. Расширенный режим означает использование двухбайтовых полей управления для кадров двух других типов;

• *Ненумерованное подтверждение (UA)*. Эта команда служит для подтверждения установления или разрыва соединения;

• *Сброс соединения (REST)*. Эта команда является запросом на разрыв соединения.

После установления соединения данные и положительные квитанции на кадры начинают передаваться в информационных кадрах. Логический канал протокола LLC2 является дуплексным, следовательно, данные могут передаваться в обоих направлениях. Если поток дуплексный, то положительные квитанции на кадры также доставляются в информационных кадрах. Если же потока кадров в обратном направлении нет или необходимо передать отрицательную квитанцию, то используются супервизорные кадры.

В информационных кадрах имеется поле  $N(S)$  для указания номера отправленного кадра, а также поле  $N(R)$  для указания номера кадра, который приемник ожидает получить от передатчика следующим. При работе протокола LLC2 используется скользящее окно размером в 127 кадров, а для их нумерации циклически используется 128 чисел (от 0 до 127).

Приемник всегда помнит номер последнего кадра, принятого от передатчика, и поддерживает переменную с указанным номером кадра, который он ожидает принять от передатчика следующим. Обозначим этот номер  $V(R)$  — это и будет значение, которое передается в поле  $N(R)$  кадра, посылаемого передатчику. Если в ответ на этот кадр приемник принимает кадр, в котором номер посланного кадра  $N(S)$  совпадает с номером ожидаемого кадра  $V(R)$ , то такой кадр считается корректным (если, конечно, корректна его контрольная сумма). Если приемник принимает кадр с номером  $N(S)$ , который не равен  $V(R)$ , то этот кадр отбрасывается и посылается отрицательная квитанция *Отказ (REJ)* с номером  $V(R)$ . При приеме отрицательной квитанции передатчик обязан повторить передачу кадра с номером  $V(R)$ , а также всех кадров с большими номерами, которые он уже успел отослать, пользуясь механизмом окна в 127 кадров.

В состав супервизорных кадров входят следующие кадры:

• *Отказ (REJect)*;

• *Приемник не готов (Receiver Not Ready — RNR)*;

• *Приемник готов (Receiver Ready — RR)*.

Команда RR с номером  $N(R)$  часто используется как положительная квитанция, когда поток данных от приемника к передатчику отсутствует, а команда RNR — для замедления потока кадров, поступающих в приемник. Такое замедление может быть необходимо, если приемник не успевает обработать поток кадров, присылаемых

1. Многие подразделения в организации имеют свои собственные локальные сети, например факультеты в университетах, отделы в институтах и т.п. В силу различия стоящих перед ними задач эти подразделения используют разные приложения и, что естественно, разные сети. При этом рано или поздно наступает момент, когда необходимо интегрировать информационные потоки всей организации, а следовательно, объединить сети между собой.

2. Организация может занимать несколько зданий и, возможно, целесообразно в каждом здании иметь свою сеть, выполнив объединение через мосты.

3. Иногда при высоких рабочих нагрузках приходится разбивать сеть на несколько подсетей в целях локализации трафика в каждой подсети. Например, понятно, что класс рабочих станций для студентов лучше оформлять как самостоятельную подсеть, локализовав трафик в ней, поскольку ни к чему распространять по всему факультету трафик с фотографиями и музыкой (рис. 4.21).

4. В некоторых случаях причиной для использования моста может служить большое расстояние между объединяемыми сетями, поскольку используя мост, можно увеличить длину сегмента локальной сети.

5. Мост может увеличить надежность сети. В локальной сети один узел может нарушить работоспособность сети в целом. Мосты, размещенные в критических точках сети, подобно запасным пожарным

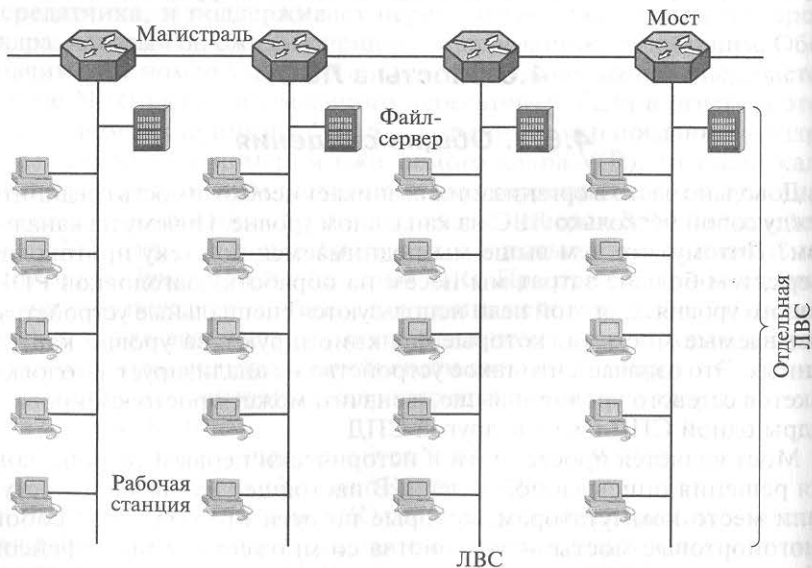


Рис. 4.21. Пример локальных сетей, соединенных магистралью для распределения нагрузки между СПД

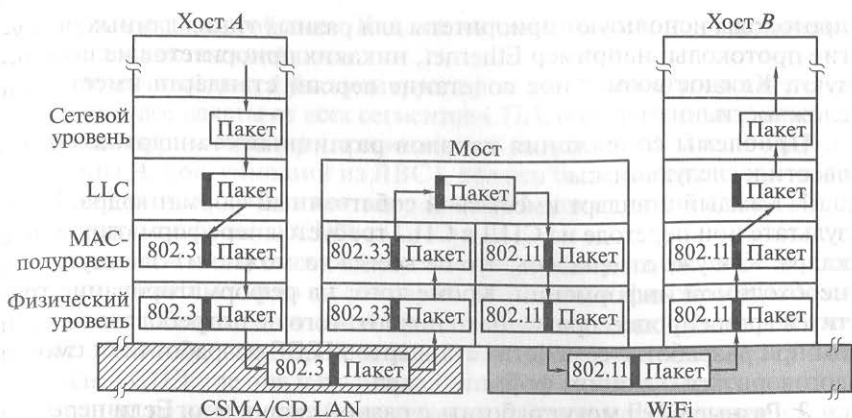


Рис. 4.22. Схема работы двухпортового моста между Ethernet и WiFi

выходам, могут заблокировать такой узел и предотвратить нарушение работы системы в целом.

6. Мост может повысить безопасность сети. Большинство интерфейсов в ЛВС имеют специальный режим, при котором компьютер получает все пакеты, проходящие в сети, а не только те, которые адресованы ему. Всякого рода злоумышленники и просто любопытствующая публика просто обожают этот режим. С помощью правильно расставленных мостов можно добиться, чтобы определенный трафик проходил лишь по определенным маршрутам и не мог попасть в чужие руки.

Теперь, когда понятно для чего необходимы мосты, рассмотрим, как они работают. На рис. 4.22 показана схема работы простого двухпортового моста между Ethernet и WiFi.

#### 4.6.2. Мосты СПД IEEE 802.x в СПД IEEE 802.x

На первый взгляд может показаться, что построить мост для каналов, работающих по стандартам IEEE 802 несложно. Все что требуется — трансформировать один формат кадра в другой. Однако многие стандарты в семействе IEEE 802 несовместимы между собой как на физическом уровне, так и на MAC-подуровне. В частности, таковыми являются не рассматриваемые здесь *кольцо с маркером* (Token Ring) и *шина с маркером* (Token Bus), т.е. 802.5 и 802.4 соответственно, в которых машина получает доступ к каналу, только если она обладает специальным пакетом — маркером.

В подразд. 5.2 описан протокол FDDI для организации высокоскоростных локальных сетей, который является преемником протокола Token Bus и также использует маркерный доступ. Некоторые

протоколы используют приоритеты для разных типов данных, а другие протоколы, например Ethernet, никаких приоритетов не используют. Каждое возможное сочетание версий стандарта имеет свои сложности.

Проблемы сопряжения каналов различных стандартов можно свести к следующим:

1. Каждый стандарт имеет свой собственный формат кадра. В результате при переходе из СПД в СПД требуется переформатирование кадра. Как уже отмечалось, это не всегда возможно из-за отсутствия необходимой информации. Кроме того, на реформатирование тратится время процессора. Однако ничего этого не потребовалось, если бы при разработке семейства стандартов IEEE разработчики смогли договориться о едином формате кадра.

2. Разные СПД могут работать с разной скоростью. Если передача производится из скоростной СПД в медленную СПД, то мост должен обладать достаточным буфером. Эта проблема может усугубляться непостоянством скорости передачи в результате коллизий. К тому же несколько СПД могут посылать трафик в одну и ту же СПД, что опять приведет к перекосу скоростей.

3. Важной является также проблема моста как источника временной задержки, которая может влиять на тайм-аут на верхних уровнях. Предположим, что сетевой уровень над канальным уровнем 802.11 пытается послать длинное сообщение в виде последовательности кадров. После отправки последнего кадра таймер устанавливается на ожидание уведомления о получении. Если при этом сообщение проходит через мост с медленной СПД 802.3, то существует опасность, что тайм-аут наступит прежде чем последний кадр будет передан в медленную СПД. Сетевой уровень решит, что все сообщение утеряно, и начнет все сначала. После нескольких попыток сетевой уровень сообщит транспортному уровню, что получатель отсутствует.

4. Наиболее серьезной проблемой является то, что стандарты могут иметь разную максимальную длину кадра. Для 802.3 при скорости 10 Мбит/с — это 1 500 байт, а для 802.11 (WiFi) — 2 346 байт.

### 4.6.3. Прозрачные мосты

Рассмотрим сначала *прозрачный мост*, или *мост с деревом соединений*. Основной заботой разработчиков этого моста было обеспечение его полной прозрачности, т. е. требовалось создать устройство, поддерживающее стандарт IEEE 802.3, которое пользователь мог бы купить в магазине, подключить к нему кабели своих многочисленных сегментов локальной сети и начать работать. Подключение этого устройства к СПД не должно было требовать каких-либо изменений в оборудовании, программном обеспечении, его переинсталляции, загрузки каких-либо таблиц и т. п. Просто купил, принес,

включил, и ... все работает. Как это ни удивительно, но разработчики почти достигли своей цели.

Прозрачный мост функционирует в режиме общедоступности, т. е. ему доступны все пакеты от всех сегментов СПД, подключенных к нему.

Рассмотрим пример, приведенный на рис. 4.23. Здесь кадр для машины *A*, поступивший из ЛВС1, должен быть сброшен, так как он уже в заданной СПД, а вот кадр из ЛВС1 для машины *C* или *F* надо передать в требуемую СПД.

Следовательно, по каждому поступающему кадру мост должен принять решение: надо ли его передавать дальше или сбросить, а если передавать дальше, то в какой сегмент. Для этого каждый мост должен иметь таблицу, в которой каждой станции сопоставляется номер сегмента СПД, где она находится. Эта таблица, как правило, имеющая огромные размеры, организована как таблица перемешивания, или хэш-таблица.

Когда мост включают первый раз, его таблицы пусты. Заполняются они по следующему алгоритму:

- каждый кадр с неизвестным мосту адресом доставки рассылается во все СПД, подключенные к данному мосту, кроме той, из которой поступил этот кадр;
- по реакции из каждой СПД на этот кадр мост определяет, в какой конкретно СПД находится адрес доставки и фиксирует эту информацию в таблице (как это происходит, будет рассмотрено далее).

Кадры с таким же адресом доставки будут всегда посылаться только в СПД, определенную этим алгоритмом, который называется *обучением с запаздыванием*.

Топология СПД может изменяться динамически. Машины и мосты могут подключаться к СПД и исключаться из нее, поэтому для каждого элемента таблицы указывается время, когда от этой машины или моста поступал кадр. Периодически таблица просматривается, и для всех ее элементов, у которых время последнего поступления кадра отличается от текущего более чем на несколько минут, запускается

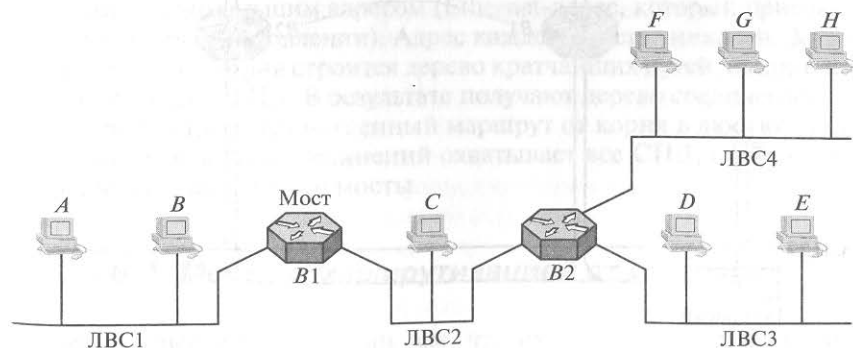


Рис. 4.23. Конфигурация из четырех ЛВС и двух мостов (*B1*, *B2*)

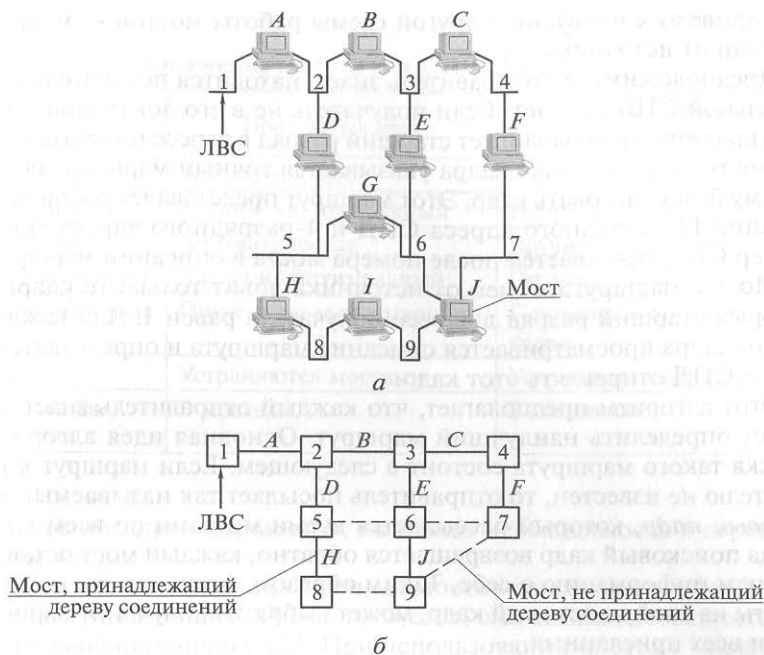


Рис. 4.25. Граф (а) и дерево соединений (б) в ЛВС с мостами

На рис. 4.25 показана СПД, состоящая из девяти локальных СПД, соединенных мостами. Граф соединений этой системы, показанный на рис. 4.25, а, можно сократить до дерева соединений, как показано на рис. 4.25, б, в котором для каждой СПД в любую другую СПД имеется только один путь.

Как строится дерево соединений? Прежде всего, надо из всех мостов выбрать один в качестве корня дерева, например можно взять для этого мост с наименьшим адресом (Ethernet-адрес, который присваивают мосту при изготовлении). Адрес каждого моста уникален. Затем для полученного корня строится дерево кратчайших путей, соединяющих его с каждой СПД. В результате получают дерево соединений.

Алгоритм строит единственный маршрут от корня в любую СПД. При этом хотя дерево соединений охватывает все СПД, в нем могут быть представлены не все мосты.

#### 4.6.4. Мосты с маршрутизацией от источника

Прозрачные мосты хороши тем, что их достаточно только подключить, и все работает. Однако они никак не учитывают (и не могут этого делать) оптимальное распределение пропускной способности.

процедура поиска в СПД, т. е. все изменения в СПД отслеживаются динамически. Если какую-то машину исключают из одной СПД, перенесут ее и включают в другой СПД, описанный алгоритм отметит это изменение через несколько минут.

Итак, каждый раз, когда поступает кадр, мост выполняет следующие действия:

1. Если адрес отправителя и адрес получателя один и тот же, кадр сбрасывается.
2. Если адрес отправителя и адрес получателя разные, то кадр направляется в надлежащую СПД.
3. Если в таблице нет информации о том, куда направлять кадр, его посылают во все доступные СПД.

В некоторых случаях для обеспечения большей надежности две СПД соединяются двумя мостами, как это показано на рис. 4.24. Однако у такой конфигурации есть одна опасность. Пусть в СПД 1 был сгенерирован кадр  $F$ . Этот кадр будет сдублирован во все СПД и мостом  $B1$ , и мостом  $B2$ . Пусть мост  $B1$  породил кадр  $F1$ , а мост  $B2$  — кадр  $F2$ . Мост  $B1$ , увидев кадр  $F2$  с неизвестным адресом доставки, сдублирует его в СПД 1 как кадр  $F3$ . Также мост  $B2$ , увидев кадр  $F1$ , сдублирует его в виде кадра  $F4$ . Этот цикл будет длиться до бесконечности.

Решение данной проблемы состоит в обеспечении возможности мостам во взаимодействии друг с другом накладывать на фактическую структуру соединений СПД ограничения, в результате которых подобные циклы стали бы невозможными.

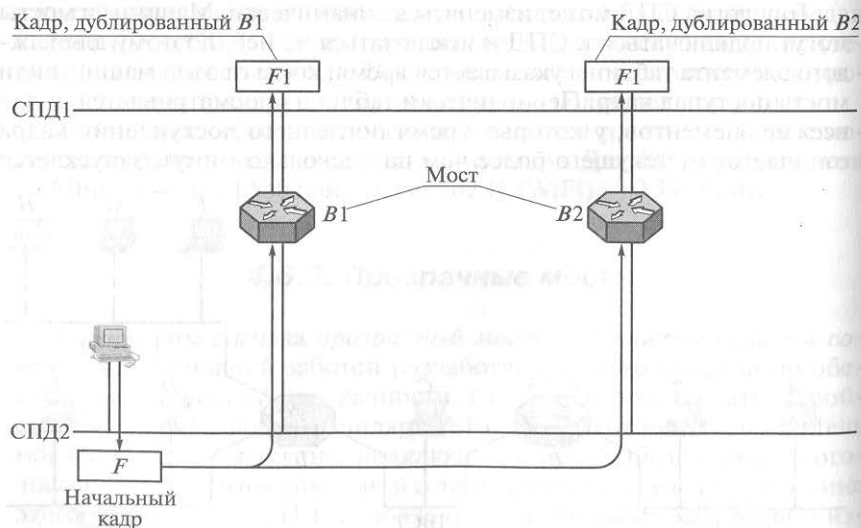


Рис. 4.24. Конфигурация ЛВС с двумя параллельными прозрачными мостами

Это привело к появлению другой схемы работы мостов — маршрутизации от источника.

Предположим, что отправитель знает, находится получатель в его локальной СПД или нет. Если получатель не в его локальной СПД, то отправитель устанавливает старший разряд в адресе получателя в 1. Кроме того, в заголовке кадра указывается точный маршрут, по которому будет следовать кадр. Этот маршрут представляет собой чередование 12-разрядного адреса СПД и 4-разрядного адреса моста. Номер СПД указывается после номера моста в описании маршрута.

Мост с маршрутизацией от источника ловит только те кадры, у которых старший разряд в адресе получателя равен 1. Для каждого такого кадра просматривается описание маршрута и определяется, в какую СПД отправлять этот кадр.

Этот алгоритм предполагает, что каждый отправитель знает или может определить наилучший маршрут. Основная идея алгоритма поиска такого маршрута состоит в следующем. Если маршрут к получателю не известен, то отправитель посылает так называемый *поисковый кадр*, который рассылается всеми мостами по всем СПД. Когда поисковый кадр возвращается обратно, каждый мост оставляет в нем информацию о себе. Таким образом, отправитель, получив ответы на свой поисковый кадр, может выбрать наилучший маршрут среди всех присланных.

Этот алгоритм действительно позволяет найти наилучший маршрут, но он имеет один серьезный недостаток — экспоненциальный рост числа поисковых кадров.

Обнаружив наилучший путь, каждый хост в СПД хранит его. Естественно, это накладывает определенные требования на ресурсы хоста, что делает использование этого подхода не столь прозрачным, как в первом случае.

#### **4.6.5. Сравнение мостов для СПД IEEE 802.3**

Прозрачные мосты и мосты с маршрутизацией от источника имеют свои достоинства и недостатки, которые для сравнения представлены в виде табл. 4.2.

Одно из основных различий между этими мостами заключается в различии СПД, ориентированных на соединение, и неориентированных на соединение. Прозрачные мосты не поддерживают концепции виртуального соединения и маршрутизируют каждый кадр независимо друг от друга. Мосты с маршрутизацией от источника, наоборот, определяют маршрут с помощью поискового кадра, а затем используют этот маршрут постоянно.

Прозрачные мосты полностью совместимы со всеми продуктами в стандартах 802 в отличие от мостов с маршрутизацией от источника, при использовании которых все машины в сети должны знать схему подключения мостов к СПД. Любое изменение в СПД, затра-

Сравнение мостов для СПД IEEE 802

Признак	Прозрачный мост	Мост с маршрутизацией от источника
Ориентация	Без соединения	С соединением
Прозрачность	Полностью прозрачный	Непрозрачный
Настройка	Автоматическая	Вручную
Выбор маршрута	Частично оптимальный	Оптимальный
Способ обучения моста	Обучение с запаздыванием	С помощью поискового кадра
Сбои	Устраняются мостами	Устраняются машинами
Наибольшая сложность	В мостах	В машинах

гивающее подключение мостов, вызывает необходимость в перестройке машин.

При использовании прозрачных мостов никаких специальных усилий по управлению СПД не требуется, они автоматически отслеживают конфигурацию СПД. При использовании мостов с маршрутизацией от источника требуется значительная ручная работа. В этом случае любая ошибка в адресах СПД или мостов может вызвать тяжелые последствия, и обнаружить ее бывает очень трудно.

При соединении двух функционирующих СПД через прозрачный мост ничего делать не надо кроме его подключения. При их соединении через мост, маршрутизирующий от источника, может потребоваться изменение адресов СПД и мостов, чтобы избежать дублирования.

Одним из основных преимуществ мостов с маршрутизацией от источника является то, что они хотя бы теоретически могут строить оптимальные маршруты, в то время как прозрачные мосты ограничены в выборе маршрута деревом соединений. Мосты с маршрутизацией от источника также могут работать с мостами, включенными в параллель (см. подразд. 4.6.3).

Механизмы определения места доставки кадра также имеют свои достоинства и недостатки. В случае использования прозрачных мостов недостаток состоит в необходимости ожидания, когда придет кадр от машины получателя, а в случае использования моста с маршрутизацией от источника — экспоненциальный рост числа поисковых кадров.

Реакция на ошибки в СПД в обоих случаях также разная. При использовании прозрачных мостов все происходит автоматически, т.е. мосты сами слушают, что происходит в СПД и реагируют должным образом. Самим машинам делать ничего не приходится. При использовании мостов с маршрутизацией от источника вся сложность исправления ошибок и отказов в сети ложится на машины.

## 4.7. Сетевые коммутаторы

### 4.7.1. Общие сведения

Сетевой коммутатор (далее просто коммутатор) представляет собой устройство с несколькими портами, к которым можно подключать сегменты каналов с множественным доступом (далее КМД), например сегменты 802.3. На основании таблицы коммутации, расположенной в памяти коммутатора, кадры с входного порта коммутатор передает на надлежащий выходной порт, поэтому трафик на отдельных сегментах существенно ниже, чем на коммутаторе в целом. Коммутаторы работают на более высоких скоростях, чем мосты, и функционально являются более гибкими.

По сравнению с мостами у коммутаторов больше портов. Достаточно распространены коммутаторы с 24 и 48 портами со скоростями соответственно 10 и 100 Мбит/с. Коммутаторы на крупных предприятиях могут поддерживать сотни портов. У коммутаторов больше размер буферного пространства для сохранения принимаемых кадров, что весьма полезно, особенно если элементы сети перегружены. В зависимости от стоимости коммутатора возможна поддержка локальных сегментов СПД с КМД с разными скоростями: 10 Мбит/с, 100 Мбит/с, 1 Гбит/с или 10 Гбит/с.

Для коммутации данных между сетевыми портами коммутаторы используют один из следующих методов:

- *коммутация без буферизации кадров.* При использовании этого метода коммутатор, получив 6-байтовый MAC-адрес получателя, сразу занимает требуемый выходной порт и начинает передачу. Обнаружения ошибок при этом не происходит. Если на входе произойдет коллизия, то кадр будет потерян;

- *коммутация с буферизацией кадров.* При использовании этого метода коммутатор сохраняет в буфере весь кадр, причем во время сохранения кадра коммутатор анализирует его и производит обнаружение ошибок. После этого, убедившись в отсутствии коллизии на входе, он передает кадр;

- *коммутация с исключением фрагментов.* Коммутация без буферизации кадров обеспечивает малое время задержки. Получив 64-байтовый заголовок кадра, коммутатор занимает требуемый выходной порт и начинает передачу. Обнаружения ошибок при этом не происходит. Коммутация с исключением фрагментов гарантирует, что из источника считывается достаточное число байтов, чтобы обнаружить коллизию до пересылки.

Коммутация с исключением фрагментов — это метод, обеспечивающий компромисс между большим временем задержки с гарантией передачи кадра при коммутации с буферизацией, и небольшим временем задержки с риском потери кадра при коммутации без буферизации кадров. На практике разница между коммутацией с буфе-

ризацией и без буферизации кадров неважна, поскольку незначительное уменьшение времени задержки при коммутации без буферизации, возмещается незначительными колебаниями времени ожидания при коммутации с буферизацией.

#### **4.7.2. Функционирование сетевого коммутатора**

Для каждого порта коммутатор формирует таблицу MAC-адресов, связанных с сегментом, подключенным к порту коммутатора. Затем коммутатор использует эти MAC-адреса при принятии решения о дальнейших операциях с кадрами: фильтрация, пересылка или лавинная рассылка.

Когда на порт поступает кадр, коммутатор сравнивает MAC-адрес адресата с адресами в таблицах. Если MAC-адрес получателя кадра находится в том же сегменте сети, что и отправитель, коммутатор сбрасывает кадр. Этот процесс называется фильтрацией, и с его помощью коммутаторы могут значительно уменьшить трафик между сегментами сети. Если MAC-адрес получателя кадра находится в другом сегменте, коммутатор пересылает кадр на порт, к которому подключен соответствующий сегмент.

Если у коммутатора нет записи об адресе получателя, то он передаст кадр всем портам, кроме того порта, с которого кадр был получен. Устройство-получатель отвечает на широковещательную рассылку специальным кадром по адресу отправителя. Коммутатор вводит искомый MAC-адрес получателя и номер соответствующего порта коммутатора в таблицу MAC-адресов. Теперь коммутатор может пересылать кадры между отправителем и получателем без широковещательной рассылки.

#### **4.7.3. Структурирование трафика**

Коммутируемые СПД КМД — это самый распространенный в настоящее время тип СПД для локальных сетей. Сегодня цена за порт на коммутаторе уменьшилась настолько, что концентраторы и мосты больше не рассматриваются при принятии решения о покупке сетевого оборудования.

Коммутаторы позволяют структурировать трафик, т.е. разбивать его на фрагменты по определенному признаку, чаще всего по физическому расположению абонентских машин пользователей. Например, все пользователи, подключенные к коммутатору на первом этаже офисного здания, принадлежат одной рабочей группе, а пользователи, подключенные к коммутатору на втором этаже, — к другой. Такая организация позволяет каждой группе обращаться к устройствам в сети, например серверам, с меньшей вероятностью возникновения коллизий и повышает общую производительность сети.

#### 4.7.4. Сравнение коммутаторов и мостов

Во многом аналогичные мостам сетевые коммутаторы обладают и особыми характеристиками, которые делают их эффективным средством снижения перегрузки сетей за счет увеличения их фактической полосы пропускания.

Сходство мостов и коммутаторов заключается в следующем:

- мосты, и коммутаторы соединяют сегменты СПД КМД;
- мосты и коммутаторы используют таблицу MAC-адресов для идентификации сегмента, в который нужно переслать кадр с данными;
- мосты и коммутаторы помогают уменьшить сетевой трафик.

Дополнительные преимущества по устранению коллизий обеспечиваются следующие особые характеристики коммутаторов:

- *выделенный канал связи между устройствами.* Если на каждый порт сетевого коммутатора подключить только линию от одного абонента (это так называемая микросегментация), то каждый пользователь получит доступ к каналу передачи и не будет конкурировать с другими пользователями, а значит, и коллизий возникать не будет;

- *параллельные сеансы связи.* Параллельность сеансов связи обеспечивается посредством одновременной пересылки нескольких кадров между разными парами портов, что увеличивает пропускную способность СПД в соответствии с числом поддерживаемых сеансов связи. Например, при пересылке кадров между портами 1 и 2 может проходить параллельный сеанс связи между портами 5 и 6;

- *полнодуплексная система связи.* После выполнения микросегментации в подключении участвуют только коммутатор и подключенный абонент. Теперь можно настроить порт таким образом, чтобы он мог получать и отправлять данные в одно и то же время, т.е. обеспечивать дуплексный канал связи. Например, соединение типа «точка—точка» обладает скоростью передачи 100 Мбит/с и скоростью приема 100 Мбит/с, обеспечивая эффективную пропускную способность 200 Мбит/с на одном соединении. Выбор между полудуплексом и дуплексом происходит автоматически во время создания канала;

- *адаптация к скорости среды.* Сетевой коммутатор, имеющий порты на разные скорости, может автоматически выбирать между скоростями передачи 10/100 Мбит/с или 100/1 000 Мбит/с.

### 4.8. Виртуальные сети

#### 4.8.1. Понятие виртуальной сети

При создании СПД на основе каналов с множественным доступом всем узлам локальной сети доступен широковещательный трафик, который изначально не ограничивает ни концентратор, ни мост, ни коммутатор.

Виртуальной сетью — VLAN — называют группу узлов сети, в которой весь трафик, включая широковещательный, полностью изолирован на канальном уровне от других узлов [31]. Это означает, что передача кадров между узлами сети, относящимися к различным виртуальным сетям, на основании адреса канального уровня невозможна (хотя виртуальные сети могут взаимодействовать друг с другом на сетевом уровне с использованием маршрутизаторов). Основное средство структурирования СПД на основе каналов с множественным доступом представляет собой систему виртуальных сетей, построенных с использованием коммутаторов.

Изолирование отдельных узлов сети на канальном уровне с использованием технологии виртуальных сетей позволяет решать одновременно несколько задач. Во-первых, виртуальные сети способствуют повышению производительности сети, локализуя широковещательный трафик в пределах виртуальной сети, т. е. широковещательные кадры (а также кадры с групповыми и неизвестными адресами) пересылаются внутри виртуальной сети, но не между виртуальными сетями. Во-вторых, изоляция виртуальных сетей друг от друга на канальном уровне позволяет повысить безопасность сети, делая часть ресурсов для определенных категорий пользователей недоступной.

#### **4.8.2. Типы виртуальных сетей**

До появления стандарта IEEE 802.1Q по организации виртуальных сетей каждый производитель сетевого оборудования использовал собственную технологию организации VLAN. Такой подход имел существенный недостаток: технологии одного производителя были несовместимы с технологиями других фирм. Поэтому при построении виртуальных сетей на базе нескольких коммутаторов необходимо было использовать оборудование только от одного производителя.

Появление стандарта виртуальных сетей IEEE 802.1Q позволило преодолеть проблему несовместимости. Однако до сих пор существуют коммутаторы, которые либо не поддерживают стандарт IEEE 802.1Q, либо помимо этого стандарта используют и другие технологии.

Существуют разные способы построения виртуальных сетей, но в коммутаторах в настоящее время в основном используются технология группировки портов и используется спецификация IEEE 802.1Q.

#### **Виртуальные сети на основе группировки портов**

Виртуальные сети на основе группировки портов (Port-based) обычно реализуются в так называемых Smart-коммутаторах, или управляемых коммутаторах, в дополнение к реализации VLAN на базе стандарта IEEE 802.1Q.

Этот способ создания виртуальных сетей достаточно простой. Каждый порт коммутатора приписывается к той или иной виртуаль-

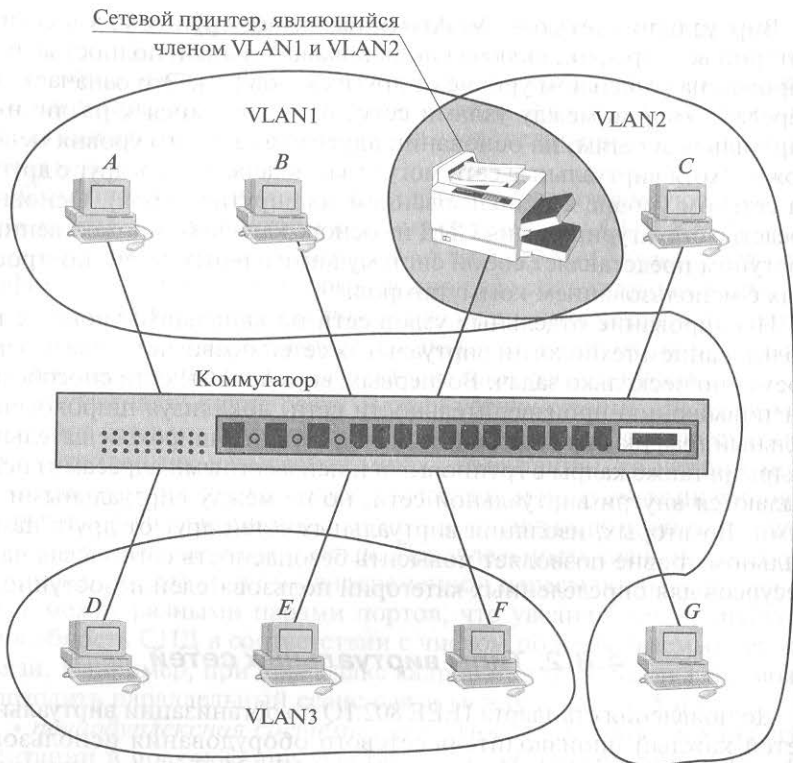


Рис. 4.26. Создание разделяемого ресурса между несколькими виртуальными сетями с использованием технологии группировки портов

ной сети, т.е. порты группируются в виртуальные сети. Адресация кадра в такой сети основывается на MAC-адресе получателя и ассоциированного с ним порта. Если к порту, приписанному к определенной виртуальной сети, например к VLAN1, подключить ПК пользователя, то этот ПК автоматически будет принадлежать сети VLAN1. Если же к данному порту подключить коммутатор, то все порты этого коммутатора также будут принадлежать VLAN1.

При использовании группировки портов один и тот же порт может одновременно приписываться к нескольким виртуальным сетям, что позволяет реализовывать разделяемые ресурсы между пользователями различных виртуальных сетей. Например, чтобы реализовать совместный доступ к сетевому принтеру или файл-серверу пользователей виртуальных сетей VLAN1 и VLAN2, необходимо порт коммутатора, к которому подключается сетевой принтер или файл-сервер, приписать одновременно к сетям VLAN1 и VLAN2 (рис. 4.26).

Описываемый прием обладает рядом преимуществ по сравнению с использованием стандарта IEEE 802.1Q, но имеет и свои недостатки.

К достоинствам приема группировки портов можно отнести простоту конфигураций создаваемых виртуальных сетей, причем в этом случае не требуется, чтобы конечные узлы сети поддерживали стандарт IEEE 802.1Q. При такой организации виртуальных сетей можно создавать разделяемые сетевые ресурсы.

Однако если СПД достаточно крупная и построена на нескольких коммутаторах, то возможности по организации виртуальных сетей с использованием группировки портов имеют существенные ограничения. Прежде всего, этот прием ограничивает возможность наращивания как числа самих VLAN, так и числа узлов в каждой из них. В большинстве случаев применение этого приема распространяется лишь на сети с одним коммутатором.

Рассмотрим для примера ситуацию, когда сеть изначально построена на базе двух коммутаторов, поддерживающих организацию виртуальных сетей на основе группировки портов (рис. 4.27).

Пусть необходимо, чтобы одна часть портов первого и второго коммутаторов относилась к VLAN1, а другая — к VLAN2. Для этого необходимо, во-первых, чтобы оба коммутатора позволяли не только организовывать виртуальные сети на основе группировки портов, но и распространять такие сети на несколько коммутаторов (подобная функция реализована далеко не у всех коммутаторов), а, во-вторых,

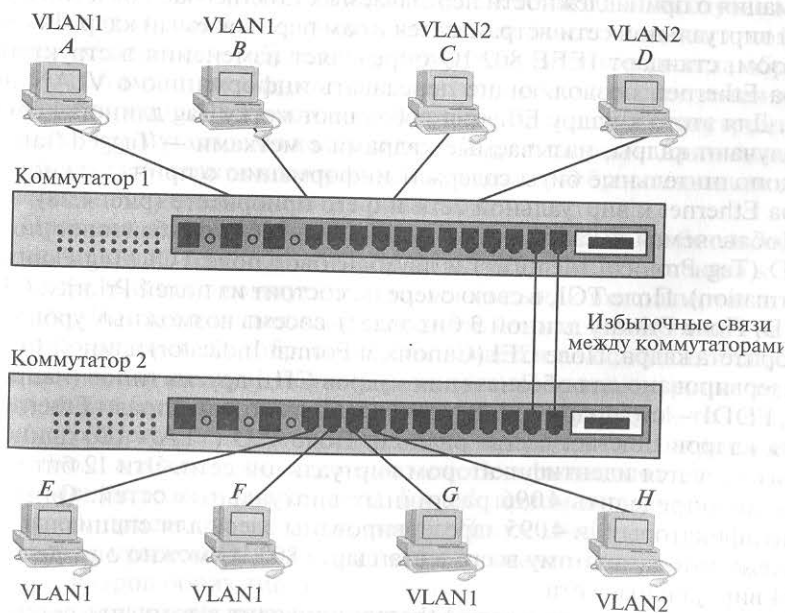


Рис. 4.27. Реализация виртуальных сетей с использованием группировки портов для сетей на базе двух коммутаторов

чтобы между коммутаторами было установлено столько физических соединений, сколько создано виртуальных сетей.

Рассмотрим два шестипортовых коммутатора. Пусть в первом коммутаторе порты 1 и 2 относятся к VLAN1, а порты 3 и 4 — к VLAN2; во втором коммутаторе порты 1, 2 и 3 относятся к VLAN1, а порт 4 — к VLAN2. Чтобы пользователи VLAN1 первого коммутатора могли общаться с пользователями VLAN1 второго коммутатора, эти коммутаторы должны быть связаны между собой портами, относящимися к VLAN1 (например, порт 5 первого и второго коммутаторов необходимо приписать к VLAN1). Аналогично для общения пользователей VLAN2 первого коммутатора с пользователями VLAN2 второго коммутатора следует связать эти коммутаторы через порты, приписанные к VLAN2 (это могут быть порты 6 на обоих коммутаторах).

Таким образом, проблему наращивания числа виртуальных сетей при использовании технологии группировки портов можно решить (правда, не во всех случаях) за счет установления избыточных связей между коммутаторами.

### **Виртуальные сети на основе стандарта IEEE 802.1Q**

В виртуальных сетях, основанных на стандарте IEEE 802.1Q, информация о принадлежности передаваемых Ethernet-кадров к той или иной виртуальной сети встраивается в сам передаваемый кадр. Таким образом, стандарт IEEE 802.1Q определяет изменения в структуре кадра Ethernet, позволяющие передавать информацию о VLAN по сети. Для этого к кадру Ethernet добавляют метку Tag длиной 4 байт и получают кадры, называемые кадрами с метками — Tagged frame, где дополнительные биты содержат информацию о принадлежности кадра Ethernet к виртуальной сети и о его приоритете (рис. 4.28).

Добавляемая к кадру метка включает в себя двухбайтовое поле TPID (Tag Protocol Identifier) и двухбайтовое поле TCI (Tag Control Information). Поле TCI, в свою очередь, состоит из полей Priority, CFI и VID. Поле Priority длиной 3 бит задает восемь возможных уровней приоритета кадра. Поле CFI (Canonical Format Indicator) длиной 1 бит зарезервировано для обозначения кадров СПД других типов (например, FDDI — см. подразд. 5.2), передаваемых по магистрали Ethernet, и для кадров Ethernet всегда равно 0. Поле VID (VLAN ID) длиной 12 бит является идентификатором виртуальной сети. Эти 12 бит позволяют определить 4096 различных виртуальных сетей. Однако идентификаторы 0 и 4095 зарезервированы здесь для специального использования, поэтому всего в стандарте 802.1Q можно определить 4094 виртуальные сети.

Изменение формата кадра Ethernet приводит к тому, что сетевые устройства, не поддерживающие стандарт IEEE 802.1Q (называемые Tag-unaware), не могут работать с кадрами, в которые вставлены



Рис. 4.28. Сравнение структур обычного Ethernet-кадра и кадра с меткой

метки, а подавляющее большинство этих устройств (в частности, сетевые Ethernet-контроллеры конечных узлов сети) в настоящее время не поддерживают этот стандарт. Следовательно, для обеспечения совместимости с устройствами, поддерживающими стандарт IEEE 802.1Q (Tag-aware-устройства), коммутаторы стандарта IEEE 802.1Q должны поддерживать как традиционные Ethernet-кадры, т.е. кадры без меток (Untagged), так и кадры с метками (Tagged).

При этом входящий и исходящий трафики в зависимости от типа источника и получателя могут образовываться и из кадров типа Tagged, и из кадров типа Untagged, так как только в этом случае можно обеспечить совместимость с внешними по отношению к коммутатору устройствами. Трафик же внутри коммутатора всегда образуется пакетами типа Tagged. Следовательно, для обеспечения поддержки различных типов трафиков и образования внутреннего трафика коммутатора из пакетов типа Tagged кадры на принимаемом и передающем портах коммутатора должны преобразовываться в соответствии с определенными правилами.

**Правила входного порта.** Рассмотрим более подробно процесс передачи кадра через коммутатор (рис. 4.29). По отношению к трафику каждый порт коммутатора может быть как входным, так и выходным. После принятия кадра входным портом коммутатора решение о его дальнейшей обработке принимается на основании определенных правил входного порта (Ingress rules). Поскольку принимаемый кадр может быть как типа Tagged, так и типа Untagged, то правила входного порта определяют, какие типы кадров должны приниматься портом, а какие отфильтровываться. Возможны следующие варианты: прием только кадров типа Tagged, прием только кадров типа Untagged, прием кадров обоих типов. По умолчанию для всех коммутаторов правилами входного порта устанавливается возможность приема кадров обоих типов.

Если правилами входного порта определено, что он может принимать кадр типа Tagged, в котором имеется информация о принадлежности к конкретной виртуальной сети (VID), то этот кадр пере-



Рис. 4.29. Процесс продвижения кадров в коммутаторе, совместимом со стандартом IEEE 802.1Q

дается без изменения. Если же этими правилами определена возможность работы с кадрами типа Untagged, в которых не содержится информация о принадлежности к виртуальной сети, то прежде всего такой кадр преобразуется входным портом коммутатора к типу Tagged (напомним, что внутри коммутатора все кадры должны иметь метки о принадлежности к виртуальной сети).

Чтобы такое преобразование стало возможным, каждому порту коммутатора присваивается уникальный идентификатор PVID (Port VLAN Identifier), определяющий принадлежность порта к конкретной виртуальной сети внутри коммутатора (по умолчанию все порты коммутатора имеют одинаковый идентификатор PVID = 1). Для преобразования кадра типа Untagged к типу Tagged его необходимо дополнить меткой VID. Значение поля VID входного Untagged-кадра устанавливается равным значению PVID входящего порта, т.е. все входящие Untagged-кадры автоматически приписываются к той виртуальной сети внутри коммутатора, к которой принадлежит входной порт.

**Правила продвижения пакетов.** После того как все входящие кадры отфильтрованы, преобразованы или оставлены без изменения в соответствии с правилами входного порта, решение об их передаче к выходному порту основывается на определенных правилах продвижения пакетов (Forwarding Process).

Правило продвижения пакетов внутри коммутатора заключается в том, что пакеты могут передаваться только между портами, ассоциированными с одной виртуальной сетью. Как уже отмечалось, каждому порту присваивается идентификатор PVID, который используется для преобразования принимаемых Untagged-кадров, а также для определения принадлежности порта к виртуальной сети внутри коммутатора с идентификатором VID = PVID. Таким образом, порты с одинаковыми идентификаторами внутри одного коммутатора ассоциируются с одной виртуальной сетью.

Если же виртуальная сеть строится на базе одного коммутатора, то идентификатора порта PVID, определяющего его принадлежность

к виртуальной сети, вполне достаточно. Правда, создаваемые таким образом сети не могут перекрываться, поскольку каждому порту коммутатора соответствует только один идентификатор, и в этом случае создаваемые виртуальные сети не будут обладать такой же гибкостью, как виртуальные сети, создаваемые на основе портов.

Однако стандарт IEEE 802.1Q с самого начала задумывался для обеспечения построения масштабируемой инфраструктуры виртуальных сетей, включающей в себя множество коммутаторов, и в этом состоит его главное преимущество по сравнению с технологией образования VLAN на основе портов. При этом для расширения сети за пределы одного коммутатора наличие одних идентификаторов портов недостаточно, поэтому каждый порт может быть ассоциирован с несколькими виртуальными сетями, имеющими различные идентификаторы VID.

Если адрес назначения пакета соответствует порту коммутатора, принадлежащему к той же виртуальной сети, что и сам пакет (могут совпадать VID пакета и VID порта или VID пакета и PVID порта), то такой пакет может быть передан. Если же передаваемый кадр принадлежит к виртуальной сети, с которой выходной порт никак не связан (VID пакета не соответствует PVID или VID порта), то кадр не может быть передан и отбрасывается.

**Правила выходного порта.** После того как кадры внутри коммутатора переданы на выходной порт, их дальнейшее преобразование зависит от правил выходного порта (Egress rules). Как уже говорилось, трафик внутри коммутатора создается только пакетами типа Tagged, а входящий и исходящий трафики могут быть образованы пакетами обоих типов. Соответственно правилами выходного порта (правилом контроля метки — Tag Control) определяется, следует ли преобразовывать кадры Tagged к формату Untagged.

Каждый порт коммутатора может быть сконфигурирован как Tagged Port или Untagged Port.

Если выходной порт коммутатора определен как Tagged Port, то исходящий трафик будет создаваться кадрами типа Tagged с информацией о принадлежности к виртуальной сети. Следовательно, выходной порт в этом случае не изменяет тип кадров, оставляя их такими же, какими они были внутри коммутатора. К такому порту может подсоединяться только устройство, совместимое со стандартом IEEE 802.1Q, например коммутатор или сервер с сетевой картой, поддерживающей работу с виртуальными сетями данного стандарта.

Если же выходной порт коммутатора определен как Untagged Port, то все исходящие кадры преобразуются к типу Untagged, т. е. из них удаляется дополнительная информация о принадлежности к виртуальной сети. К такому порту можно подключать любое сетевое устройство, в том числе коммутатор, не совместимый со стандартом IEEE 802.1Q, или ПК конечных клиентов, сетевые карты которых не поддерживают работу с виртуальными сетями этого стандарта.

# ПРИМЕРЫ СИСТЕМ ПЕРЕДАЧИ ДАННЫХ

## 5.1. Телефонные сети

### 5.1.1. Общие сведения

Назначение системы передачи данных — обеспечение передачи данных между абонентскими машинами и маршрутизаторами. Основными характеристиками любой СПД являются: масштаб (территория потенциального действия), пропускная способность, топология, типы используемых каналов связи, поддерживаемые сервисы.

В качестве первого примера СПД рассмотрим телефонные сети.

Если требуется соединить несколько рядом стоящих компьютеров, обычно прокладывают кабель. Однако необходимость пересечения дороги или городских коммуникаций усложняет процесс прокладки кабеля, а следовательно, возрастает стоимость этих работ. В этих случаях обычно обращаются за помощью в телефонную компанию.

Телефонная сеть создавалась давно и ее задачи были далеки от тех, которые требуется решать при передаче данных между ЭВМ. Для обеспечения качественной передачи данных по телефонной сети требуются специальные ухищрения, т.е. пришлось приложить большие усилия, чтобы научиться использовать столь низкого качества линии для передачи данных между компьютерами. Однако ситуация изменялась по мере совершенствования каналаобразующей аппаратуры, замены меди на оптоволокно и перехода на цифровые системы передачи. В настоящее время телефонные сети активно используются в компьютерных сетях, особенно класса WAN, поэтому знание принципов организации работы телефонной сети необходимо для понимания организации работы сети ЭВМ.

### 5.1.2. Немного истории

В 1876 г. А. Белл запатентовал телефон, буквально несколькими часами раньше своего основного конкурента Э. Грея [70]. Надо отметить, что открытие телефона, т.е. способа передачи звука на расстояние, произошло достаточно случайно. А. Белл был специалистом по фонетике английского языка, т.е. обучал людей хорошему произношению (вспомним профессора Хиггинса из пьесы Б. Шоу «Пиг-

малион») и мечтал создать машину, которая позволила бы представить произнесенные человеком звуки в графическом виде. Это было необходимо ему, чтобы учить говорить глухих людей. Для реализации этого проекта требовались деньги, и он решил принять участие в конкурсе, объявленном телеграфной компанией «Вестерн Юнион», на создание устройства по передаче нескольких телеграмм по одному и тому же проводу, т. е., говоря современным языком, мультиплексора для телеграфа. В ходе работ над этим мультиплексором А. Белл и открыл способ преобразования акустических волн в электромагнитные и обратно. При этом он изобрел и фонограф, обеспечивающий запись звука, но увлеченный основным проектом не осознал сделанного (позднее уже Эдисон изобрел и запатентовал фонограф).

Структура телефонной сети представлялась тогда ему очень простой. Абоненты соединялись неизолированным проводом по принципу «каждый с каждым». Роль второго провода играла Земля. Если какой-либо абонент хотел поддерживать связь с несколькими другими абонентами в городе, то к нему приходили несколько проводов, и вскоре некоторые дома стали напоминать джунгли. К 1878 г. стало ясно, что так развить телефонную сеть нельзя (рис. 5.1, а).

В 1878 г. А. Белл в городе Нью-Хевен штата Коннектикут построил первую станцию коммутации, к которой были подсоединены все абоненты. При необходимости позвонить абонент крутил ручку телефонного аппарата, вызывая оператора, сообщал, с кем он хочет соединиться, и оператор с помощью штыря соединял проводом гнезда коммутатора, к которым были подключены эти абоненты. В результате получилась структура, подобная изображенной на рис. 5.1, б.

Спустя некоторое время абоненты одного города выразили желание общаться с абонентами в других городах, т. е. потребовалось соединить между собой станции коммутации в разных городах (рис. 5.1, в).

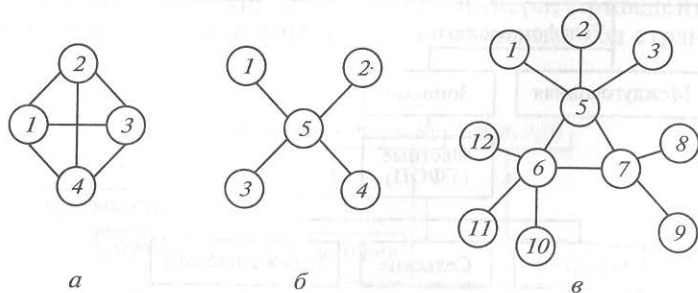


Рис. 5.1. Схемы построения телефонных сетей:

а — по принципу «каждый с каждым»; б — по радиальному принципу; в — по радиально-узловому принципу; 1... 4, 8... 12 — абоненты; 5... 7 — операторы

подразделяются на городские телефонные сети, т. е. обслуживающие город и ближайшие пригороды (ГТС), и сельские, обеспечивающие связь в пределах сельского административного района (СТС).

Учрежденческо-производственная телефонная сеть (УПТС) служит для внутренней связи предприятий, учреждений, организаций и может либо соединяться с сетью общего пользования, либо быть автономной.

Зоновая телефонная сеть включает в себя всех абонентов определенной территории, охватываемой единой семизначной нумерацией, и является частью ОАКТС. Территории зонových сетей совпадают с территориями административных областей (республик). В зависимости от конфигурации области и телефонной плотности территории нескольких областей могут быть объединены в одну зону, и наоборот, одна область может быть разделена на две зоны и более. Зоновая сеть включает в себя ГТС и СТС, причем на территории одной зоны может быть несколько ГТС и СТС. Крупные города с семизначной нумерацией абонентов, такие как Москва и С.-Петербург, выделяются в отдельные зоны.

Сельские телефонные сети охватывают более обширные территории, чем городские, так как плотность телефонных аппаратов в них значительно меньше. Следовательно, емкость автоматических телефонных станций (АТС) в сельских местностях значительно меньше, чем в городах.

Территория города делится на районы, обслуживаемые районными АТС емкостью от 10 000 до 100 000 номеров. Протяженность абонентских линий районированной ГТС сокращается, так как АТС приближаются к местам установки телефонных аппаратов. Районные АТС соединяются соединительными линиями (СЛ) по принципу «каждая с каждой».

Приведенное описание является существенным упрощением реальности, но дает достаточно полное представление об устройстве телефонной сети.

Рассмотрим структуру телефонного номера, приведенную на рис. 5.3, включающую в себя четыре компонента: код страны, код

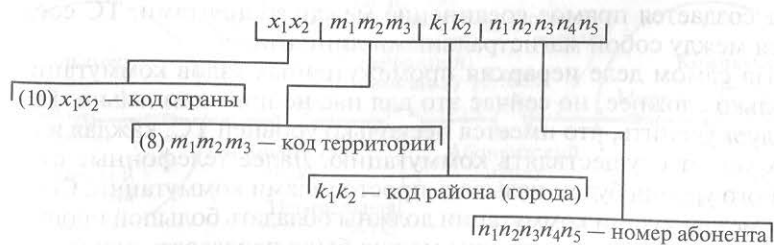


Рис. 5.3. Структура телефонного номера

К 1890 г. была осознана необходимость наличия для создания телефонной сети трех основных компонентов: локального соединения (или абонентской линии клиент—станция коммутации), станций коммутации и магистралей — протяженных соединений между станциями коммутации. Естественно, все три компонента телефонной сети постоянно совершенствовались, но в основных своих чертах они остаются более 100 лет такими, какими их создал А. Белл.

### 5.1.3. Структура телефонной сети

Структура современной телефонной сети весьма избыточная и многоуровневая. На рис. 5.2 показана структура телефонной сети России. Общегосударственная телефонная сеть (ОАКТС) Российской Федерации состоит из междугородной телефонной сети и зональных телефонных сетей. Междугородная телефонная сеть обеспечивает соединение автоматических междугородных телефонных станций (АМТС) различных зон.

Зональная телефонная сеть состоит из местных телефонных сетей, расположенных на территории зоны, и внутризональной телефонной сети, соединяющей между собой эти сети. Местные телефонные сети



Рис. 5.2. Организация телефонной сети России:

АКТС — автоматическая коммутируемая телефонная сеть; ТФОП — телефоны общего пользования

зоны в стране, затем код территории в зоне (сельского района или крупного города) и только потом номер абонента.

Код страны состоит из кода региона и собственно страны. Регионам присвоены следующие коды:

- Северная и Центральная Америка — 1;
- Африка — 2
- Европа — 3 и 4;
- Южная Америка — 5;
- страны бывшего СССР — 7;
- Центральная Азия и Дальний Восток — 8;
- Индия и Ближний Восток — 9.

В каждом из указанных регионов странам присваиваются одно-, двух- и трехзначные коды, первой цифрой в которых является код региона. Например, код 49 соответствует Германии, где 4 — код региона, а 9 — код собственно страны. При этом общее число знаков в телефонном номере не должно превышать 11.

Обратите внимание, что структура телефонного номера хорошо согласуется со структурой телефонной сети, изображенной на рис. 5.2.

Каждый абонент соединен двумя витыми парами с ближайшей местной телефонной станцией (ТС). Это соединение называется локальным соединением, абонентской линией или последней милей. В России протяженность локального соединения колеблется от сотен метров до 5 км [55], причем в городе оно короче, а в сельской местности длиннее.

Местная ТС соединена в крупных городах с районной ТС либо городской ТС. Районные и городские ТС соединены с региональными или междугородными ТС и т. д. в соответствии со структурой телефонного номера, изображенной на рис. 5.3.

Если один абонент звонит другому абоненту, который подключен к той же местной ТС, что и звонящий, то коммутаторы этой ТС соединяют абонентов напрямую. Каждая местная ТС соединена с ТС следующего уровня: районными или городскими ТС и междугородными ТС. Если один абонент звонит другому абоненту, телефон которого подключен к другой местной ТС, то местная ТС звонящего соединяется с надлежащей ТС вышерасположенного уровня, которая устанавливает соединение с местной ТС того, кому звонят. В результате создается прямое соединение между абонентами. ТС соединяются между собой магистральными линиями.

На самом деле иерархия промежуточных узлов коммутации несколько сложнее, но сейчас это для нас не принципиально. Главное следует уяснить, что имеется несколько уровней ТС, каждая из которых может осуществлять коммутацию. Далее телефонные станции любого уровня будем называть просто узлами коммутации. Соединения между узлами коммутации должны обладать большой пропускной способностью, чтобы по ним можно было передавать одновременно несколько разговоров. Пропускная способность местной линии

должна быть достаточной для одного телефонного разговора. Для абонентских линий чаще всего применяли и применяют витую пару. Для магистралей между узлами коммутации используют коаксиальные кабели, оптоволокно и радиорелейные линии на микроволнах.

В прошлом телефонная система на всех уровнях была аналоговой, т. е. по проводам передавали колебания напряжения, соответствующие акустическим колебаниям, принимаемым мембраной микрофона. С появлением цифровых методов передачи аналоговая техника стала вытесняться, и в настоящее время аналоговыми остались только абонентские линии, да и то не везде.

Итак, современная телефонная сеть включает в себя:

- абонентскую линию (соединение типа клиент—местная ТС);
- магистрали оптоволоконные или микроволновые (соединение типа ТС—ТС);
- станции коммутации (ТС).

Рассмотрим подробно функционирование и организацию этих трех компонентов телефонной сети.

#### 5.1.4. Абонентская линия

Абонентская линия, или локальное соединение, связывает абонента с ближайшим узлом коммутации. Это соединение также называется последней милей. Организация локального соединения показана на рис. 5.4, из которого видно, что при передаче данные приходится преобразовывать четыре раза из цифровой формы в аналоговую и обратно. Несмотря на то, что между узлами коммутации передача осуществляется в цифровой форме, в локальном соединении она часто аналоговая.

Напомним, что при передаче аналогового сигнала имеются три источника искажений: затухание, искажение формы, шум (см. гл. 3).

Поскольку степень телефонизации современного общества очень высока, например по России в среднем более 90 %, то абонентские

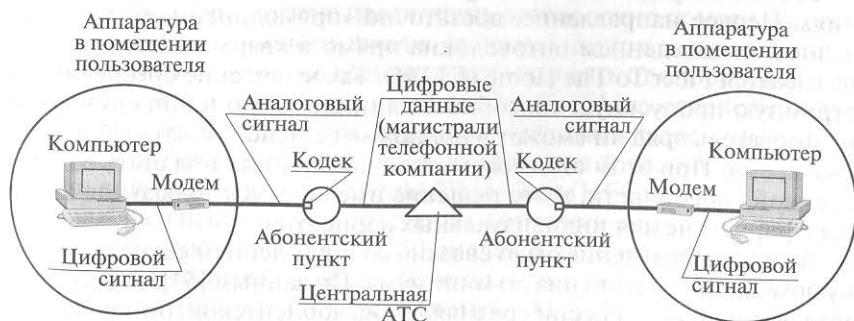


Рис. 5.4. Схема передачи цифровых данных по телефонной сети

линии представляются очень перспективными для доставки информационных услуг потребителям. Основной проблемой здесь является непригодность витой пары для высокоскоростной передачи данных. Рассмотрим несколько решений этой проблемы.

### Модем

Как мы уже знаем, из-за наличия искажений желательно использовать при передаче сигнал с как можно меньшим числом гармоник. Однако скачкообразная форма цифрового сигнала как раз требует для более точного его воспроизведения использование большого числа гармоник при передаче, а следовательно, широкой полосы пропускания канала.

Решение проблемы заключается в использовании при передаче несущей частоты в сочетании с разными способами модуляции сигнала. Три основных способа модуляции — амплитудная, частотная, фазовая и их комбинации рассматривались в гл. 3. И мы уже знаем, что устройство, которое преобразует поток битов в модулированный сигнал и обратно, называется модем.

Наряду с функциями модуляции сигнала в модем также встраиваются средства для контроля и коррекции ошибок (см. гл. 3), а также для сжатия передаваемой последовательности битов.

### Проблема последней мили

По мере развития сетевых услуг (информационного обслуживания, образования, видеоинформации по заказу и т. д.) росла потребность доступа в сеть у индивидуальных абонентов. Пропускной способности 3 кГц обычной телефонной абонентской линии стало недостаточно. Возникла проблема, как обеспечить частные квартиры и дома линиями связи надлежащей пропускной способности, — так называемая проблема последней мили.

Работы по решению этой проблемы велись в четырех направлениях. Первое направление, достаточно «прямолинейное», т. е. связанное с подведением оптоволоконного кабеля прямо в квартиру (рис. 5.5, а), называется Fiber To The Home (FTTH). Такое решение обеспечивало огромную пропускную способность линии, которую индивидуальный пользователь вряд ли сможет в полной мере использовать в ближайшее время. При этом стоимость такой линии была под стать ее пропускной способности, и это решение имело смысл только для крупных фирм, а не для индивидуальных абонентов.

Второе направление было связано со стремлением сократить длину локального соединения до минимума. По данным [53], в городских телефонных сетях России средняя длина абонентской линии составляет 1 280 м (коэффициент вариации 0,59), и ни одна абонентская линия ни в городе, ни в сельской местности не превышает 5 км.

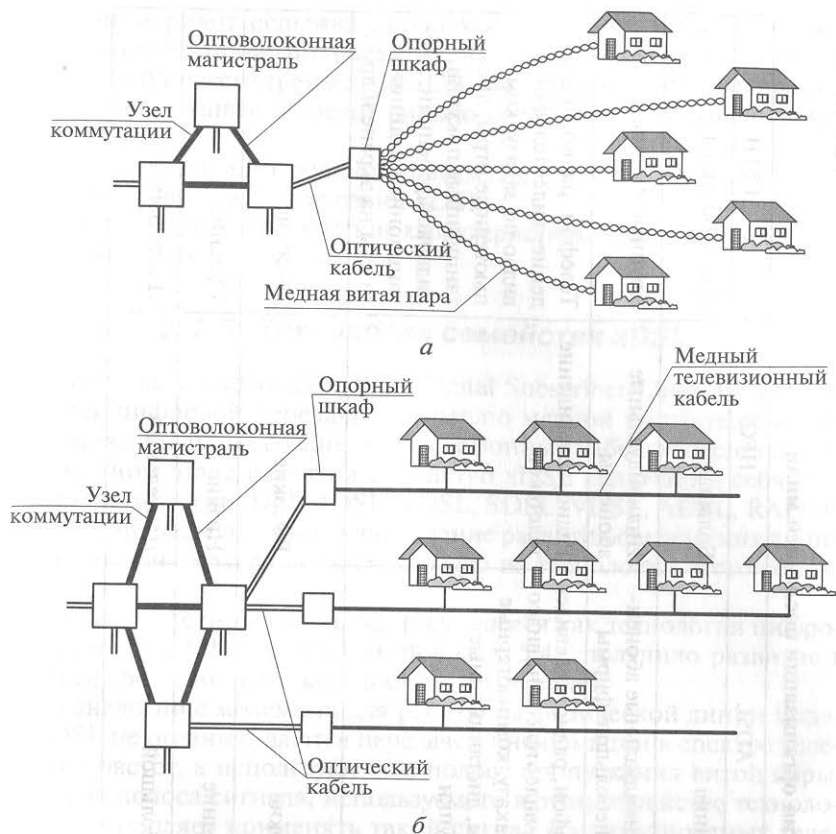


Рис. 5.5. Схемы сокращения длины абонентской линии с помощью витой пары (а) и с помощью коаксиального кабеля (б)

Поэтому было предложено протягивать оптоволоконно от местного узла коммутации до опорного шкафа развязки внутри микрорайона, а далее были возможны два варианта: использовать от опорного шкафа либо обычную витую пару с технологией HDSL из семейства xDSL (семейство этих технологий будем рассматривать далее), либо коаксиальные кабели сети кабельного телевидения (рис. 5.5, б). Это решение получило название Hybrid Fiber Coax (HFC).

Коаксиальный кабель в сочетании с оптоволоконном обеспечивают одновременную передачу 40...50 аналоговых каналов, в том числе радиовещания, телевизионных передач, телетекста. При использовании асимметричной DSL-технологии (ADSL), обеспечивающей интерактивность, добавляются видеoinформация по заказу, игры и доступ в Интернет.

## Технологии организации последней мили

Характеристика	WLL	ADSL	HFC	FTTH
Ширина полосы пропускания	Малая	Средняя	Большая	Очень большая
Круг пользователей	Индивидуальные абоненты, фирмы	Индивидуальные абоненты, небольшие фирмы	Индивидуальные абоненты	Крупные фирмы
Предоставляемые услуги	Телефон, радио, телевидение	Телефон, радио, телевидение, видеотелефон, видео по заказу, компьютерные игры, дистанционные покупки	Радио, телевидение, телетекст	Телефон, радио, телевидение, видеотелефон, видео по заказу, компьютерные игры, дистанционные покупки, видеоконференции, дистанционная медицина, газеты на экране и др.
Стоимость: первоначальные вложения вложения в развите	Низкие	Низкие	Высокие	Высокие
	Низкие	Средние	Низкие	Средние
Срок ввода в эксплуатацию	Небольшой	Небольшой	Длительный	Длительный

Третий вариант решения проблемы последней мили — это использование беспроводных технологий Wireless Local Loop — WLL, которые будут рассмотрены далее. Сейчас лишь отметим, что доступный для них диапазон частот сильно ограничен международными соглашениями.

Четвертый вариант решения рассматриваемой проблемы — это использование стандартов серии xDSL.

В табл. 5.1 приведены краткие характеристики технологий решения проблемы последней мили.

### **5.1.5. Технологии семейства xDSL**

Семейство технологий xDSL (Digital Subscriber Line) предназначено для цифровой передачи данных по медной витой паре существующих локальных соединений телефонных кабельных систем. На современном этапе развития семейство xDSL включает в себя следующие технологии: DSL, IDSL, HDSL, SDSL, VDSL, ADSL, RADSL, UADSL. Это весьма важное направление развития физических линий связи, поэтому кратко опишем каждую из технологий этого семейства.

Семейство технологий xDSL, родившееся как технология цифровых каналов в ISDN-сетях (см. подразд. 5.4), получило развитие в новой сфере — абонентском доступе в Интернет.

По аналогии с модемами для работы на физической линии модемы xDSL не ограничиваются передачей информации в спектре телефонных частот, а используют всю полосу пропускания витой пары. Широкая полоса сигнала, используемого в этом семействе технологий, не позволяет применять такой сигнал в коммутируемых телефонных линиях (телефонные коммутаторы не рассчитаны на такой спектр частот). Модемы xDSL могут работать только на участке телефонных кабельных систем между абонентом и ближайшей телефонной станцией поставщика услуг или между двумя абонентами при непосредственном соединении их абонентских линий (без участия станции коммутации). Это так называемые выделенные линии.

Технологии семейства xDSL используют спектр частот, не пересекающийся со спектром частот телефонного канала, благодаря чему по абонентской линии можно вести телефонные переговоры одновременно с передачей цифровой информации.

Рассмотрим, что представляет собой физический сигнал в xDSL-системах [10], где используется цифровое кодирование. Стандартный метод цифрового кодирования 2B1Q (см. разд. 3.2.2) применяется практически во всех типах оборудования xDSL за исключением технологий ADSL и VDSL.

Гораздо чаще в компьютерных сетях используется метод QAM и его модификация — DMT. Поскольку QAM (Quadrature Amplitude Manipulation) означает квадратурную амплитудную манипуляцию

(здесь манипуляция тождественна модуляции, применимой к цифровым сигналам), QAM-сигнал представляет собой сумму двух гармонических колебаний с амплитудами, дискретно изменяющимися и сдвинутыми на  $180^\circ$  относительно друг друга. При этом одну составляющую называют синфазной, а вторую — квадратурной.

Квадратурная амплитудная модуляция обычно является многопозиционной, т. е. за счет множества разрешенных уровней амплитуды за один такт работы модулятора может быть передано несколько бит информации. Число комбинаций (их также называют сигнальными точками) указывается через дефис в обозначении QAM, например: QAM-4, QAM-16, QAM-256. За один цикл работы модулятора QAM-16 передается 4 бит информации, а модулятора QAM-256 — 8 бит.

В настоящее время в подавляющем большинстве xDSL-линий используется DMT-модуляция (Discrete Multi-Tone), при которой все частотное пространство разбивается на 256 каналов шириной по 4 312,5 Гц, и в каждом из этих каналов используется квадратурная амплитудная модуляция с различным числом сигнальных точек. Для каждого конкретного соединения число сигнальных точек различно, т. е. передающее и приемное устройства сами выбирают число сигнальных позиций в зависимости от наличия в кабеле помех на той или иной частоте. Согласно спецификации стандарта [61] нижние семь каналов вообще никогда не используются, два канала зарезервированы для служебных целей, 25 каналов отводится на восходящий поток и 224 канала, включая служебные, — на нисходящий поток.

## Технология DSL

Технология DSL (цифровая абонентская линия) позволяет использовать существующие линии связи для передачи цифровой информации по одной витой паре со скоростью до 160 Кбит/с (при этом в прямом и обратном направлениях поддерживается одинаковая скорость). Технология разрабатывалась для организации цифровой абонентской линии BRI для сетей ISDN (см. разд. 5.4). Интерфейс DSL оборудования, предназначенного для использования в ISDN-сетях с BRI-линиями получил название IDSL. В оборудовании IDSL не предусматривается поддержка аналоговой телефонной линии, так как телефонная связь может осуществляться по цифровым каналам ISDN. В настоящее время существуют модификации оборудования DSL — Fast DSL, передающие информацию со скоростью до 256 Кбит/с.

Технология DSL поддерживает аналоговую телефонную линию. Максимальное расстояние (т. е. максимальная длина двухпроводной линии, на которой может работать аппаратура) для этой технологии составляет 6 км при диаметре жилы кабеля 0,5 мм, что вполне соответствует длине абонентских линий в России.

## Технология HDSL

Технология HDSL (High-data-rate DSL) — высокоскоростная цифровая абонентская линия. Оборудование HDSL обеспечивает дуплексный (симметричный) обмен информацией со скоростью 768 или 1024 Кбит/с по одной витой паре и 2048 Кбит/с — по двум и трем витым парам. Система является однокабельной, т.е. по каждой паре проводов осуществляются и прием, и передача информации. Неисправность, возникающая в одной паре кабеля, не приводит к прекращению передачи, а только уменьшает ее скорость. Максимальная удаленность между репитерами (промежуточными усилителями) здесь составляет не более 3 км, поэтому при использовании этой технологии в России требуется в среднем один репитер на каждую абонентскую линию. Стандартная ширина сигнала, используемого при передаче, в этом случае составляет 80...196 кГц.

Оборудование HDSL в основном предназначено для применения в корпоративных сетях. Отсутствие поддержки аналоговой телефонной линии компенсируется здесь возможностью передачи речи в цифровом виде через интерфейсы E1 (стандарт E1 будет рассмотрен в подразд. 5.1.6).

SDSL (Single Line DSL) — разновидность технологии HDSL. Системы SDSL обеспечивают дуплексную передачу потока данных со скоростью 2048 Кбит/с по одной витой паре проводов на расстояние 3...4 км при диаметре жилы кабеля 0,4...0,5 мм.

В настоящее время существенного различия между технологиями HDSL и SDSL не делают, и выпускают оборудование HDSL, передающее информацию как по нескольким, так и по одной паре проводов. Также иногда название SDSL расшифровывают как Symmetric DSL, подчеркивая тем самым симметричность потоков информации.

## Технология VDSL

Технология VDSL (Very High-data-rate DSL) находится в стадии разработки. Ожидается, что с ее помощью будет достигнута скорость передачи по абонентской линии от 12 до 51 Мбит/с. Здесь наряду с использованием медного кабеля рассматривается возможность использования оптического кабеля. Оборудование VDSL может функционировать в режиме как асимметричных, так и симметричных цифровых потоков. Применяемый метод кодирования — DMT.

Существующие образцы аппаратуры VDSL обеспечивают организацию канала связи при максимальных скоростях передачи на расстоянии не более 1,5 км. Применение оптического кабеля позволит значительно увеличить дальность связи, но потребует замены существующих медных абонентских кабелей.

Предполагается следующее разделение полосы частот:

- голосовой телефонный сервис — 0...4 кГц;
- ISDN — 4...80 кГц;
- исходящий поток — 300...700 кГц;
- входящий поток — 1 МГц.

### **Технология ADSL**

Асимметричная DSL (Asymmetric DSL) — дальнейшее развитие технологии HDSL — в настоящее время является наиболее продвинутой в семействе xDSL. Она обеспечивает передачу по витой паре потоков со скоростью до 9 Мбит/с в одном направлении (как правило, в сторону пользователя) и до 640 Кбит/с — в другом направлении. По широкому входящему каналу абонент получает данные или видеоинформацию из Интернета, а исходящий канал используется для отправки запросов на получение информации. Следует отметить, что пропускной способности исходящего канала здесь достаточно для передачи электронной почты, файлов и для проведения голосовых переговоров через Интернет. Технология ADSL ориентирована на абонентов индивидуального сектора и благодаря применению внутренних или внешних речевых разделителей позволяет вести обычные телефонные переговоры одновременно с передачей данных.

Указанные предельные скорости передачи в прямом и обратном направлениях могут быть ниже, так как они зависят от конкретного типа оборудования, кабеля и протяженности абонентской линии. Оборудование ADSL способно автоматически или принудительно настраиваться таким образом, чтобы на конкретной абонентской линии обеспечивать максимальную скорость передачи с минимальным коэффициентом ошибок. Максимальное расстояние передачи без повторителей составляет здесь 5,5 км.

Разновидностью ADSL-технологии является технология RADSL (Rate-adaptive DSL), которая может функционировать как в асимметричном режиме (ADSL), так и в симметричном (HDSL). Технология RADSL позволяет отслеживать текущее состояние кабеля (электрические параметры и уровень шума — помех) и динамически регулировать пропускную способность каналов связи, а также поддерживать максимально возможную степень передачи при требуемом минимальном уровне ошибок в канале связи.

В табл. 5.2 приведены сравнительные характеристики различных технологий семейства xDSL.

#### **5.1.6. Магистралы и мультиплексирование**

Следующим важным компонентом телефонных систем являются магистралы, соединяющие узлы коммутации разного уровня. Рассмотрим их организацию и функционирование.

Сравнение характеристик различных технологий семейства xDSL

Технология	ADSL	HDSL	SDSL	VDSL
Скорость	1,5...9 Мбит/с — входящий трафик; 16...640 Кбит/с — исходящий трафик	1,544 или 2,048 Мбит/с	1,544 или 2,048 Мбит/с	13...52 Мбит/с — входящий трафик; 1,5...2,3 Мбит/с — исходящий трафик
Режим	Асимметричный	Симметричный	Симметричный	Асимметричный
Число пар проводов	1	2	1	1
Радиус действия (неэкранированная витая пара)	3,7...5,5 км	3,7 км	3,0 км	1,4 км
Тип сигнала	Аналоговый	Цифровой	Цифровой	Аналоговый
Метод кодирования	DMT	2B1Q	2B1Q	DMT
Частота	1...5 МГц	196 кГц	196 кГц	10 МГц

Одним из существенных факторов, определяющих организацию магистрали, был и остается экономический. Дело в том, что затраты на прокладку кабеля в значительной степени обуславливают внешние условия (город, сельская местность, необходимая глубина залегания кабеля, наличие инженерных коммуникаций и т. д.), а не технические характеристики, например пропускная способность. Следовательно, чем больше абонентов смогут использовать один и тот же кабель, тем быстрее окупятся затраты на его прокладку и тем дешевле будет стоить каждому из них эксплуатация этого кабеля.

Вспомним историю. Компания «Вестерн Юнион» объявила в свое время конкурс на решение проблемы передачи нескольких телеграмм по одной линии, которым заинтересовался А. Белл. За 100 лет существования телефона были инвестированы огромные средства в создание методов и оборудования, позволяющих использовать одну и ту же магистраль одновременно для передачи нескольких разговоров. Такой технический прием называется мультиплексированием, или уплотнением. Мы будем использовать термин мультиплексирование.

Созданные в телефонии схемы мультиплексирования можно подразделить на два больших класса: мультиплексирование с разделением частот (Frequency Division Multiplexing) и мультиплексирование с разделением по времени (Time Division Multiplexing). Кроме того, были разработаны методы мультиплексирования на основе разделения длин волн (WDM — Wavelength Division Multiplexing) и на основе разделения кодов (CDM — Code Division Multiplexing). Метод разделения длин волн применяется в оптоволоконных системах. Методы разделения кодов используются в системах беспроводной связи, и некоторые из них рассматривались в гл. 3 при обсуждении семейства стандартов WiFi и в гл. 4 при обсуждении метода CDMA.

## **Мультиплексирование с разделением частот**

Идея мультиплексирования с разделением частот заключается в следующем (см. гл. 2): весь диапазон частот полосы пропускания кабеля разбивается на поддиапазоны, которые называются каналами. По каждому каналу производится независимая передача.

Рассмотрим, например, как с помощью метода мультиплексирования с разделением частот три телефонных канала можно мультиплексировать, т. е. объединить (уплотнить) в одной магистрали. Вся полоса пропускания магистрали разбивается на полосы шириной в 3 кГц. С помощью фильтров полоса пропускания каждого канала ограничивается шириной 3 000 Гц, но в своем диапазоне частот. При мультиплексировании большого числа каналов полоса пропускания увеличивается до 4 000 Гц в целях предотвращения «залезания» одной полосы на другую (по 500 Гц с каждой стороны) и тем самым уменьшается интермодуляционный шум.

Объединение 12 голосовых каналов с пропускной способностью по 4 000 Гц в полосе от 60 до 108 кГц называется *группой*. Пять групп по 12 каналов мультиплексируют в супергруппу, а пять супергрупп — в мастергруппу. Современные стандарты МСЭ позволяют объединять до 230 000 голосовых каналов.

### **Мультиплексирование с разделением длин волн**

Этот способ мультиплексирования, используемый для волоконно-оптических каналов, заключается в следующем.

Два волоконно-оптических кабеля с импульсами разной длины волны подводятся к одной призме. Свет, пройдя через эту призму (или дифракционную решетку), смешивается в единый луч, который на другом конце разделяется с помощью другой такой же призмы. Поскольку каждый канал занимает лишь несколько гигагерц, а пропускная способность одного оптоволоконного канала около 25 000 ГГц (быстрее преобразовывать световой сигнал в электрический пока не получается), то возможности оптоволоконна для мультиплексирования огромны. Метод мультиплексирования с разделением длин волн применяется в технологии FTTN (см. подразд. 5.1.4).

### **Мультиплексирование с разделением по времени**

Мультиплексирование с разделением по времени, или TDM-мультиплексирование (Time Division Multiplexing), предполагает использование цифрового оборудования и хорошо соответствует возможностям компьютера. Следует отметить, что такое мультиплексирование подходит для работы только с данными в цифровой форме, поэтому, поскольку по абонентской линии телефонный сигнал передается в аналоговой форме, его надо сначала оцифровать.

Оцифровка сигнала происходит на местном узле коммутации, где сходятся абонентские линии с аналоговыми сигналами. На местном узле коммутации аналоговые сигналы с абонентских линий оцифровываются, объединяются и передаются на узлы коммутации следующего уровня по магистральным шинам. Рассмотрим, как это происходит.

В подразд. 3.2.4 подробно рассматривались методы оцифровки аналоговых сигналов, т.е. преобразования аналоговых сигналов в цифровую форму. Напомним только, что преобразование аналогового сигнала в цифровые и цифровых в аналоговые осуществляет специальное устройство, называемое кодек (coder-decoder). Имеется два основных метода преобразования аналогового сигнала в цифровую форму и обратно. Это метод импульсно-кодовой модуляции (ИКМ-метод) и разностный метод дельта-модуляции.

Напомним, что при ИКМ аналоговая линия сканируется в соответствии с теоремой Котельникова с удвоенной частотой старшей

гармоники, например в телефонных системах с частотой 8 000 Гц. Амплитуда аналогового сигнала в этом случае разбивается на определенное число уровней, и при каждом замере определяется не абсолютное значение сигнала, а его уровень. Номер этого уровня и передается в виде двоичного кода.

Когда ИКМ начала развиваться, МСЭ не смогло сразу ввести единый стандарт на применение этого метода в телефонии. В результате появились два варианта стандарта: Е1 — европейский и Т1, получивший распространение в США и Японии.

Стандарт Е1 предполагает мультиплексирование 30 каналов. Каждая из 30 линий сканируется с частотой 8 000 Гц. Результаты каждого измерения представляют 8-битовое число. Это означает, что в методе ИКМ используются 256 уровней. В стандарте Т1 используют 7 бит, т. е. 128 уровней.

Полученные 240 бит упаковывают в кадр. Кадр в стандарте Е1 содержит 32 канала по восемь разрядов и занимает 125 мкс. При этом 30 каналов используется для передачи данных, а два — для целей управления. Таким образом, стандарт Е1 обеспечивает скорость передачи 2,048 Мбит/с и мультиплексирует 30 линий одновременно.

Стандарт Т1, структура которого показана на рис. 5.6, позволяет мультиплексировать 24 линии, но в каждом канале под данные используется лишь семь разрядов и один разряд для целей управления. Кадр в стандарте Т1 содержит 193 бит и занимает те же 125 мкс, что и в стандарте Е1, обеспечивая скорость передачи 1,544 Мбит/с. Отметим также, что в Е1 из 256 бит кадра 16 бит используются для служебных целей, а в Т1 из 193 бит для служебных целей используются 24 бит, т. е. Е1 экономичней.

Так как аналоговый сигнал оцифрован, возникает искушение сжать передаваемые данные. Примером такого сжатия может служить метод *дифференциальной импульсно-кодовой модуляции*, основанного на том, что если разность между последовательными замерами сигнала не превосходит, например 8 уровней, в то время как соб-

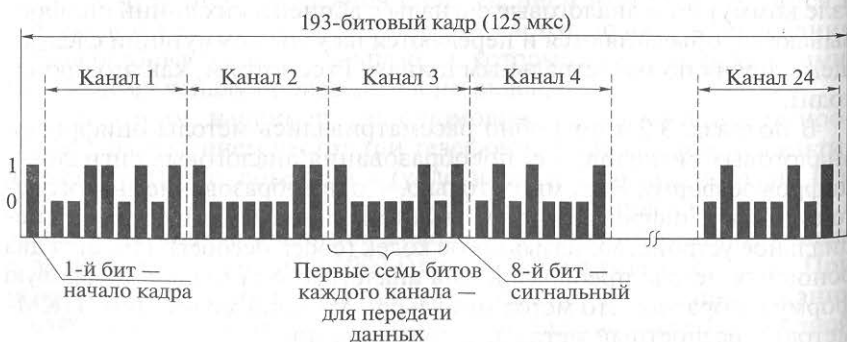


Рис. 5.6. Структура кадра по стандарту Т1

ственно значения этого сигнала колеблются в диапазоне  $\pm 64$  единицы, то вместо 6 разрядов цифрового кода требуется всего 3 уровня. Частным случаем такого подхода является дельта-модуляция (см. подразд. 3.2.4), при котором предполагается, что соседние значения сигнала отличаются не более чем на  $\pm 1$ . При передаче голоса этот метод работает неплохо.

Другой метод сжатия данных основан на экстраполяции очередного значения сигнала на основе предыдущих значений. Это так называемый метод *статистической импульсно-кодовой модуляции*, в котором передается разница между предсказанием и фактическим значением сигнала. Очевидно, что при этом на обоих концах канала должен использоваться один и тот же алгоритм предсказания.

TDM-мультиплексирование позволяет мультиплексировать уже мультиплексированные каналы. Так, согласно стандарту T1 четыре канала уровня T1 можно объединить в один канал уровня T2, затем шесть каналов уровня T2 объединить в один канал уровня T3 и семь каналов уровня T3 — в один канал уровня T4. В результате на уровне T4 максимальная скорость передачи будет равна 274,176 Мбит/с.

Согласно стандарту E1 группировать можно только четыре канала, однако в этом случае будет четыре уровня вложенности, а не три, как в стандарте T1, поэтому скорость передачи составит на уровне E1 2,048, на E2 — 8,848, на E3 — 34,304, на E4 — 139,264, а на E5 — 565,148 Мбит/с.

### Технология мультиплексирования SONET

Технология SONET (Synchronous Optical NETwork) была разработана американской компанией Bell Core и стандартизована ANSI для построения сетей передачи данных по оптическим линиям связи. Позднее МСЭ выпустил стандарт, совместимый с SONET и названный SDH (Synchronous Digital Hierarchy), который был опубликован в рекомендациях G.707, G.708, G.709. Этот стандарт был разработан в целях устранения разнобоя в передаче сигналов по оптоволоконным линиям в телефонии. Такие линии применяются для создания высокоскоростных каналов между телефонными станциями уровней района и выше.

На первых порах каждая телефонная компания устанавливала свои стандарты TDM-мультиплексирования по оптическим линиям связи. В настоящее время многие телефонные компании, в том числе и в России, на своих магистральных линиях используют стандарт SDH.

Создание стандарта SONET преследовало четыре основные цели:

- обеспечить возможность использования разных физических сред в телефонной сети, что требовало проработки стандартов кодировки на физическом уровне, выбора длины волны, частоты, временных характеристик сигналов, структуры кадра;

- унифицировать американские, европейские и японские цифровые системы, в которых используются каналы с пропускной способностью 64 Кбит/с с импульсно-кодовой модуляцией;

- обеспечить иерархическое мультиплексирование нескольких цифровых каналов (на сегодня его используют до уровня T3, хотя стандарт определяет и уровень T4);

- определить правила функционирования, администрирования и поддержки оптических каналов связи.

С самого начала было принято решение использовать в стандарте SONET традиционное TDM-мультиплексирование, где вся ширина оптоволоконной линии используется под один канал, содержащий временные слоты подканалов. Следовательно, SONET создавали как синхронную систему, в которой имеются главные часы, тактирующие ее работу с частотой  $10^{-9}$  с с высокой степенью точности.

Биты на линии SONET имеют строго выверенную длительность, контролируемую главными часами. Когда позднее для высокоскоростного ISDN был предложен метод передачи, где кадры могли поступать через нерегулярные интервалы времени, то этот метод в противоположность SONET был назван асинхронным, а сейчас он известен как ATM (см. подразд. 5.4.9).

Система передачи данных SONET состоит из коммутаторов, мультиплексоров и повторителей, соединенных оптическими линиями. В терминологии SONET сплошной фрагмент оптоволоконного кабеля между двумя устройствами называется секцией. Канал между двумя мультиплексорами (возможно с несколькими повторителями между ними) называется линией. Канал между двумя оконечными абонентами называется путем.

Кадр SONET содержит 810 байт и занимает 125 мкс. Стандарт SONET допускает разные топологии каналов связи, но чаще это двунаправленное кольцо (поясим это при рассмотрении системы FDDI). Так как система SONET синхронная, то кадры генерируются строго один за другим без перерывов вне зависимости от того, имеются данные для передачи или нет. Скорость передачи 8 000 кадров/с как раз соответствует каналам с ИКМ-модуляцией, используемым в цифровой телефонии. Исходя из этого, нетрудно подсчитать, что пропускная способность канала SONET составляет 51,84 Мбит/с.

Для описания кадра SONET представим его 810 байт в виде матрицы из 9 строк и 90 столбцов, как показано на рис. 5.7 [40]. Каждый элемент такой матрицы — один байт. Первые три элемента в каждой строке — это служебная информация, используемая для администрирования и управления передачей. Первые три элемента первых трех строк образуют заголовок секции, а каждые три первых элемента в следующих шести строках — заголовок линии. Заголовки секции генерируются и проверяются в начале и в конце каждой секции. Аналогично генерируются и проверяются заголовки на каждой линии.

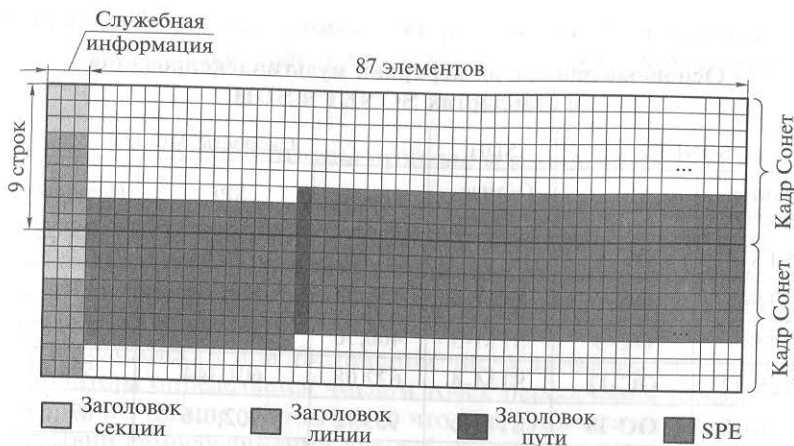


Рис. 5.7. Устройство кадра SONET

Скорость передачи 8 000 кадров/с соответствует основному каналу, называемому Synchronous Transport Signal-1 (STS-1).

Оставшиеся в 87 столбцах и 9 строках 783 байт приходятся на данные пользователей, которые образуют так называемый SPE-конверт (Synchronous Payload Envelope), содержащий как данные пользователя, так и служебную информацию, которая занимает 13 байт. SPE-конверт может начинаться с любого байта в оставшихся  $9 \times 87$  байтах. Начало SPE-конверта указано в первых двух байтах третьей строки. Учитывая, что в SONET генерируется 8 000 кадров в секунду, получаем, что полезная пропускная способность составит

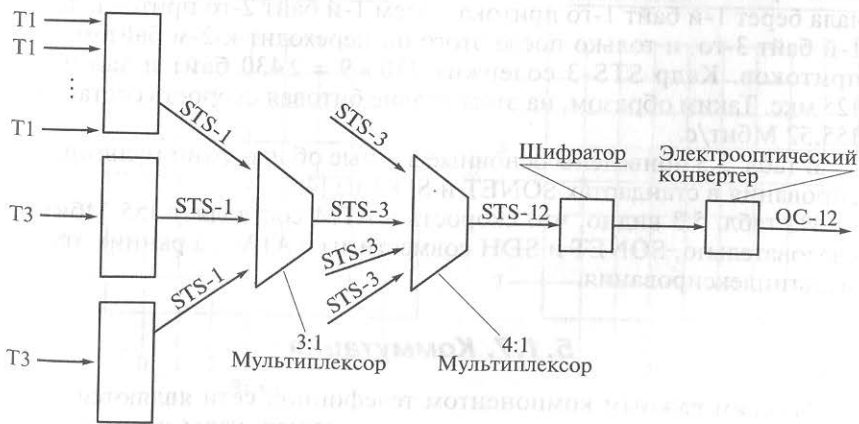


Рис. 5.8. Мультиплексирование множественных потоков данных в системе SONET

**Основные данные об иерархии мультиплексирования  
в стандартах SONET и SDH**

SONET		SDH	Скорость, Мбит/с		
Электрическое	Оптическое	Оптическое	Брутто	SPE	Пользователь
STS-1	OC-1		51,84	50,112	49,536
STS-3	OC-3	STM-1	155,52	150,336	148,608
STS-9	OC-9	STM-3	466,56	451,008	445,824
STS-12	OC-12	STM-4	622,08	601,344	594,432
STS-18	OC-18	STM-6	933,12	902,016	891,648
STS-24	OC-24	STM-8	1 244,16	1 202,688	1 188,864
STS-36	OC-36	STM-12	1 866,24	1 804,032	1 783,296
STS-48	OC-48	STM-16	2 488,32	2 405,376	2 377,728

$8\,000 \times 783 \times 8 = 50,112$  Мбит/с. Нетрудно увидеть, что такая организация работы канала предполагает плотную его загрузку со стороны абонентов (сравните с организацией работы каналов по IEEE 802).

Мультиплексирование множественных потоков данных, называемых в системе SONET притоками, показано на рис. 5.8. Мультиплексирование происходит побайтно. Например, когда три притока STS-1, каждый из которых имеет скорость 51,84 Мбит/с, объединяются в один приток STS-3 со скоростью 155,52 Мбит/с, мультиплексор сначала берет 1-й байт 1-го притока, затем 1-й байт 2-го притока, затем 1-й байт 3-го, и только после этого он переходит к 2-м байтам этих притоков. Кадр STS-3 содержит  $270 \times 9 = 2\,430$  байт и занимает 125 мкс. Таким образом, на этом уровне битовая скорость составляет 155,52 Мбит/с.

В табл. 5.3 приведены основные данные об иерархии мультиплексирования в стандартах SONET и SDH из [40].

Из табл. 5.3 видно, что скорость в ATM составляет 155 Мбит/с, следовательно, SONET и SDH совместимы с ATM на ранних этапах мультиплексирования.

### 5.1.7. Коммутация

Третьим важным компонентом телефонной сети являются телефонные станции, или, как их еще называют, узлы коммутации, основу которых составляют коммутаторы. В телефонных сетях используются два разных способа коммутации: коммутация каналов и

коммутиация пакетов, которые уже рассматривали в подразд. 2.1.2. Рассмотрим сначала работу коммутаторов в случае коммутации каналов.

### Коммутаторы прямые и каскадные

Самым простым видом является прямой коммутатор типа  $n \times n$ , т.е. коммутатор, имеющий  $n$  входных и  $n$  выходных линий (рис. 5.9), в точках пересечения которых установлены полупроводниковые переключатели, обеспечивающие замыкание соответствующих линий.

Основной недостаток коммутаторов этого типа — квадратичный рост их сложности при увеличении числа линий  $n$ , т.е. сложность коммутатора определяется числом точек пересечения (соединения) этих линий. Даже с учетом того, что для дуплексных линий и при отсутствии самосоединений для работы требуется только половина соединений (выше или ниже главной диагонали), то все равно необходимо иметь порядка  $n(n-1)/2$  переключателей. При  $n = 1000$  на кристалле можно поместить такое количество переключателей, но при этом у него должно быть 2000 ножек, что обеспечить очень не просто. Поэтому такие прямолинейные решения схем коммутаторов возможны лишь для небольших организаций.

На рис. 5.10 показаны схемы каскадных коммутаторов. Идея построения таких коммутаторов заключается в разделении прямого коммутатора на части и соединении этих частей между собой промежуточными дополнительными коммутаторами.

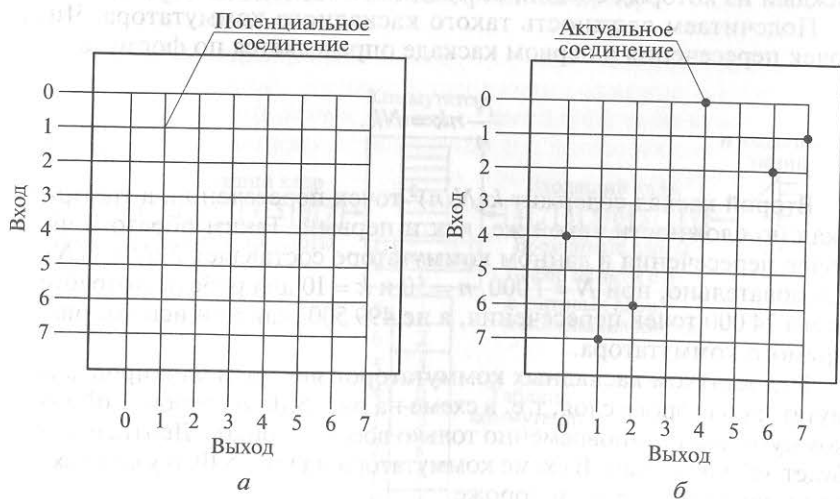


Рис. 5.9. Схемы прямых коммутаторов с потенциальным (а) и актуальным (б) соединениями

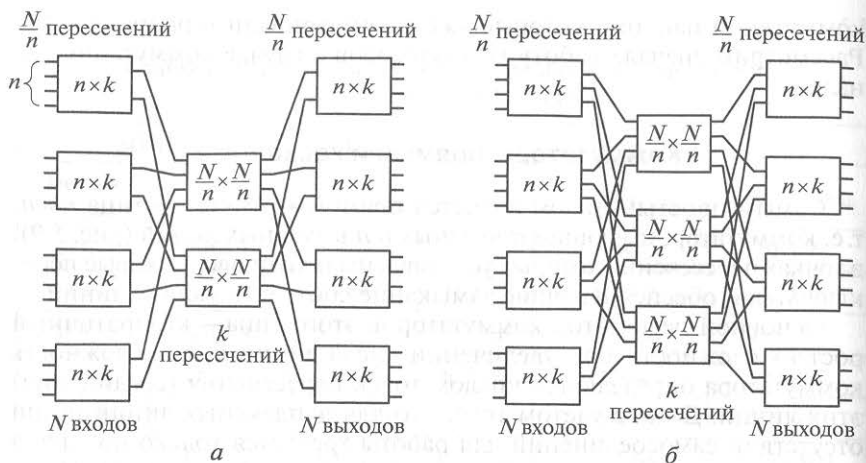


Рис. 5.10. Схемы каскадных коммутаторов:  
 а — при  $N = 16$ ,  $n = 4$ ,  $k = 2$ ; б — при  $N = 16$ ,  $n = 4$ ,  $k = 3$

Рассмотрим для примера трехслойный каскадный коммутатор. В первом слое такого коммутатора  $N$  входных линий разбивают на группы по  $n$  линий в каждой группе. Каждую из  $N/n$  групп обслуживает прямой коммутатор  $n \times k$ . Во втором слое  $k$  прямых коммутаторов обеспечивают соединение  $Nk/n$  входных линий с  $Nk/n$  выходными линиями. Третий слой состоит из  $N/n$  прямых коммутаторов, каждый из которых соединяет  $k$  линий с  $n$  линиями.

Подсчитаем сложность такого каскадного коммутатора. Число точек пересечения в первом каскаде определяется по формуле

$$\frac{N}{n}nk = Nk.$$

Второй каскад содержит  $k(N/n)^2$  точек пересечения, а третий каскад по сложности такой же, как и первый. Таким образом, число точек пересечения в данном коммутаторе составляет  $2kN + k(N/n)^2$ . Следовательно, при  $N = 1000$ ,  $n = 50$  и  $k = 10$  для работы потребуется всего 24 000 точек пересечения, а не 499 500, как при использовании прямого коммутатора.

Недостатком каскадных коммутаторов является блокировка коммутаторов второго слоя, т. е. в схеме на рис. 5.10, а второй слой может коммутировать одновременно только восемь звонков. Девятый звонок будет заблокирован. В схеме коммутатора на рис. 5.10, б уже 12 входов во втором слое, но он и дороже.

В 1953 г. Клос показал, что при  $k = 2n - 1$  блокировок в каскадных коммутаторах не будет [62].

## Коммутаторы с разделением времени

На рис. 5.11 показана схема коммутатора с разделением времени. Пусть имеется  $n$  линий, которые необходимо коммутировать. Эти линии сканируют последовательно одна за другой в течение определенного временного слота.

Образуется кадр из  $n$  ячеек по  $k$  бит в каждой. Например, в стандарте Е1 каждая ячейка содержит 8 бит, кадр — 32 ячейки, а всего за секунду проходит 8 000 кадров.

Затем кадр попадает в коммутатор ячеек, который переставляет ячейки в соответствии с таблицей коммутации. Обработка кадра происходит следующим образом. Входной кадр записывается в память в том порядке, в каком ячейки считывались с линий. Затем ячейки считываются из памяти в порядке, задаваемом таблицей коммутации.

Ясно, что таблица коммутации — это вектор перестановок, а скорость коммутации ограничена скоростью считывания из памяти. Например, если временной слот составляет 125 мкс, и требуется обработать кадр из  $n$  ячеек, а время считывания из памяти  $T$ , мкс, то  $2nT = 125$  мкс или  $n = 125/(2T)$ . Если скорость работы памяти 100 нс, то можно обработать не более 625 линий.

Итак, мы закончили рассмотрение организации и функционирования телефонных сетей и поняли, что телефонная сеть как СПД предоставляет возможность создания физического канала для передачи данных, поверх которого можно использовать разные протоколы канального уровня, и в этой СПД действует единая система адресации, где адрес абонента — его телефонный номер.



Рис. 5.11. Коммутатор с разделением времени

## 5.2. Системы FDDI

### 5.2.1. Основы технологии FDDI

К середине 1980-х гг. у исследовательских центров США возникла потребность в высокоскоростных надежных и территориально протяженных локальных сетях для объединения суперкомпьютерных центров. При этом основной задачей являлось обеспечение возможности передачи больших объемов данных между узлами сети, которые находятся на достаточном удалении друг от друга. Существовавшие на тот момент стандарты локальных сетей семейства IEEE 802 не обеспечивали требуемого качества сервиса и технических характеристик, поэтому институт ANSI занялся разработкой нового стандарта, который получил впоследствии наименование X3T9.5, или FDDI (Fiber Distributed Data Interface). Этот стандарт предполагает использование оптоволоконных линий связи, скорость передачи не ниже 100 Мбит/с и распространение действия сетей на расстояния большие, чем в уже рассмотренных стандартах IEEE 802.

Основы технологии FDDI рассмотрим в соответствии с [33]. Эта технология является высокопроизводительным развитием технологии Token Bus [40], позволяющей работать со скоростями не ниже 100 Мбит/с на расстоянии до 200 км и объединяющей до 1 000 рабочих станций.

Разработчики технологии FDDI ставили перед собой в качестве наиболее приоритетных следующие цели:

- повысить скорость передачи данных до 100 Мбит/с;
- повысить отказоустойчивость СПД за счет стандартных процедур восстановления после отказов различного рода — повреждения кабеля, некорректной работы узла, концентратора, возникновения высокого уровня помех на линии и т. п.;
- максимально эффективно использовать потенциальную пропускную способность СПД как для асинхронного, так и для синхронного трафика.

СПД FDDI строится на основе двух оптоволоконных колец, по одному из которых трафик направлен по часовой стрелке, а по дру-

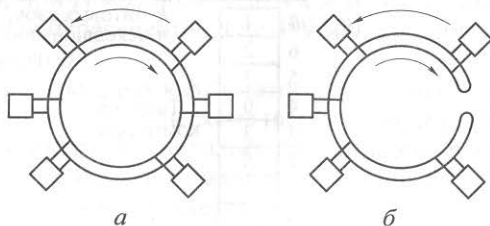


Рис. 5.12. Реконфигурация двух колец (а) в одно (б)

гому — против часовой стрелки. При этом в случае выхода из строя одного из колец его трафик может быть запущен через второе кольцо. Если оба кольца окажутся поврежденными в одном и том же месте, то они могут быть объединены в одно кольцо, как показано на рис. 5.12. Такая реконфигурация производится силами концентраторов и (или) сетевых адаптеров FDDI.

Использование двух колец — это основной способ повышения отказоустойчивости FDDI, и чтобы им воспользоваться, узел должен быть подключен к обоим кольцам. В нормальном режиме работы СПД данные проходят через все узлы и все участки кабеля первичного (Primary) кольца, поэтому этот режим называется Thru — сквозным или транзитным. Вторичное кольцо (Secondary) в этом режиме не используется. При образовании общего кольца из двух колец передатчики станций по-прежнему остаются подключенными к приемникам соседних станций, что позволяет правильно передавать и принимать информацию соседним станциям.

В стандартах FDDI отводится много внимания различным процедурам, которые позволяют определить наличие отказа, а затем произвести необходимую реконфигурацию. СПД FDDI может полностью восстанавливать свою работоспособность в случае единичных отказов ее элементов. При множественных отказах СПД распадается на несколько не связанных СПД.

Кольца в СПД FDDI рассматриваются как общая разделяемая среда передачи данных, поэтому для нее определен специальный метод доступа. Этот метод очень близок к методу доступа в сетях Token Ring и также называется методом кольца с маркером. Станция может начать передачу своих собственных кадров данных только в том случае, если она получила от предыдущей станции специальный кадр — маркер доступа. После этого она может передавать свои кадры в течение времени, называемого временем удержания маркера (Token Holding Time — ТНТ). После истечения значения ТНТ станция обязана завершить передачу своего очередного кадра и передать маркер доступа следующей станции. Если же в момент получения маркера у станции нет кадров для передачи, то она немедленно передает маркер следующей станции.

У каждой станции имеется предшествующий сосед (upstream neighbor) и последующий сосед (downstream neighbor), определяемые ее физическими связями и направлением передачи информации. Каждая станция постоянно принимает передаваемые ей предшествующим соседом кадры и анализирует их адрес назначения. Если адрес назначения не совпадает с ее собственным, то она транслирует кадр своему последующему соседу. Напомним, что если станция получила маркер и передает свои собственные кадры, то на протяжении этого периода времени она не транслирует приходящие кадры, а удаляет их. Если же адрес кадра совпадает с адресом станции, то она копирует этот кадр в свой внутренний буфер, проверяет его коррект-

ность (с помощью контрольной суммы), передает его поле данных для последующей обработки протоколу, расположенному выше FDDI-уровня (например, IP), а затем передает исходный кадр по кольцу последующей станции.

В передаваемом по кольцу кадре станция-получатель отмечает три признака: распознавания адреса, копирования кадра и отсутствия или наличия в нем ошибок. Станция-отправитель проверяет эти признаки и таким образом определяет, дошел ли кадр до станции получателя и не был ли он при этом поврежден. Процесс восстановления информационных кадров не входит в функции протоколов FDDI, этим должны заниматься протоколы более высоких уровней.

### **5.2.2. Протоколы технологии FDDI**

В технологии FDDI используются протокол физического уровня и протокол подуровня доступа к среде (MAC) канального уровня. Как и во многих других технологиях передачи данных, в технологии FDDI используется также протокол 802.2 подуровня управления каналом данных (LLC), определенного в стандартах IEEE 802.2 и ISO 8802.2, при котором узлы работают в дейтаграммном режиме, т. е. без установления соединений и без восстановления потерянных или поврежденных кадров.

Физический уровень подразделяется на независимый от среды подуровень PHY (Physical) и зависящий от среды подуровень PMD (Physical Media Dependent). Работу всех уровней контролирует протокол управления станцией SMT (Station Management). Напомним, что мы уже сталкивались с таким делением на подуровни при рассмотрении семейства Ethernet IEEE 802.3. Аналогично организован физический уровень в СПД АТМ.

Подуровень PMD обеспечивает необходимые средства для передачи данных от одной станции к другой по оптоволокну. В его спецификации определяются:

- требования к мощности оптических сигналов и к многомодовому оптоволоконному кабелю;
- требования к оптическим обходным переключателям (optical bypass switches) и оптическим приемопередатчикам;
- параметры оптических разъемов MIC (Media Interface Connector) и их маркировка;
- длина волны 1300 нм, на которой работают приемопередатчики;
- представление сигналов в оптических волокнах в соответствии с кодировкой NRZI-1.

Подуровень PHY выполняет кодирование и декодирование данных, циркулирующих между подуровнями MAC и PMD, а также обеспечивает тактирование информационных сигналов. В его спецификации определены:

- правила кодирования информации в соответствии со схемой 4В/5В (которая рассматривалась при изучении Fast Ethernet);
- правила тактирования сигналов;
- требования к стабильности тактовой частоты 125 МГц;
- правила преобразования информации из параллельной формы в последовательную.

Подуровень MAC ответственен за управление доступом к сети, а также за прием и обработку кадров данных. В его спецификации определены:

- правила захвата и передачи маркера;
- правила формирования кадра;
- правила генерации и распознавания адресов;
- правила вычисления и проверки 32-разрядной контрольной суммы.

Уровень SMT выполняет все функции по управлению и мониторингу остальных уровней стека протоколов FDDI. В управлении кольцом принимает участие каждый узел сети FDDI, поэтому все узлы обмениваются специальными кадрами SMT для управления сетью. В спецификации SMT определены:

- алгоритмы обнаружения ошибок и восстановления после сбоя;
- правила мониторинга работы кольца и станций;
- алгоритм управления кольцом;
- процедуры инициализации кольца.

### **5.2.3. Типы узлов и правила их соединения**

Все станции в СПД FDDI подразделяются на конечные станции и концентраторы, а также их различают по способу присоединения к первичному и вторичному кольцам и по числу MAC-адресов у одной станции.

Для того чтобы передавать собственные данные в кольцо (а не просто ретранслировать данные соседних станций), станция должна иметь в своем составе хотя бы один MAC-узел со своим уникальным MAC-адресом. Станции могут не иметь ни одного MAC-узла, а значит, участвовать только в ретрансляции чужих кадров, но обычно все станции в СПД FDDI, даже концентраторы, имеют хотя бы один MAC-узел. Концентраторы используют MAC-узел для захвата и генерации служебных кадров, например кадров инициализации кольца, кадров поиска неисправности в кольце и т. п.

### **5.2.4. Функции MAC-подуровня**

Подуровень MAC выполняет в технологии FDDI следующие функции:

- поддерживает сервисы для подуровня LLC;
- формирует кадр определенного формата;
- управляет процедурой передачи маркера;
- управляет доступом станции к среде;
- обеспечивает адресацию станции;
- копирует кадры, предназначенные для данной станции, в буфер и уведомляет подуровень LLC и блок управления станцией SMT о прибытии кадра;
- генерирует контрольную сумму кадра с помощью CRC-кода и проверяет ее у всех кадров, циркулирующих по кольцу;
- удаляет из кольца все кадры, которые сгенерировала данная станция;
- управляет таймерами, которые контролируют логическую работу кольца, т. е. таймером удержания маркера, таймером оборота маркера и т. д.;
- осуществляет мониторинг определенных событий, что помогает обнаружить и локализовать неисправности;
- определяет механизмы, используемые кольцом для реакции на ошибочные ситуации, т. е. на повреждение кадра, потерю кадра, потерю маркера и т. д.

В каждом блоке подуровня MAC параллельно работают два процесса: процесс передачи символов (MAC Transmit) и процесс приема символов (MAC Receive). За счет этого подуровень MAC может одновременно передавать символы одного кадра и принимать символы другого кадра.

### Форматы кадра и маркера

В СПД FDDI информация передается в форме двух блоков данных: кадра и маркера. Формат кадра FDDI представлен на рис. 5.13.

Рассмотрим назначение полей кадра.

*Преамбула (PA)*. Любой кадр должен предваряться преамбулой, состоящей как минимум из 16 символов Idle (I). Эта последовательность сигналов предназначена для синхронизации приемника и передатчика кадра.

*Начальный ограничитель (Starting Delimiter — SD)*. Состоит из пары символов JK, которые позволяют однозначно определить границы для остальных символов кадра.

*Поле управления (Frame Control — FC)*. Идентифицирует тип кадра и детали работы с ним. Имеет 8-битовый формат и передается с помощью двух символов. Состоит из подполей, обозначаемых CLFFZZZZ, которые имеют следующее назначение:

- C — определяет тип трафика, который переносит кадр (синхронный — значение 1, асинхронный — значение 0);
- L — определяет длину адреса кадра, который может занимать 2 или 6 байт;

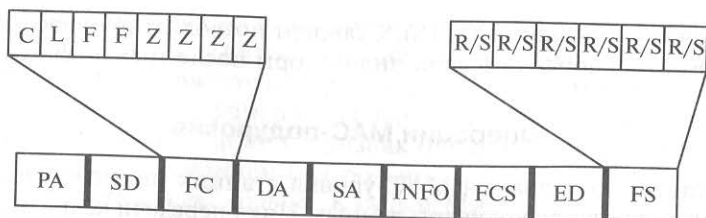


Рис. 5.13. Формат кадра FDDI

- FF — определяет тип кадра (01 — обозначение кадра LLC (пользовательских данных), 00 — обозначение служебного кадра MAC-подуровня). Служебными кадрами MAC-подуровня являются кадры процедуры инициализации кольца Claim Frame, кадры процедуры сигнализации о логической неисправности Beacon Frame и кадры процедуры управления кольцом SMT Frame;

- ZZZZ — детализирует тип кадра.

**Адрес назначения** (Destination Address — DA). Идентифицирует станцию (уникальный адрес) или группу станций (групповой адрес), которым предназначен кадр. Может содержать 2 или 6 байт.

**Адрес источника** (Source Address, SA). Идентифицирует станцию, сгенерировавшую данный кадр. Это поле должно быть той же длины, что и поле адреса назначения.

**Информация** (INFO). Содержит информацию, относящуюся к операции, указанной в поле управления. Может иметь длину от 0 до 4 478 байт (от 0 до 8 956 символов). Стандарт FDDI допускает размещение в этом поле информации о маршруте для алгоритма маршрутизации от источника (Source Routing), устанавливаемого стандартом 802.5, который определяет работу СПД «Кольцо с маркером» (Token Ring). При этом в два старших бита поля адреса источника SA помещается комбинация 102 — групповой адрес, не имеющая отношения к адресу источника, а обозначающая присутствие информации о маршруте в поле данных.

**Контрольная последовательность** (Frame Check Sequence — FCS). Содержит 32-битовую последовательность, вычисленную стандартным методом CRC-32, принятым и для других протоколов IEEE 802. Контрольная последовательность охватывает поля FC, DA, SA, INFO и FCS.

**Конечный ограничитель** (Ending Delimiter — ED). Содержит единственный символ Terminate (T), обозначающий границу кадра. За ним располагаются признаки статуса кадра.

**Статус кадра** (Frame Status — FS). Первые три признака в этом поле являются индикаторами ошибки (Error — E), распознавания адреса (Address recognized — A) и копирования кадра (Frame Copied — C). Каждый из этих индикаторов кодируется одним символом, причем нулевое состояние индикатора обозначается символом Reset (R), а

единичное — символом Set (S). Стандарт позволяет производителям оборудования добавлять свои индикаторы после трех обязательных.

## Операции MAC-подуровня

С помощью операций MAC-уровня станции получают доступ к кольцу и передают свои кадры данных. Цикл передачи кадра от одной станции к другой включает в себя несколько этапов: захват маркера станцией, которой необходимо передать кадр; передача одного или нескольких кадров данных; освобождение маркера передающей станцией; ретрансляция кадра промежуточными станциями; распознавание и копирование кадра станцией-получателем; удаление кадра из сети станцией-отправителем. Рассмотрим эти операции.

*Захват маркера.* Если станция имеет право захватить маркер, то после ретрансляции на выходной порт символов PA и SD маркера она удаляет из кольца символ FC, по которому распознала маркер, а также конечный ограничитель ED. Затем вслед за уже переданным символом SD станция передает символы своего кадра. Таким образом, станция, как и прежде, формирует новый кадр из маркера, который она захватила.

*Передача кадра.* После удаления полей FC и ED маркера станция начинает передавать символы кадров, которые ей предоставил для передачи уровень LLC, и может передавать кадры до тех пор, пока не истечет время удержания маркера.

Для передач кадров в сетях FDDI предусмотрены два типа трафика — синхронный и асинхронный. *Синхронный* трафик предназначен для приложений, требующих обеспечения гарантированной пропускной способности для передачи голоса, видеоизображений, управления процессами и других случаев работы в реальном времени. Для такого трафика каждой станции предоставляется фиксированная часть пропускной способности кольца FDDI, поэтому станция имеет право передавать кадры синхронного трафика всегда, когда она получает маркер от предыдущей станции. *Асинхронный* трафик — это обычный трафик для приложений без высоких требований к задержкам обслуживания. Станция может передавать асинхронные кадры только в том случае, если осталось неизрасходованное время удержания маркера. Каждая станция самостоятельно вычисляет текущее значение этого параметра по специальному алгоритму.

Станция прекращает передачу кадров в двух случаях: либо по истечении времени удержания маркера THT, либо после передачи всех имеющихся у нее кадров до истечения этого срока. После передачи последнего своего кадра станция формирует маркер и передает его следующей станции.

*Обработка кадра станцией назначения.* Распознав свой адрес в поле DA, станция назначения начинает копировать символы кадра во внутренний буфер одновременно с повторением их на выходном

порту. При этом станция назначения устанавливает признак распознавания адреса. Если же кадр скопирован во внутренний буфер, то устанавливается и признак копирования (невыполнение копирования может произойти, например из-за переполнения внутреннего буфера). Устанавливается также и признак ошибки, если ее обнаружила проверка с использованием контрольной последовательности.

**Удаление кадра из кольца.** Каждый MAC-узел ответственен за удаление из кольца кадров, которые он ранее в него поместил. Если MAC-узел при получении своего кадра занят передачей следующих кадров, то он удаляет все символы вернувшегося по кольцу кадра. Если же MAC-узел уже освободил маркер, то он прежде чем распознает свой адрес в поле SA повторяет на выходе несколько полей этого кадра. В этом случае в кольце возникает усеченный кадр, у которого после поля SA следуют символы Idle и отсутствует конечный ограничитель. Этот усеченный кадр будет удален из кольца какой-нибудь станцией, принявшей его, находясь в состоянии собственной передачи.

### Инициализация кольца

Процедура инициализации кольца, известная под названием Claim Token, выполняется для того, чтобы все станции кольца убедились в его потенциальной работоспособности. Кроме того, в ходе этой процедуры станции должны прийти к соглашению о значении параметра  $T_{\text{Org}}$  — максимально допустимого времени оборота маркера по кольцу, на основании чего они вычисляют время удержания маркера THT.

Процедура Claim Token выполняется в следующих случаях:

- при включении новой станции в кольцо и при выходе станции из кольца;
- при обнаружении какой-либо станцией факта утери маркера (маркер считается утерянным, если станция не наблюдает его в течение двух периодов максимального времени оборота маркера  $T_{\text{Org}}$ );
- при обнаружении длительного отсутствия активности в кольце, т.е. когда станция в течение определенного времени не наблюдает проходящих через нее кадров данных;
- по команде от блока управления станцией SMT.

Для выполнения процедуры инициализации каждая станция должна знать о своих требованиях к максимальному времени оборота маркера по кольцу. Эти требования содержатся в параметре TTRT (Target Token Rotation Time) — требуемом времени оборота маркера. Параметр TTRT отражает степень потребности станции в пропускной способности кольца — чем меньше время TTRT, тем чаще станция желает получать маркер для передачи своих кадров. Процедура инициализации позволяет станциям узнать требования к времени оборота маркера других станций и выбрать минимальное его значение в

качестве общего параметра  $T\_Org$ , на основании которого в дальнейшем будет распределяться пропускная способность кольца. Параметр  $TTRT$ , который должен находиться в пределах от 4 до 165 мс, может изменяться администратором сети.

Если какая-либо станция решает начать процесс инициализации кольца по своей инициативе, то она формирует кадр Claim Token со своим значением требуемого времени оборота маркера. Захвата маркера для этого не требуется. При этом любая другая станция, получив кадр Claim Token, начинает выполнять процедуру Claim Token.

Для выполнения процедуры инициализации каждая станция поддерживает таймер текущего времени оборота маркера — TRT (Token Rotation Timer), который используется и в дальнейшем при работе кольца в нормальном режиме. TRT запускается каждой станцией при обнаружении начала процедуры Claim Token. В качестве предельного значения таймера выбирается максимально допустимое время оборота маркера, т.е. 165 мс. Истечение значения TRT до завершения процедуры означает ее неудачное окончание — кольцо не удалось инициализировать. В случае неудачи процесса Claim Token запускаются процедуры, с помощью которых станции пытаются выявить некорректно работающую часть кольца и отключить ее.

Процедура Clime Token работает следующим образом. Каждая станция генерирует кадр Clime со своим значением  $T\_Req$ , равным значению ее параметра  $TTRT$ . При этом станция устанавливает значение  $T\_Org$ , равное значению  $TTRT$ . Приняв кадр Claim от предыдущей станции, она обязана сравнить значение  $T\_Req$ , указанное в этом кадре, со своим значением  $TTRT$ . Если другая станция просит установить время оборота маркера меньше, чем это значение (т.е.  $T\_Req < TTRT$ ), то данная станция перестает генерировать собственные кадры Claim и начинает повторять чужие кадры Claim, так как видит, что в кольце есть более требовательные станции. Одновременно эта станция фиксирует в своей переменной  $T\_Org$  минимальное значение  $T\_Req$ , которое ей встретилось в чужих кадрах Claim. Если же поступивший кадр имеет значение  $T\_Req$  большее, чем собственное значение  $TTRT$  станции, то он удаляется из кольца.

Процесс Claim завершается для станции в том случае, если она получает кадр Claim со своим адресом назначения. Это означает, что данная станция является победителем состязательного процесса, и ее значение  $TTRT$  оказалось минимальным. При равных значениях параметра  $TTRT$  преимущество отдается станции с бóльшим значением MAC-адреса.

Обнаружив, что оказалась победителем процесса Claim Token, станция должна сформировать маркер и отправить его по кольцу. Первый оборот маркера является служебным, так как за время этого оборота станции кольца узнают, что процесс Claim Token успешно завершен. При этом они устанавливают признак Ring\_Operational в состояние True, означающее начало нормальной работы кольца. При

следующем проходе маркера его можно будет использовать для захвата и передачи кадров данных.

Если же у какой-либо станции во время выполнения процедур инициализации значение TRT истекло, а маркер так и не появился на ее входе, то станция начинает процесс инициализации. После нормального завершения этого процесса у всех станций кольца устанавливается одинаковое значение переменной  $T\_Org$ .

### Управление доступом к кольцу

Управление доступом к кольцу FDDI распределено между его станциями. Каждая станция, получив маркер, самостоятельно решает, может она его захватить или нет, а если может, то на какое время. Если у станции есть для передачи синхронные кадры, то она всегда может захватить маркер на фиксированное время, выделенное ей администратором. Если же у станции для передачи есть лишь асинхронные кадры, то условия захвата маркера определяются следующим образом.

Станция ведет таймер текущего времени оборота маркера (TRT), а также счетчик числа опозданий маркера  $Late\_Ct$ . Напомним, что значение TRT равно значению максимального времени оборота маркера  $T\_Org$ , выбранному станциями при инициализации кольца.

Счетчик  $Late\_Ct$  всегда обнуляется, когда маркер проходит через станцию. Если же маркер опаздывает, то TRT достигает значения  $T\_Org$  раньше очередного прибытия маркера. При этом таймер обнуляется и начинает отсчет времени заново, а счетчик  $Late\_Ct$  увеличивается на единицу, фиксируя факт опоздания маркера. При прибытии опоздавшего маркера (при этом  $Late\_Ct = 1$ ) TRT значение не сбрасывает, а продолжает считать, накапливая время опоздания маркера. Если же маркер прибыл раньше, чем истек интервал  $T\_Org$ , то значение TRT сбрасывается в момент прибытия маркера.

Возможны следующие комбинации событий, связанных с поступлением маркера и состоянием таймера:

- *момент А* — маркер прибыл вовремя, так как значение TRT не достигло порога  $T\_Org$ ;

- *момент С* — время, заданное таймером, истекло раньше, чем маркер прибыл на станцию. TRT перезапускается, а счетчик  $Late\_Ct$  увеличивается на единицу;

- *момент D* — маркер прибыл, но опоздал, при этом счетчик  $Late\_Ct$  равен 1. Счетчик сбрасывается в нуль, но таймер не перезапускается, так как при поступлении маркера счетчик не был равен нулю;

- *момент E* — маркер прибыл на станцию до истечения времени, заданного таймером, и при нулевом значении счетчика  $Late\_Ct$ , поэтому считается, что он прибыл вовремя. Таймер перезапускается.

Станция может захватывать маркер только в случае, если он прибывает вовремя, т.е. если в момент его прибытия счетчик Late\_Ct равен нулю.

Время удержания маркера управляется таймером удержания маркера — ТНТ (Token Holding Timer). Значение этого таймера полагается равным  $T\_Org - TRT$ , где  $TRT$  — значение таймера  $TRT$  в момент прихода маркера. Если у станции в буфере имеются кадры для передачи в момент прибытия маркера и маркер прибыл вовремя, то станция захватывает его и удерживает в течение периода, определяемого значением ТНТ. Для отслеживания разрешенного времени удержания маркера в момент его захвата значение  $TRT$  присваивается ТНТ, а затем  $TRT$  обнуляется и перезапускается. ТНТ считает до границы  $T\_Org$ , после чего считается, что время удержания маркера исчерпано. Станция перестает передавать кадры данных и передает маркер следующей станции.

Описанный алгоритм позволяет адаптивно распределять пропускную способность кольца между станциями, а точнее, ту часть пропускной способности, которая осталась после распределения ее между синхронным трафиком станций.

На рис. 5.14 приведен пример, иллюстрирующий работу этого алгоритма:

- момент  $A$  — маркер прибыл вовремя, так как значение  $TRT$  не достигло порога  $T\_Org$ . Следовательно,  $TRT$  перезапускается и начинает считать заново. У станции нет в это время асинхронных кадров, поэтому она просто передает маркер соседу;

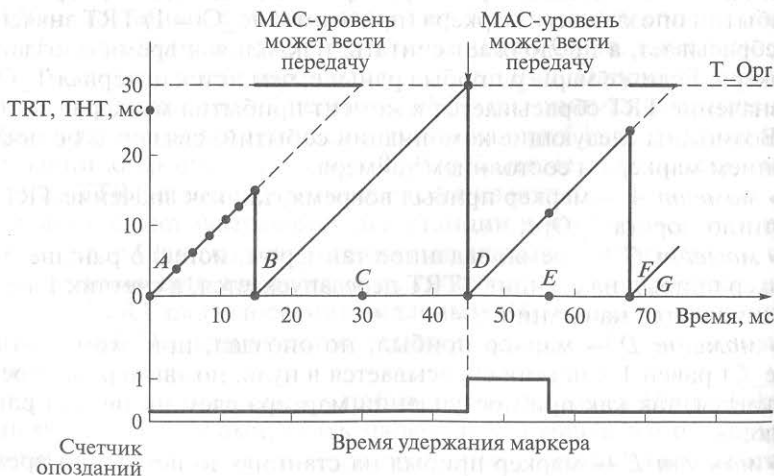


Рис. 5.14. Пример распределения пропускной способности кольца между станциями

- момент *B* — маркер прибыл вовремя. Станция имеет к этому моменту асинхронные кадры для передачи. ТНТ присваивается значение TRT (16), и он начинает считать до значения *T\_Org* (30). TRT перезапускается. Станция начинает передавать кадры, что может продолжаться в течение 14 мс. Если станция закончит передачу имеющихся кадров раньше, то она обязана немедленно освободить маркер;

- момент *C* — время, заданное ТНТ, истекло, и станция должна прекратить передачу асинхронных кадров. Станция завершает передачу текущего кадра и передает маркер соседней станции. Счетчик TRT при этом продолжает работать;

- момент *D* — значение, заданное TRT, истекает раньше очередного прибытия маркера. Таймер перезапускается, а счетчик *Late\_Ct* увеличивается на 1;

- момент *E* — маркер поступил, но опоздал, так как *Late\_Ct* имеет значение 1. Станция не может захватить маркер при значении *Late\_Ct*, отличном от нуля, и маркер передается соседней станции. Счетчик *Late\_Ct* обнуляется, а TRT не перезапускается;

- момент *F* — маркер прибывает на станцию. Так как время, заданное TRT, еще не истекло, а значение *Late\_Ct* равно 0, следовательно, маркер прибыл вовремя. ТНТ инициализируется значением TRT (22) и начинает считать до границы *T\_Org*. TRT перезапускается. Станция может передавать кадры в течение 8 мс;

- момент *G* — время, заданное таймером ТНТ, истекает, и передача асинхронных кадров прекращается. Станция передает маркер соседней станции.

В стандарте FDDI определены еще два механизма управления доступом к кольцу. Первый — в маркере можно задавать уровень приоритета маркера, а для каждого уровня приоритета задается свое время порога, до которого считает таймер удержания маркера ТНТ. Второй — использование особой формы маркера — сдерживающего маркера (*restricted token*), с помощью которого две станции могут некоторое время монопольно обмениваться данными по кольцу.

И, наконец, если время, заданное TRT, истечет при значении *Late\_Ct*, равном 1, то такое событие считается потерей маркера и порождает выполнение процесса реинициализации кольца *Claim Token*.

### 5.3. СПД Frame Relay

#### 5.3.1. Общие сведения

Ретрансляция кадров (*Frame Relay — FR*) — это СПД с коммутацией пакетов для сетей класса WAN, т.е. для сетей, объединяющих несколько ЛВС. Первоначально разработка стандарта FR предназначалась для цифровых СПД с интегрированным сервисом — ISDN (*Integrated Services Digital Networks*). Однако позже стало ясно, что

технология FR применима и в других СПД (где под данными понимается любое сообщение, представленное в цифровой форме). К числу достоинств протокола Frame Relay, прежде всего, необходимо отнести его совместимость с протоколами верхних уровней модели OSI, малое время задержки кадра, простой формат кадров, содержащих минимум управляющей информации и дейтаграммный режим работы, обеспечивающий высокую пропускную способность системы. Надежную передачу кадров технология FR не обеспечивает. СПД FR, специально разработанная как общественная сеть для соединения частных локальных сетей, обеспечивают скорость передачи данных до 2 Мбит/с.

Особенностью технологии FR является гарантированная поддержка основного показателя качества передачи данных — средней скорости передачи данных по виртуальному каналу при допустимых пульсациях трафика. Кроме технологии FR гарантии качества обслуживания в настоящее время может предоставить только технология АТМ, в то время как остальные технологии предоставляют требуемое качество обслуживания только в режиме «С максимальными усилиями» (best effort), т. е. без гарантий.

### **5.3.2. Архитектура Frame Relay**

Технология Frame Relay использует для передачи данных технику виртуальных соединений, аналогичную той, которая применяется в СПД АТМ, однако стек протоколов FR передает кадры (при установленном виртуальном соединении) по протоколам только физического и канального уровней, а третий пакетный уровень здесь не используется. При таком подходе уменьшаются накладные расходы на передачу пакетов локальных сетей, так как эти пакеты вкладываются сразу в кадры канального уровня СПД FR.

Протокол канального уровня FR использует кадры переменной длины и работает только по виртуальным соединениям, которые могут быть постоянными (PVC) или коммутируемыми (SVC). Прежде чем два узла начнут обмениваться информацией, между ними необходимо установить виртуальное соединение.

Постоянное виртуальное соединение PVC (Permanent Virtual Circuits) устанавливается между двумя узлами вручную в процессе конфигурирования сети, т. е. когда в каждом узле коммутации вручную прописывают, на какой выход передавать кадры определенного виртуального соединения. Для этого пользователь сообщает провайдеру FR-услуг или сетевому администратору, какие узлы должны быть соединены, и последний устанавливает PVC между этими узлами.

PVC включает в себя конечные станции, среду передачи и все коммутаторы, расположенные между конечными станциями. После установки для PVC резервируется определенная часть полосы пропускания каналов, поэтому двум конечным станциям не требуется

каждый раз устанавливать или сбрасывать соединение. При этом благодаря методу статистического мультиплексирования несколько PVC могут разделять разные полосы одного канала передачи.

Статистическое мультиплексирование — это метод мультиплексирования, при котором полоса пропускания канала распределяется между потоками данных (виртуальными каналами) по мере необходимости. Например, при передаче видеоинформации малоподвижные сюжеты генерируют поток данных, который требует меньшей скорости передачи, чем динамичные сюжеты (например, трансляция гонок Формула-1). Основной целью статистического мультиплексирования является кодирование с постоянным качеством за счет выделения большей полосы более сложным динамичным потокам. Определение «статистическое» говорит о том, что среднестатистические потоки данных по виртуальным каналам не могут превзойти пропускную способность физического канала.

Коммутируемые виртуальные соединения — SVC (Switched Virtual Circuits) устанавливаются по мере необходимости, т.е. всякий раз, когда один узел пытается передать данные другому узлу, и динамически, как в телефонных сетях, на основе информации, заложенной при инициализации СПД.

PVC имеют два преимущества по сравнению с SVC. Во-первых, сеть, в которой используются SVC, должна тратить время на установление соединений, а PVC устанавливаются предварительно, а значит, обеспечивают более высокую производительность. Во-вторых, PVC обеспечивают лучший контроль над СПД, так как провайдер или сетевой администратор может заранее выбирать маршрут, по которому будут передаваться кадры.

Однако и SVC имеют ряд преимуществ по сравнению с PVC: используют полосу пропускания только по мере необходимости, тогда как PVC должны постоянно ее резервировать на случай, если она понадобится; требуют меньшей административной работы, поскольку устанавливаются автоматически, а не вручную; обеспечивают отказоустойчивость, т.е. когда коммутатор, находящийся на пути соединения, выходит из строя, другие коммутаторы выбирают альтернативный путь.

Однако в настоящее время SVC не получили широкого распространения в силу сложности их реализации, а следовательно, PVC является наиболее распространенным режимом связи в СПД FR.

### **5.3.3. Канальный уровень FR**

На канальном уровне СПД FR используется бит-ориентированный синхронный протокол LAP-F (стандарт Q.922 МСЭ) [40], являющийся весьма упрощенной версией протокола LAP-D, заимствованного из технологии ISDN, который, в свою очередь, является упрощенной версией протокола HDLC (см. подразд. 4.2.7).

У протокола канального уровня LAP-F есть два режима работы: основной (core) и управляющий (control). В основном режиме кадры передаются без преобразования и контроля, как и в коммутаторах локальных сетей. За счет этого СПД FR обладают весьма высокой производительностью, так как кадры в коммутаторах не подвергаются преобразованию, а сеть не передает подтверждения между коммутаторами на каждый пользовательский кадр. Пульсации трафика передаются СПД FR достаточно быстро и без больших задержек.

Протокол LAP-F работает на любых каналах сети ISDN, а также на каналах типа T1/E1. Терминальное оборудование посылает в сеть кадры LAP-F в любой момент времени, считая, что виртуальный канал в сети коммутаторов уже проложен. При использовании PVC оборудованию СПД FR требуется поддерживать только протокол LAP-F core.

Протокол LAP-F control является необязательной надстройкой над LAP-F core, которая выполняет функции контроля доставки кадров и управления потоком. С помощью протокола LAP-F control СПД FR реализует службу коммутации кадров.

Для установки SVC используется канал D (см. подразд. 5.4) пользовательского интерфейса, на котором по-прежнему работает протокол LAP-D, используемый для надежной передачи кадров в СПД ISDN. Устанавливают виртуальное соединение на основе адресов конечных абонентов, а также номера виртуального соединения, который в технологии Frame Relay называется Data Link Connection Identifier — DLCI.

После установки коммутируемого виртуального канала с помощью протоколов LAP-D кадры могут транслироваться по протоколу LAP-F, который коммутирует их с помощью таблиц коммутации портов, где используются локальные значения DLCI. Протокол LAP-F в основном режиме работы выполняет не все функции канального уровня по сравнению с протоколом LAP-D.

Действие СПД FR заканчивается на канальном уровне, поэтому она хорошо согласуется с идеей тунелирования, т.е. инкапсуляции пакетов единого сетевого протокола, например IP, в кадры канального уровня любых сетей, составляющих Интернет. Процедуры взаимодействия протоколов сетевого уровня с протоколом канального уровня FR стандартизованы, например принята спецификация RFC 1490, определяющая методы инкапсуляции в трафик FR трафика сетевых протоколов и протоколов канального уровня локальных сетей.

Другой особенностью технологии FR является отказ от коррекции обнаруженных в кадрах искажений. Протокол LAP-F подразумевает, что конечные узлы будут обнаруживать и корректировать ошибки за счет работы протоколов транспортного или более высоких уровней. Это требует некоторой степени интеллектуальности от конечного оборудования, что по большей части справедливо для современных

Флаг	Заголовок		Информация	Проверка	Флаг		
DLCI (1-й октет)	CFI	EA	DLCI (2-й октет)	FECN	BECN	DE	EA
8...3	2	1	8...5	4	3	2	1
		«0»					«1»

Рис. 5.15. Структура кадра Frame Relay (LAP-F)

локальных сетей. В этом отношении технология FR близка к технологиям локальных сетей, таким как Ethernet, Token Ring и FDDI, которые тоже только отбрасывают искаженные кадры, а повторной их передачей не занимаются.

Структура кадра протокола FR (LAP-F) (рис. 5.15) включает в себя следующие элементы:

- Флаг** — комбинация 01111110, которой начинаются и заканчиваются все кадры;
- Заголовок** (стандарты ANSI и МСЭ допускают размер заголовка до 4 байт), который содержит:
  - адрес в пределах кадра FR (стандарт FRF), который занимает 6 бит первого байта и 4 бит второго байта заголовка кадра. Эти 10 бит представляют собой идентификатор виртуального канала передачи данных (Data Link Connection Identifier — DLCI) и определяют абонентский адрес в СПД FR;
  - бит CFI, зарезервированный для возможного применения в различных протоколах более высоких уровней управления OSI. Этот бит не используется протоколом FR и «прозрачно» пропускается аппаратно-программными средствами СПД FR;
  - бит расширения адреса (Extended Address — EA). Минимальная длина идентификатора канала передачи данных DLCI составляет 10 бит, входящих в два байта заголовка. Однако возможно расширение заголовка на целое число дополнительных байтов для указания адреса, состоящего более чем из 10 бит. Адрес может иметь длину 16 бит либо 23 бит. Для расширения используется бит EA в конце каждого байта заголовка; если он имеет значение 1, то это означает, что данный байт в заголовке последний. Стандарт FR рекомендует использовать заголовки, состоящие из двух байтов. В этом случае значение бита EA первого байта будет соответствовать 0, а второго — 1;
  - бит уведомления (сигнализации) приемника о явной перегрузке (Forward Explicit Congestion Notification — FECN),

устанавливающийся в 1, если надо информировать получателя о том, что произошла перегрузка в направлении передачи данного кадра, т.е. что в этом направлении возник слишком большой поток кадров, в результате чего поток превзошел пропускную способность канала, выделенного под данное виртуальное соединение, и какие-то кадры были сброшены;

- бит уведомления (сигнализации) отправителя о явной перегрузке (Backward Explicit Congestion Notification — BECN), который устанавливается в 1 для уведомления отправителя сообщения о том, что произошла перегрузка в направлении, обратном направлению передачи содержащего этот бит кадра. Бит BECN может не использоваться терминалами абонентов (рис. 5.16);
- бит разрешения сброса (Discard Eligibility — DE), указывающий на то, что в случае перегрузки данный кадр может быть уничтожен в первую очередь, т.е. пользователю предоставлено право выбирать, какими кадрами он может «пожертвовать». Однако при перегрузках узлы коммутации в СПД FR уничтожают не только кадры с битом DE.

3. **Поле «Информация»**, которое содержит данные пользователя и состоит из целого числа байтов. Его максимальный размер определен стандартом FR и равен 4 096 байт (минимальный размер — 1 байт). Содержание этого поля передается без изменений.

4. **Поле «Проверка»**, которое используется для обнаружения возможных ошибок при передаче и состоит из двух байтов. Это поле формируется с помощью CRC-кода аналогично протоколу HDLC (см. подразд. 4.2.7).

Все указанные поля должны присутствовать в каждом кадре FR, передаваемом между двумя оконечными пользовательскими системами.

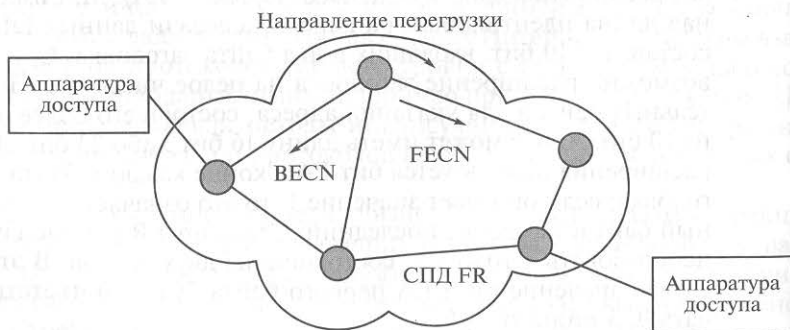


Рис. 5.16. Управление перегрузками в СПД Frame Relay

Одним из основных отличий протокола FR от HDLC является то, что FR не предусматривает передачу управляющих сообщений (в нем нет командных или супервизорных кадров, как в HDLC). Для передачи служебной информации в FR используется специально выделенный канал D. Другим важным отличием FR является отсутствие нумерации последовательно передаваемых (принимаемых) кадров. Дело в том, что в протоколе FR нет механизмов для подтверждения правильно принятых кадров. Это означает, что этот протокол предполагает использование достаточно надежной физической среды.

Протокол FR является весьма простым и включает в себя небольшой свод правил и процедур обмена данными. Основная процедура состоит в том, что если кадр получен без искажений, он должен быть направлен далее по соответствующему маршруту. При возникновении перегрузки узлы СПД FR могут сбрасывать любой кадр.

Узлам в СПД FR разрешено уничтожать искаженные кадры, не уведомляя об этом пользователя. При этом искаженным считается кадр, у которого:

- нет корректного ограничения флагами;
- между флагами менее пяти байтов;
- присутствует ошибка контрольной суммы, хранящейся в двухбайтовом поле контрольной суммы FCS;
- искажено поле адреса (для случая, когда проверка не выявила ошибки в поле FCS);
- содержится несуществующий DLCI;
- превышен допустимый максимальный размер (в некоторых вариантах реализации стандартов FR возможна принудительная обработка кадров, превышающих допустимый максимальный размер).

#### **5.3.4. Управление качеством сервиса**

В технологии FR особое внимание уделено управлению качеством сервиса, предоставляемого транспортной среде. Вместо приоритезации трафика, как например в технологии FDDI, в этой технологии используется процедура заказа качества обслуживания при установлении соединения.

Для каждого виртуального соединения определяется несколько параметров, влияющих на качество обслуживания:

- CIR (Committed Information Rate) — согласованная скорость передачи данных, с которой сеть будет передавать данные пользователя;
- Bc (Committed Burst Size) — согласованный объем пульсации, т.е. максимальное число байтов, которое сеть будет передавать от этого пользователя за фиксированный интервал времени  $T$ ;
- Be (Excess Burst Size) — дополнительный объем пульсации, т.е. максимальное число байтов, которое сеть будет пытаться передать сверх установленного значения параметра Bc за интервал времени  $T$ .

Если эти параметры определены, то время  $T = Vc/CIR$ . Если задать значения  $CIR$  и  $T$ , то можно найти значение всплеска трафика  $Vc$ .

Гарантий по задержкам передачи кадров технология FR не дает, оставляя эту услугу сетям ATM.

Основным параметром, по которому абонент и сеть заключают соглашение при установлении виртуального соединения, является согласованная скорость передачи данных. Для постоянных виртуальных каналов это соглашение составляет часть контракта на пользование услугами СПД. При установлении коммутируемого виртуального канала заключение соглашения о качестве обслуживания является частью протокола LAP-D, в котором требуемые параметры  $CIR$ ,  $Vc$  и  $Ve$  передаются в пакете запроса на установление соединения.

Так как скорость передачи данных измеряется в каком-то интервале времени, то интервал  $T$  и является таким контрольным интервалом, в котором проверяются условия соглашения. В общем случае пользователь не должен за этот интервал времени передавать в сеть данные со средней скоростью, превосходящей  $CIR$ . Если же он нарушает соглашение, то СПД не только не гарантирует доставку кадра, но помечает этот кадр признаком DE (Discard Eligibility), равным 1, т. е. как кадр, подлежащий удалению. Однако кадры, отмеченные таким признаком, удаляются из СПД только в том случае, если коммутаторы СПД испытывают перегрузки. Если же перегрузок нет, то кадры с признаком  $DE = 1$  доставляются адресату. Некоторые операторы СПД (поставщики услуг) предлагают значительные скидки при передаче кадров с битом DE, установленным в 1.

Такое щадящее поведение сети соответствует случаю, когда общее количество данных, переданных пользователем в СПД за период  $T$ , не превышает объема  $Vc + Ve$ . Если же этот порог превышен, то кадр не помечается признаком DE, а немедленно удаляется из СПД.

Например, пусть за интервал времени  $T$  в СПД по виртуальному каналу поступило пять кадров:  $f_1, f_2, f_3, f_4, f_5$ . Пусть средняя скорость поступления информации в СПД составила в этом интервале  $R$ , бит/с, и оказалась выше  $CIR$ . Пусть кадры  $f_1, f_2$  и  $f_3$  доставили в сеть данные, суммарный объем которых не превысил порог  $Vc$ , и поэтому они уйдут дальше транзитом с признаком  $DE = 0$ . Пусть данные кадра  $f_4$ , прибавленные к данным кадров  $f_1, f_2$  и  $f_3$ , превысили порог  $Vc$ , но еще не превысили порог  $Vc + Ve$ , тогда кадр  $f_4$  также уйдет дальше, но уже с признаком  $DE = 1$ . Пусть данные кадра  $f_5$ , прибавленные к данным предыдущих кадров, превысили порог  $Vc + Ve$ , тогда этот кадр будет удален из СПД.

Для контроля соглашения о параметрах качества обслуживания все коммутаторы СПД FR используют так называемый алгоритм дырявого ведра (Leaky Bucket), который подробно рассматривается в т. 2 данного учебника при изучении сетевого уровня в сетях ЭВМ. Здесь же только кратко скажем, что в этом алгоритме используется счетчик  $S$  поступивших от пользователя байтов, который каждые  $T$

секунд уменьшается на значение  $V_c$  (или же сбрасывается в 0, если значение счетчика меньше, чем  $V_c$ ). Все кадры, данные которых не увеличили значение счетчика свыше порога  $V_c$ , пропускаются в сеть со значением признака  $DE = 0$ . Кадры, данные которых привели к значению счетчика, большему  $V_c$ , но меньшему  $V_c + V_e$ , также передаются в сеть, но с признаком  $DE = 1$ . И наконец, кадры, которые привели к значению счетчика, большему  $V_c + V_e$ , отбрасываются коммутатором.

Пользователь может договориться о включении не всех параметров качества обслуживания на данном виртуальном канале, а только некоторых.

Например, можно использовать только параметры CIR и  $V_c$ . Этот вариант обеспечивает более качественное обслуживание, так как кадры никогда не отбрасываются коммутатором сразу. Коммутатор только помечает кадры, которые превышают порог  $V_c$  за время  $T$ , признаком  $DE = 1$ . Если в СПД не возникает перегрузок, то кадры такого канала всегда доходят до конечного узла, даже если пользователь постоянно нарушает договор СПД.

Популярен еще один вид заказа на качество обслуживания, при котором оговаривается только порог  $V_e$ , а скорость CIR полагается равной нулю. Все кадры такого канала сразу же отмечаются признаком  $DE = 1$ , но отправляются в СПД, а при превышении порога  $V_e$  они отбрасываются. В этом случае контрольный интервал времени  $T = V_e/R$ , где  $R$  — скорость доступа к каналу.

В технологии FR определен еще и дополнительный (необязательный) механизм управления потоками кадров, основанный на использовании битов FECN и BECN в кадре FR. Это механизм оповещения конечных пользователей о том, что в коммутаторах СПД возникли перегрузки (переполнение необработанными кадрами).

Бит FECN (Forward Explicit Congestion Bit) кадра извещает принимающую сторону о переполнении в СПД. На основании значения этого бита принимающая сторона должна с помощью протоколов более высоких уровней (TCP/IP, SPX и т. п.) известить передающую сторону о том, что она должна снизить интенсивность отправки пакетов в сеть.

Бит BECN (Backward Explicit Congestion Bit) кадра извещает о переполнении в СПД передающую сторону и является рекомендацией немедленно снизить темп передачи. Обычно он обрабатывается на уровне устройств доступа к СПД FR. Протокол LAP-F не требует от устройств, получивших кадры с установленными битами FECN и BECN, немедленного прекращения передачи кадров в данном направлении. Эти биты служат лишь указанием для протоколов более высоких уровней (TCP, SPX, NCP и т. п.) о необходимости снижения темпа передачи пакетов. Так как управление потоком в разных протоколах организовано по-разному и принимающей, и передающей сторонами, то разработчики протоколов FR учли оба

направления, снабдив их предупреждающей информацией о переполнении СПД.

В общем случае биты FECN и BECN могут игнорироваться, но обычно устройства доступа к СПД FR (Frame Relay Access Device — FRAD) обрабатывают по крайней мере признак BECN.

При создании коммутируемого виртуального канала параметры качества обслуживания передаются в СПД с помощью протокола LAR-D, который устанавливает виртуальное соединение посредством нескольких служебных пакетов.

### 5.3.5. Управление доступом

Абонент СПД FR, который хочет установить коммутируемое виртуальное соединение с другим абонентом СПД FR, должен передать через адаптер FRAD по каналу D сообщение SETUP, определяемое следующими параметрами:

- DLCI;
- адрес назначения;
- максимальный размер кадра в данном виртуальном соединении;
- запрашиваемое значение CIR для двух направлений;
- запрашиваемое значение  $V_c$  для двух направлений;
- запрашиваемое значение  $V_e$  для двух направлений.

Коммутатор, с которым соединен пользователь, сразу же передает ему пакет CALL PROCEEDING — обработка вызова. Затем он анализирует параметры, указанные в пакете, и если коммутатор может их удовлетворить (располагая, естественно, информацией о том, какие виртуальные каналы на каждом порту он уже поддерживает), то пересылает сообщение SETUP следующему коммутатору, который выбирается по таблице маршрутизации.

Протокол автоматического составления таблиц маршрутизации для технологии FR не определен, следовательно, может использоваться фирменный протокол производителя оборудования или же ручное составление таблицы. Если все коммутаторы на пути к конечному узлу согласны принять запрос, то пакет SETUP передается в конечном счете вызываемому абоненту. Вызываемый абонент немедленно передает в сеть пакет CALL PROCEEDING и начинает обрабатывать запрос. Если запрос принимается, то вызываемый абонент передает в сеть новый пакет — CONNECT, который проходит в обратном порядке по виртуальному пути. Все коммутаторы должны отметить, что данный виртуальный канал принят вызываемым абонентом. При поступлении сообщения CONNECT вызываемому абоненту последний должен передать в сеть пакет CONNECT ACKNOWLEDGE.

СПД также должна передать вызываемому абоненту пакет CONNECT ACKNOWLEDGE. На этом соединении считается установленным, и по виртуальному каналу могут передаваться данные.

### 5.3.6. Использование СПД Frame Relay

Услуги Frame Relay обычно предоставляются теми же операторами, которые эксплуатируют сети X.25. В настоящее время большая часть производителей выпускает коммутаторы, которые могут работать как по протоколам X.25, так и по протоколам Frame Relay.

Технология Frame Relay начинает занимать в территориальных сетях с коммутацией пакетов ту же нишу, которую заняла в локальных сетях технология Ethernet. Эти технологии предоставляют только быстрые базовые транспортные услуги, доставляя кадры в узел назначения без гарантий, т.е. дейтаграммным способом. При этом если кадры теряются, то СПД Frame Relay, как и СПД Ethernet, не предпринимает никаких усилий для их восстановления. Отсюда можно сделать простой вывод: полезная пропускная способность прикладных протоколов при работе через СПД Frame Relay зависит от качества каналов и методов восстановления пакетов на уровнях стека, расположенного над протоколом Frame Relay. Если каналы качественные, то кадры теряются и искажаются редко, и скорость восстановления пакетов протоколов TCP или NCP будет вполне приемлема. Если же кадры искажаются и теряются часто, полезная пропускная способность в СПД Frame Relay может упасть в десятки раз, как это и происходит в СПД Ethernet при плохом состоянии кабельной системы.

Следовательно, СПД Frame Relay можно использовать, только если магистральные каналы выполнены из волоконно-оптических кабелей высокого качества. При этом каналы доступа могут быть выполнены и на витой паре, как это разрешает интерфейс G.703 или абонентское окончание ISDN. Используемая в каналах доступа аппаратура передачи данных должна обеспечить приемлемый уровень искажения данных — не ниже  $10^{-6}$  на бит.

На значения задержек Frame Relay гарантий не дает, и это является основной причиной, сдерживающей применение этой СПД для передачи голоса. Передача видеоизображений тормозится и другим отличием СПД Frame Relay от АТМ: низкой скоростью доступа (2 Мбит/с), которой для передачи видеоданных часто недостаточно.

Тем не менее многие производители оборудования для СПД Frame Relay поддерживают передачу голоса. Поддержка такой передачи устройствами доступа заключается в присвоении кадрам, переносящим замеры голоса, приоритетов. При этом магистральные коммутаторы Frame Relay должны обслуживать такие кадры в первую очередь. Кроме того, желательно, чтобы СПД Frame Relay, передающая кадры с замерами голоса, была недогруженной. В этом случае в коммутаторах не возникает очередей кадров, и средние задержки в очередях близки к нулевым.

Для качественной передачи голоса необходимо также соблюдение еще одного условия: передавать замеры голоса необходимо в кадрах небольших размеров, иначе на качество будут влиять задержки упа-

ковки замеров в кадр, так называемые задержки пакетизации (см. подразд. 5.4.9).

Для стандартизации механизмов качественной передачи голоса через СПД Frame Relay выпущена спецификация FRF.11, однако в ней решены еще не все проблемы передачи голоса, поэтому работа в этом направлении продолжается.

В коммерческих сетях СПД Frame Relay преобладают услуги постоянных коммутируемых каналов с гарантированной пропускной способностью, т.е. эти СПД предоставляют услуги, очень похожие на услуги цифровых выделенных телефонных линий T1/E1, но только за существенно меньшую плату.

При использовании PVC СПД Frame Relay хорошо подходит для объединения локальных сетей с помощью мостов, так как в этом случае от моста не требуется поддержка механизма установления виртуального канала, а требуется лишь некоторый программный «интеллект». Мост может отправлять кадры протоколов Ethernet или FDDI непосредственно в кадрах протокола LAP-F или же может использовать поверх протокола LAP-F протокол PPP. Стандарт Internet RFC 1490 определяет формат заголовка SNAP для случая передачи через СПД Frame Relay непосредственно кадров канально-го уровня.

Чаше доступ к СПД Frame Relay реализуется не через удаленные мосты, а с помощью маршрутизаторов, которые в случае поддержки на последовательных портах протокола Frame Relay как основного, называются устройствами доступа FRAD.

Использование виртуальных каналов в качестве основы построения корпоративной сети имеет один недостаток: при большом числе точек доступа и смешанном характере связей необходимо наличие большого числа виртуальных каналов, каждый из которых оплачивается отдельно. В сетях с маршрутизацией отдельных пакетов, таких как TCP/IP, абонент платит только за число точек доступа, а не за число связей между ними.

В заключение следует отметить, что все бóльшие и бóльшие объемы трафика локальных сетей передаются по глобальным сетям. Трафик, создаваемый ЛВС, — это трафик, создаваемый клиент-серверными приложениями, написанными для локально-сетевых сред. Как уже отмечалось, этот трафик имеет, как правило, чрезвычайно неравномерный характер: значительная пропускная способность требуется в течение коротких интервалов времени. Передача такого трафика по выделенным линиям или по сети с временным разделением каналов не эффективна, поскольку большую часть времени доступная емкость расходуется впустую, т.е. временные слоты резервируются вне зависимости от того, передается информация или нет.

В то же время развитие компьютерных приложений, требующих использования высокоскоростных коммуникаций, и доступность

высокоскоростных линий передачи с низким коэффициентом ошибок послужили причиной создания новой технологии передачи данных в территориальных сетях. Основными требованиями к такой технологии являются: высокая скорость передачи, низкие задержки, разделение портов и разделение полосы пропускания линий связи на основе виртуальных каналов. Метод TDM-коммутации каналов, используемый в телефонии, обеспечивает выполнение первых двух из этих требований, метод X.25-коммутации пакетов — двух последних, а трансляция кадров как форма коммутации пакетов в СПД Frame Relay удовлетворяет всем четырем требованиям.

## **5.4. Цифровые сети с интегрированным сервисом**

### **5.4.1. Общие сведения**

Более ста лет основной инфраструктурой, используемой в обществе для передачи данных, была телефонная сеть. Эта сеть создавалась исключительно для передачи голоса в аналоговой форме и к концу 1970-х гг. уже перестала удовлетворять современные требования как операторов телефонной связи, так и пользователей. Под давлением требований тех, кому необходима была цифровая передача данных, МСЭ в 1984 г. собрал конгресс, где было принято решение о создании новой полностью цифровой системы передачи данных, которую назвали цифровой сетью с интегрированным сервисом — ISDN (Integrated Service Digital Network).

ISDN задумывалась как всемирная телекоммуникационная сеть, которая должна была заменить телефонные сети. При этом приложения ISDN должны были поддерживать передачу голоса, звука, изображения и данных.

ISDN-телефон по замыслу проекта должен был обеспечивать самый разнообразный сервис: различные программируемые функции, автоматическое определение номера телефона (АОН), с которого поступил звонок, и имени звонящего, взаимодействие с компьютером — выдачу запроса к базе данных и показ на экране ответа, переадресацию звонков, удаленный доступ к своему телефону, выполнение автоматических звонков в скорую помощь, полицию, пожарную службу в случае опасности и т.д. Эта технология должна была предусматривать подключение цифровых приборов и оборудования напрямую к СПД, т.е. без использования модемов.

Несмотря на то что ISDN-сеть еще не достигла того же уровня распространения, как обычный телефон, уже в 1988 г. появилось второе поколение этого проекта. Первое поколение этой сети называется Narrowband ISDN — узкополосная, или низкоскоростная, ISDN (N-ISDN). Это СПД, которая поддерживает сервис с коммутацией каналов, сервис с коммутацией пакетов и передачу цифровых

данных по аналоговым каналам, обеспечивая пропускную способность цифровых каналов 64 Кбит/с. Одним из важных технических преимуществ N-ISDN стало введение передачи по протоколам Frame Relay (см. подразд. 5.3).

Второе поколение сети ISDN называется Broadband ISDN — широкополосная, или высокоскоростная, ISDN (B-ISDN). Эта сеть поддерживает высокую скорость передачи данных (сотни Мегабит в секунду) и функционирует на основе только коммутации пакетов. Одним из основных технических преимуществ сети B-ISDN стало использование асинхронного метода передачи. Здесь мы уделим основное внимание рассмотрению этого современного варианта сети ISDN — B-ISDN.

### **5.4.2. Принципы организации СПД ISDN**

Приведем принципы организации СПД ISDN, определенные МСЭ и опубликованные в рекомендации I.120 в 1993 г.

1. *Поддержка голосовых и не голосовых приложений с использованием определенного набора стандартизованных средств.* Этот принцип определяет цели ISDN и средства их достижения. СПД ISDN поддерживает разнообразные сервисы, т.е. и голосовую связь (телефон), и не голосовую связь (обмен данными в цифровой форме). Эти сервисы предоставляются в строгом соответствии со стандартами МСЭ, которые определяют интерфейсы и способы передачи данных.

2. *Поддержка приложений, использующих как коммутируемые, так и некоммутируемые каналы.* В ISDN используется и коммутация каналов, и коммутация пакетов. СПД ISDN поддерживает приложения, в которых используется:

- выделенные цифровые каналы;
- коммутируемые телефонные сети общего пользования;
- сеть передачи данных с коммутацией каналов;
- сеть передачи данных с коммутацией пакетов;
- сеть передачи данных с трансляцией кадров (FR).

3. *Ориентация на соединения с пропускной способностью 64 Кбит/с.* ISDN-соединения, основанные как на коммутации каналов, так и на коммутации пакетов, должны обеспечивать скорость передачи 64 Кбит/с. Это одна из основных характеристик ISDN, которая была выбрана вследствие того, что она являлась стандартной для передачи голоса в оцифрованной форме и поддерживалась интегрированными цифровыми сетями (Integrated Digital Network — IDN). Однако очень скоро оказалось, что этой скорости недостаточно. СПД второго поколения (B-ISDN) обеспечивает существенно большую скорость передачи.

4. *Интеллектуальные сети.* СПД ISDN должна поддерживать сервис высокого уровня: например выполнять переадресацию звонков, автоматически определять разные виды терминалов и т.д.

5. *Использование уровневой архитектуры.* Протоколы доступа к СПД ISDN должны иметь уровневую архитектуру, соответствующую OSI-модели, что обеспечивает целый ряд преимуществ:

- для OSI-модели уже создано много стандартов, например протокол HDLC;
- возможность создания новых ISDN-стандартов на основе уже существующих, а следовательно, сокращение стоимости их реализации;
- возможность независимого развития и реализации стандартов разных уровней.

6. *Использование разнообразных конфигураций каналов и физического оборудования.* Это обеспечивает приспособляемость ISDN к различиям технологической политики в разных странах, уровней технологий и имеющегося оборудования.

### 5.4.3. Архитектура СПД ISDN

Основой ISDN-архитектуры является концепция *битового потока в цифровом тракте*, или просто *цифрового тракта*. При этом неважно, чем был сформирован этот поток битов (телефоном, факс-машиной, компьютером и т. п.), а важно, что биты можно передавать по тракту в обоих направлениях.

Цифровые тракты могут мультиплексировать с разделением по времени в несколько независимых цифровых потоков. Концепция цифрового тракта строго специфицирована. В спецификации определены интерфейсы, формат цифрового потока и правила мультиплексирования потоков. Причем были разработаны два стандарта: один для низкоскоростной передачи (для домашнего использования), а второй для высокоскоростной (для бизнес-приложений).

Битовый тракт в ISDN может быть мультиплексирован по нескольким стандартным каналам:

- А — стандартный аналоговый телефонный канал;
- В — цифровой канал с импульсно-кодовой модуляцией для голоса или данных на 64 Кбит/с;
- D — цифровой канал на 16 или 64 Кбит/с;
- Н — цифровой канал на 384 (Н0), 1536 (Н1), 1920 (Н2) Кбит/с.

Канал типа В предназначен для поддержки следующих четырех видов соединений:

- *с коммутацией каналов.* Абонент инициирует вызов, под воздействием которого устанавливается соединение в СПД с коммутацией каналов, например в телефонной сети между двумя абонентами. По созданному каналу передается битовый поток;
- *с коммутацией пакетов.* Абонент подключен к узлу СПД с коммутацией пакетов и обменивается данными с другими абонентами, например посредством протоколов семейства X.25;

- *Frame Relay*. Абонент подсоединяется к узлу СПД Frame Relay, через который происходит обмен данными;

- *постоянное*. Это соединение с другим абонентом, которое было установлено заранее и динамически изменено быть не может, т.е. это соединение, подобное выделенной линии.

Канал типа D, во-первых, служит для управления коммутацией каналов, инициированной вызовом по интерфейсу с абонентом через канал В, а во-вторых, может использоваться, когда свободен, для коммутации пакетов или получения данных от оборудования на низкой скорости (до 100 бит/с).

Канал типа Н служит для высокоскоростной передачи данных. Абонент может использовать такой канал как высокоскоростную магистраль либо разделить ее с помощью метода TDM на подканалы. Обычно каналы этого типа используются для таких приложений, как факс, видео, высококачественные звуковые устройства.

Для подключения абонентов указанные каналы объединяются в так называемые интерфейсные структуры, или интерфейсы. В настоящее время лучше всего определены и часто используются два интерфейса: базовый и основной.

*Базовый интерфейс* (BRI — Basic Rate Interface), или *базовый доступ* (BA), состоит из двух каналов типа В и одного канала типа D.

*Основной интерфейс* (PRI), или *основной доступ* (PA — Primary Access), предназначен для пользователей с большими требованиями к пропускной способности сети (1 544 Кбит/с и более). Существует два варианта основного интерфейса: для передачи со скоростью 1 544 Кбит/с, что соответствует стандарту T1, и для передачи со скоростью 2 048 Кбит/с, что соответствует стандарту E1. В первом варианте основной интерфейс включает в себя 23 В-канала и один D-канал, а во втором — 30 В-каналов и один D-канал. При этом по всем каналам передача данных идет синхронно.

Длина кадра у базового интерфейса равна 48 разрядам: по 16 разрядов на каждый В-канал и 4 бит для D-канала. Остальные 12 разрядов носят служебный характер. Кадр основного интерфейса для передачи со скоростью 1,544 Мбит/с имеет длину 193 бит и занимает 125 мкс, а для передачи со скоростью 2,048 Мбит/с — длину 256 бит и занимает те же 125 мкс.

Базовый интерфейс (BRI) может поддерживать не только схему 2В + D, но и схемы В + D и просто D (когда пользователь направляет в сеть только пакетизированные данные).

Возможны варианты интерфейса PRI с меньшим числом каналов типа В, например 20В + D. Каналы типа В могут объединяться в один логический высокоскоростной канал для передачи с общей скоростью до 1 920 Кбит/с. При установке у пользователя нескольких интерфейсов PRI все они могут иметь один канал типа D. Число каналов В в интерфейсе, который не имеет канала D, может увеличиваться до 24 или 31.

Основной интерфейс может быть создан на основе каналов типа N. При этом общая пропускная способность такого интерфейса все равно не должна превышать 2,048 или 1,544 Мбит/с. Для каналов типа N0 возможны следующие схемы интерфейсов: 3N0 + D — американский вариант и 5N0 + D — европейский. Для каналов N1х возможен интерфейс, состоящий только из одного канала N11 (1,536 Мбит/с) — американский вариант или одного канала N12 (1,920 Мбит/с) и одного канала D — европейский вариант.

#### 5.4.4. Подключение оборудования пользователей

Подключение пользовательского оборудования к СПД ISDN осуществляется в соответствии со схемой, показанной на рис. 5.17, в которой все оборудование пользователей подразделяется на функциональные группы. В зависимости от функциональных групп различают несколько типов точек подключения (reference points) оборудования [40].

Устройства функциональной группы NT1 (Network Termination 1) подключаются через точку типа U. Фактически NT1 представляет собой устройство, которое работает на физическом уровне и образует дуплексный канал с соответствующим устройством, установленным на территории оператора СПД ISDN. Если пользователь подключен через интерфейс BRI, то абонентская линия — обычное окончание аналоговой телефонной сети, т. е. витая пара, используемая по стандарту DSL BRI (см. подразд. 5.1.5). Максимальная длина абонентской линии в этом случае составляет 5,5 км. При использовании интерфейса PRI абонентская линия представляет собой четырехпроводную линию, функционирующую по стандарту T1 или E1, с максимальной длиной около 1 800 м.

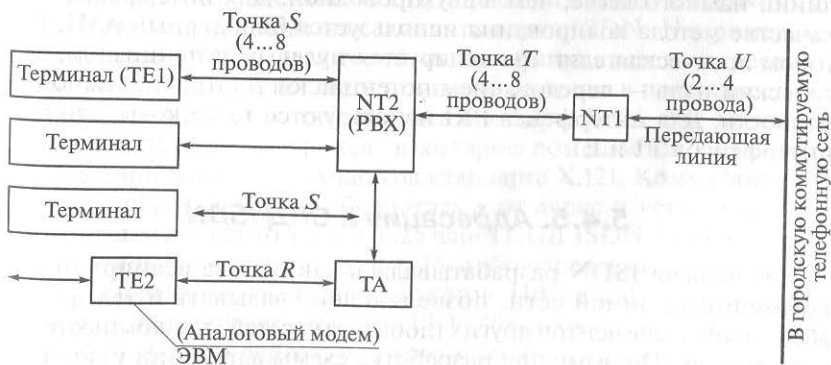


Рис. 5.17. Основные конфигурации подключения оборудования

*Устройства функциональной группы NT2* (Network Termination 2) выполняют функции концентратора битовых потоков от оборудования пользователя и осуществляют их мультиплексирование. К этому типу оборудования относятся: офисная АТС (PBX), обеспечивающая коммутацию каналов; коммутатор пакетов (например, по каналу D); простой мультиплексор TDM, который мультиплексирует несколько низкоскоростных битовых потоков в один канал типа В. Оборудование типа NT2 подключается к устройству NT1 через точку типа Т. Наличие оборудования этого типа не является обязательным в СПД ISDN в отличие от оборудования типа NT1.

*Устройства функциональной группы TE1* (Terminal Equipment 1) поддерживают интерфейс пользователя BRI или PRI. Точка подключения типа S соответствует точке подключения отдельного терминального оборудования, поддерживающего один из интерфейсов пользователя СПД ISDN, например цифрового телефона или факс-аппарата. Так как оборудование типа NT2 может отсутствовать в СПД ISDN, то точки подключения типов S и Т объединяются и обозначаются как S/T.

*Устройства функциональной группы TE2* (Terminal Equipment 2) не поддерживают интерфейсы BRI и PRI. К таким устройствам может относиться компьютер и устройства с последовательными интерфейсами, не относящимися к ISDN, например RS-232C, X.21 или V.35. Для подключения такого устройства к СПД ISDN необходимо использовать терминальный адаптер (Terminal Adaptor — TA). Для компьютеров терминальные адаптеры выпускаются в формате сетевых адаптеров, т. е. в виде встраиваемой карты.

Физически интерфейс в точке S/T представляет собой четырехпроводную линию. Кабель между устройством TE1 или TA и сетевым окончанием NT1 или NT2 обычно небольшой длины, поэтому разработчики стандартов ISDN решили не усложнять оборудование, поскольку организация дуплексного режима в четырехпроводной линии намного легче, чем в двухпроводной. Для интерфейса BRI в качестве метода кодирования используется биполярный АМІ, в котором логическая единица кодируется нулевым потенциалом, а логический ноль — чередованием потенциалов противоположной полярности. Для интерфейса PRI используются те же коды, что и для интерфейсов T1 и E1.

#### **5.4.5. Адресация в СПД ISDN**

Технология ISDN разрабатывалась как основа всемирной телекоммуникационной сети, позволяющей связывать и телефонных абонентов, и абонентов других глобальных сетей, т. е. компьютерных и телексных. Поэтому при разработке схемы адресации узлов ISDN необходимо было сделать ее, во-первых, достаточно емкой для всемирной адресации, а во-вторых, совместимой со схемами адресации

других СПД, чтобы абоненты этих СПД в случае соединения своих СПД через СПД ISDN могли бы пользоваться привычными форматами адресов.

Существуют разные подходы к созданию схем адресации. Например, разработчики стека TCP/IP пошли по пути введения собственной системы адресации, независимой от систем адресации объединяемых сетей, а разработчики технологии ISDN пошли по другому пути: они решили добиться использования в адресе ISDN адресов объединяемых сетей.

Основное назначение ISDN — это передача телефонного трафика, поэтому за основу адреса ISDN был взят формат международного телефонного плана номеров, описанный в стандарте МСЭ E.163. Однако этот формат был расширен для обеспечения поддержки большего числа абонентов и возможности использования в нем адресов других СПД, например X.25. Стандарт адресации в СПД ISDN получил номер E.164.

Формат E.163 предусматривает до 12 десятичных цифр в номере, а формат адреса ISDN в стандарте E.164 расширен до 55 десятичных цифр. В СПД ISDN различают *номер абонента* и *адрес абонента*. Номер абонента соответствует точке *T* подключения всего пользовательского оборудования к СПД. Например, вся офисная АТС может идентифицироваться одним номером ISDN. Номер ISDN, состоящий из 15 десятичных цифр, подразделяется, как и телефонный номер, по стандарту E.163 на поля «Код страны» (от 1 до 3 цифр), «Код города» и «Номер абонента». Адрес ISDN включает в себя номер и до 40 цифр подадреса. Подадрес используется для нумерации терминальных устройств за пользовательским интерфейсом, т.е. устройств, подключенных к точке *S*. Например, если на предприятии имеется офисная АТС, то ей можно присвоить один номер, например 7-095-640-20-00, а для вызова абонента, имеющего подадрес 134, внешний абонент должен набрать номер 7-095-640-20-00-134.

При вызове абонентов из СПД, не относящейся к ISDN, их адреса может непосредственно заменять адрес ISDN. Например, адрес абонента сети X.25, в которой используется система адресации по стандарту X.121, может быть помещен целиком в поле адреса ISDN, но для указания того, что это адрес стандарта X.121, ему должно предшествовать поле префикса, в которое помещается код стандарта адресации, в данном случае код стандарта X.121. Коммутаторы СПД ISDN могут корректно обработать этот адрес и установить связь с требуемым абонентом СПД X.25 через СПД ISDN либо, коммутируя канал типа В с коммутатором X.25, либо передавая данные по каналу типа D в режиме коммутации пакетов. Правила формирования префикса устанавливает стандарт ISO 7498, определяющий достаточно сложный формат адреса, и мы его здесь рассматривать не будем [40].

Еще одним способом вызова абонентов из других СПД является указание в адресе ISDN двух адресов: адреса ISDN пограничного

устройства (например, соединяющего СПД ISDN с СПД X.25) и адреса узла в СПД X.25, которые должны разделяться специальным разделителем. Эти адреса используются в два этапа: сначала СПД ISDN устанавливает соединение типа коммутируемого канала с пограничным устройством, присоединенным к ней, а затем передает этому устройству вторую часть адреса, чтобы оно осуществило соединение с требуемым абонентом.

#### 5.4.6. Стек протоколов в СПД N-ISDN

В СПД ISDN есть два стека протоколов: стек каналов типа D и стек каналов типа B (рис. 5.18).

Каналы типа D образуют достаточно традиционную СПД с коммутацией пакетов, прообразом которой послужила СПД X.25. Для сети каналов типа D установлены три уровня протоколов: физический протокол, определяемый стандартом I.430/431; канальный протокол LAP-D, определяемый стандартом Q.921, а на пакетном уровне протокол Q.931, с помощью которого выполняется коммутация вызова абонента службы с коммутацией каналов, или протокол X.25, при использовании которого в кадры протокола LAP-D вкладываются пакеты X.25 и коммутаторы ISDN выполняют роль коммутаторов X.25.

Для мониторинга и управления СПД ISDN сеть каналов типа D использует так называемую *систему сигнализации номер 7* (Signal System Number 7 — SS7). Эта система, разработанная для внутреннего мониторинга и управления коммутаторами телефонной сети обще-

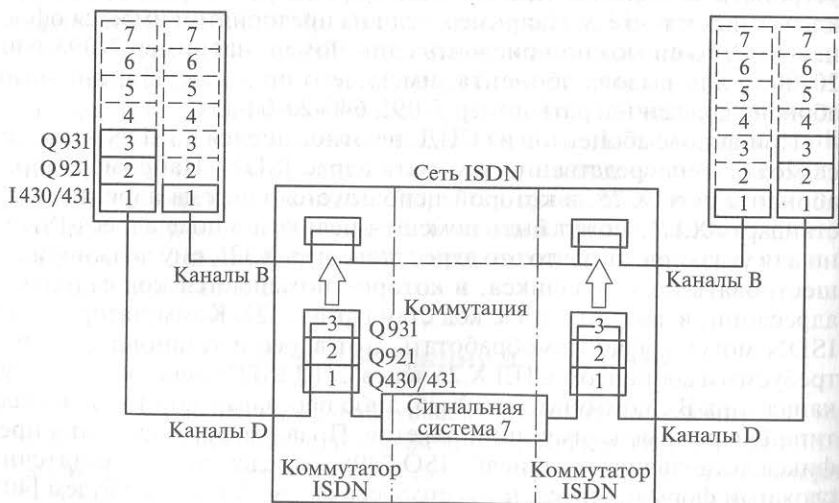


Рис. 5.18. Стек протоколов в СПД N-ICDN

го назначения, здесь рассматриваться не будет. Однако отметим, что конечному пользователю услуги службы SS7 недоступны, так как сообщениями SS7 коммутаторы сети обмениваются только между собой.

Каналы типа В образуют СПД с коммутацией цифровых каналов. В терминах модели OSI на основе каналов типа В в коммутаторах СПД ISDN определен только протокол физического уровня 1.430/431. Коммутация каналов типа В происходит по указаниям, полученным по каналу D. Когда пакеты протокола Q.931 маршрутизируются коммутатором, происходит одновременная коммутация очередной части составного канала типа В от исходного абонента к конечному.

Протокол LAP-D, являющийся аналогом протокола LAP-B в СПД X.25, принадлежит семейству HDLC и обладает всеми родовыми чертами этого семейства, но имеет некоторые особенности. Адрес кадра LAP-D состоит из двух байтов, один из которых определяет код службы, куда пересылаются вложенные в кадр пакеты, а второй — используется для адресации одного из терминалов, подключаемых у пользователя к абонентской линии NT1. Терминальное устройство может поддерживать разные службы: службу установления соединения по протоколу Q.931, службу коммутации пакетов X.25, службу мониторинга СПД и т.д. Протокол LAP-D обеспечивает два режима работы: с установлением соединения (единственный режим работы протокола LLC2) и без установления соединения (режим LLC1 стандарта IEEE 802.1). Последний режим используется, например для управления и мониторинга СПД.

#### **5.4.7. Высокоскоростные ISDN-сети и ATM-сети**

МСЭ быстро осознало отставание N-ISDN и предложило новое поколение ISDN-сетей — это высокоскоростные ISDN (Broadband ISDN — B-ISDN). Фактически B-ISDN — это цифровые виртуальные каналы, по которым передаются пакеты фиксированной длины (ячейки) со скоростью 155 Мбит/с. Этой скорости вполне достаточно, чтобы обслуживать даже такие приложения, как высококачественное телевидение.

Основу B-ISDN составляет ATM-метод (см. подразд. 2.5.4), т.е. технология с коммутацией пакетов. В области коммутации каналов накоплен огромный опыт, поэтому переход на коммутацию пакетов — это был технологически принципиальный шаг вперед.

Итак, весь более чем вековой опыт, накопленный в области телекоммуникаций, и вся старая инфраструктура должны были быть кардинально пересмотрены, плюс затраты на создание соответствующей новой инфраструктуры, а это сотни миллиардов долларов. Так что это был непростой шаг.

#### **5.4.8. Виртуальные каналы в сравнении с коммутируемыми каналами**

Сети В-ISDN построены на основе своего рода компромисса между коммутацией каналов и коммутацией пакетов. Сервис в этих СПД ориентирован на соединения, но эти соединения не являются коммутируемыми физическими каналами, это коммутируемые виртуальные каналы. Как уже отмечалось, есть два вида виртуальных каналов: постоянные и коммутируемые. Постоянные каналы устанавливает оператор по запросу пользователя. Установка такого виртуального канала занимает обычно несколько дней, а период его действия, как правило, — несколько месяцев или лет. Коммутируемые каналы подобно телефонным каналам устанавливаются динамически по требованию и перестают действовать сразу после их использования.

В СПД АТМ сначала между передатчиком и приемником устанавливается виртуальное соединение с помощью специального служебного пакета, а затем во всех коммутаторах, через которые проходит виртуальное соединение, устанавливается соответствие между надлежащей физической линией и идентификатором виртуального соединения. Когда по установленному виртуальному соединению пакет поступает на коммутатор, по информации в заголовке пакета определяют, к какому виртуальному соединению этот пакет принадлежит, и направляют его по надлежащей физической линии.

Установление постоянного соединения означает, что в таблицах коммутаторов заранее прописаны соответствующие значения независимо от того, имеется трафик по данному соединению или нет.

#### **5.4.9. Передача в АТМ-сетях**

В сетях АТМ нет строго порядка поступления ячеек от различных источников. Ячейки могут поступать от разных источников и в разном порядке. Необязательно даже, чтобы поток ячеек от одного источника был непрерывен. Если возникают разрывы, то они заполняются ячейками ожидания. В стандарте АТМ требуется, чтобы ячейки могли передаваться носителями (кадрами, фреймами и т.п.) в рамках таких стандартов, как T1, T3, E1, SONET, FDDI и некоторых других.

В настоящее время скорость 155,52 Мбит/с является стандартной для сетей АТМ, так же как и учетверенная скорость 622,08 Мбит/с. Однако в ближайшем будущем возможно достижение скорости передачи 44 736 Мбит/с.

Стандартной средой передачи для АТМ является оптоволокно. Однако на расстояниях в сотни метров в них может использоваться коаксиальный кабель или витая пара 5-й категории. Применение оптоволокна обеспечивает передачу на расстоянии многих киломе-

тров. Каждая волоконно-оптическая линия соединяет либо компьютер с АТМ-переключателем, либо два АТМ-переключателя. АТМ-линии — это соединения типа точка—точка. При этом на одной линии не может находиться более одного источника ячеек. По каждой линии передача возможна только в одном направлении, поэтому для обеспечения полного дуплекса необходимы две АТМ-линии. С помощью АТМ-переключателей возможно дублирование одной и той же ячейки для передачи ее по нескольким линиям. Так реализуется режим вещания, т. е. передача «от одного ко многим».

## АТМ-переключатели

Рассмотрим основные принципы организации и функционирования АТМ-переключателей (коммутаторов). АТМ-переключатель имеет набор входных линий, по которым в него поступают ячейки, и, как правило, такое же число исходящих линий, по которым ячейки проходят после коммутации. Обычно переключатель работает синхронно: длительность цикла строго фиксирована. В течение каждого цикла просматриваются все входные линии и, если на линию к этому моменту целиком поступила ячейка, то она считывается и передается в центр коммутации, а затем на выходную линию.

Переключатель может быть конвейерным, т. е. обработка одной ячейки может занимать более одного цикла. Ячейки поступают асинхронно, таймер переключателя отмечает момент начала очередного цикла. Если ячейка не поступила целиком к началу цикла, то она должна ожидать начала следующего цикла.

Ячейки поступают со скоростью 155 Мбит/с. Учитывая что размер ячейки 53 байт, получаем около 360 000 ячеек/с. Таким образом, на обработку одной ячейки приходится около 2,7 мкс. Выпускаемые в настоящее время переключатели имеют от 16 до 1 024 входных линий, т. е. переключатель должен быть в состоянии обрабатывать за 2,7 мкс от 16 до 1 024 ячеек. При скорости передачи 622 Мбит/с переключающий центр должен обрабатывать очередную порцию ячеек за 700 нс. Благодаря тому что ячейки имеют фиксированную длину и небольшой размер (53 байт) коммутация при таких скоростях становится возможной. При переменной длине и большем размере ячейки задача создания АТМ-переключателя была бы намного сложнее.

Все АТМ-переключатели должны удовлетворять следующим требованиям:

- терять как можно меньше ячеек;
- никогда не менять порядок поступления ячеек по каждому виртуальному соединению.

Первое требование означает, что АТМ-переключатель должен обеспечивать достаточно большую скорость переключения без потери ячеек. Считается допустимой потеря одной ячейки на каждые  $10^{12}$  ячеек. В больших переключателях считается допустимой потеря



Рис. 5.19. Иллюстрация буферизации ячеек на входе АТМ-переклю­чателя

одной-двух ячеек за час работы. Второе требование — сохранять по­рядок поступления ячеек неизменным — существенно усложняет кон­струкцию переключателя, но таково требование АТМ-стан­дарта.

Одна из ключевых проблем конструкции АТМ-переключателей состо­ит в решении вопроса: что делать, когда сразу по нескольким ли­ниям пришли ячейки, которые должны быть отправлены по одной и той же выходной линии. Напрашивается следующее решение: одну ячейку обработать, а другую сбросить, но в силу первого требования к АТМ-переключателям оно не годится.

Возможно другое решение: буферизовать ячейки на входе пере­ключателя (рис. 5.19). Пусть в начале цикла 1 на его вход поступи­ло четыре ячейки, две из которых должны быть отправлены по линии 2. Поскольку из-за линии 2 возникает конфликт, то только три ячейки передаются на выходные линии, поэтому к началу цикла на выходе переключателя появятся три ячейки, но при этом на вход поступят новые ячейки. К началу цикла 3 на входе переключателя останется только одна ячейка, и очередь «рассосется» только на четвертом цикле. В случае буферизации ячеек на входе переключателя необходимо следить за тем, чтобы дисциплина обслуживания возникающих оче­редей была справедливой, т.е. чтобы равномерно обслуживались очереди на всех линиях.

Недостаток этого решения состоит в том, что очередь на входе может блокировать даже те ячейки, которые должны быть переком­мутированы на линии, где нет конфликтов. Поэтому на соответ­ствующем виртуальном соединении скорость упадет. Этот эффект называется *блокировкой на входе*. Кроме того, буферизация ячейки на входе требует дополнительной логики в схемах, что усложняет конструкцию АТМ-переключателя.

Альтернативным решением рассматриваемой проблемы может быть буферизация ячеек на выходе переключателя (рис. 5.20). Если несколько ячеек должны уйти по одной и той же линии, то они пере­даются на выход переключателя и там их буферизуют. При этом требуется меньше циклов, т.е. в нашем примере только 3. В 1987 г.



Рис. 5.20. Иллюстрация буферизации ячеек на выходе АТМ-переключателя

К. Карол показал, что буферизация на выходе эффективнее, чем буферизация на входе [72].

Рассмотрим конструкцию АТМ-переключателя, использующего буферизацию на выходе, который называется переключателем выталкивающего типа (рис. 5.21). Каждая входная линия в таком переключателе соединена с шиной, к которой подключены все выходные линии. Каждая входная шина имеет свой независимый механизм управления, что существенно упрощает конструкцию.

У каждой поступающей на переключатель ячейки аппаратно анализируется заголовок с целью определить, какому виртуальному соединению она принадлежит. Затем с помощью таблицы коммутации определяется выходная линия, через которую эта ячейка должна покинуть переключатель. Пересечение входной линии с соответствующей выходной линией активизируется, и, когда ячейка доходит до этого пересечения, она попадает в буфер. Ресурсов переключателя достаточно, чтобы буферизовать на одном выходе ячейки со всех входов, если это потребуется, или размножить ячейки, если их надо разослать по нескольким виртуальным соединениям.

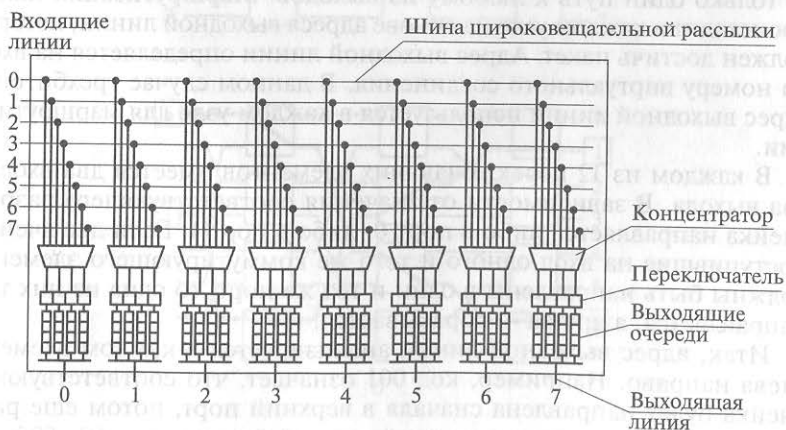


Рис. 5.21. Переключатель выталкивающего типа с конфигурацией 8 × 8 линий

Было бы естественным буферизовать все конфликтующие ячейки в выходном буфере. Однако при этом для переключателей, например на 1 024 линии, потребовалось бы 1 024 буферов по 1 024 × 53 байт, а это слишком много. Выходом из этой ситуации является выделение лишь  $n$  байт на буфер, где  $n$  — параметр настройки. Если же конфликтующих ячеек больше, то ячейки, не попавшие в буфер, сбрасываются. Причем здесь опять надо быть осторожным, определяя на каких входных линиях сбрасывать ячейки и из каких выходных буферов выталкивать ячейки на очередном цикле, чтобы предотвратить дискриминацию. Регулируя параметр  $n$ , можно варьировать стоимость и число сбрасываемых ячеек, что влияет на цену переключателя.

## Баньяновые переключатели Батчера

Основным недостатком переключателей выталкивающего типа является то, что центр коммутации — это прямой коммутатор, а следовательно, его сложность растет квадратично по отношению к числу коммутируемых линий. Из рассмотрения принципов построения коммутаторов для коммутации каналов известно, что одним из решений этой проблемы является использование каскадных коммутаторов. Аналогичное решение возможно и для коммутации пакетов.

Результат такого решения называется баньяновым переключателем Батчера. Как и переключатели выталкивающего типа, баньяновый переключатель Батчера синхронный, т. е. за один цикл он может обрабатывать несколько входных линий. На рис. 5.22, *а* показан трехступенчатый с конфигурацией  $8 \times 8$  баньяновый переключатель, получивший такое название, поскольку похож на заросли баньяновых деревьев. В баньяновых переключателях для каждого входа существует только один путь к любому из выходов. Маршрутизация пакета происходит в каждом узле на основе адреса выходной линии, которую должен достичь пакет. Адрес выходной линии определяется на входе по номеру виртуального соединения. В данном случае трехбитовый адрес выходной линии используется в каждом узле для маршрутизации.

В каждом из 12 переключающих элементов имеется два входа и два выхода. В зависимости от значения соответствующего разряда ячейка направляется либо в порт 0, либо в порт 1. Если две ячейки, поступившие на вход одного и того же коммутирующего элемента, должны быть направлены в один и тот же порт, то одна из них туда направляется, а другая — сбрасывается.

Итак, адрес выходной линии анализируется в каждом элементе слева направо. Например, код 001 означает, что соответствующая ячейка будет направлена сначала в верхний порт, потом еще раз в верхний, а только затем в нижний.

На рис. 5.22, *б* показаны примеры маршрутов следования двух ячеек в баньяновом переключателе. Коллизии в баньяновой сети

возникают, если в одном и том же элементе в одно и то же время требуется использовать один и тот же порт.

На рис. 5.23, *а* показан пример коллизий в баньяновом переключателе, а на рис. 5.23, *б* — способ их разрешения. Следовательно, можно сделать вывод, что в зависимости от распределения ячеек на входе баньяновая сеть либо будет терять ячейки, либо нет.

Идея Батчера состояла в том, чтобы переставить ячейки на входах таким образом, чтобы в баньяновой сети конфликтов не возникало.

Для сортировки входов Батчер в 1968 г. предложил специальный переключатель [58]. Подобно баньяновому переключателю переключатель Батчера строится из элементов по схеме  $2 \times 2$ , а работает синхронно и дискретно. В каждом элементе этого переключателя выходные адреса ячеек сравниваются. При этом ячейка с бóльшим адресом направляется по стрелке (рис. 5.24), а с меньшим — в противоположном направлении. Если ячейка одна, то она направляется против стрелки. Подчеркнем, что сравниваются не отдельные биты, а целые адреса как число.

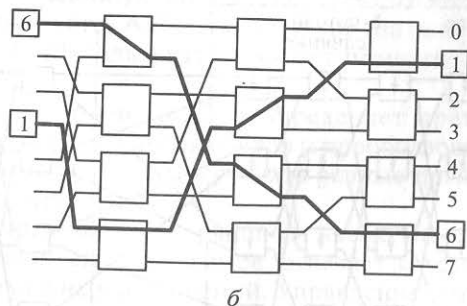
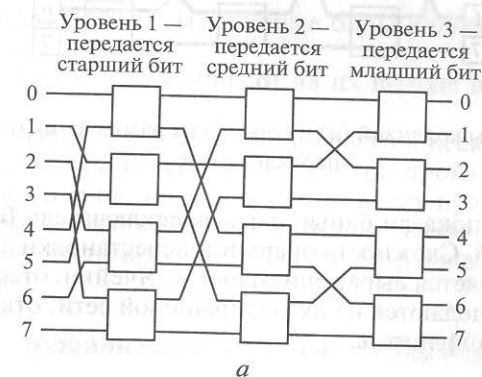
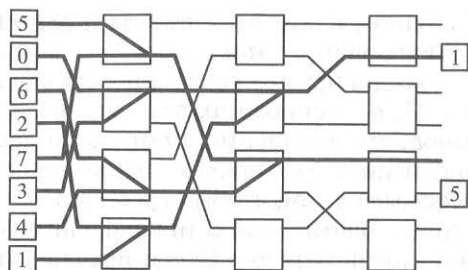
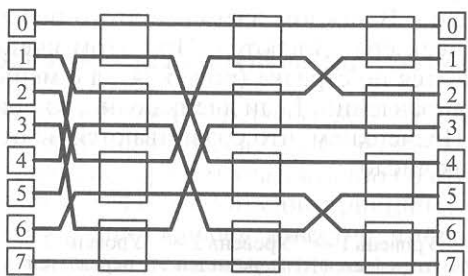


Рис. 5.22. Трехступенчатый баньяновый переключатель с конфигурацией  $8 \times 8$  линий (*а*) и примеры маршрутов следования двух ячеек в баньяновом переключателе (*б*)



а



б

Рис. 5.23. Примеры коллизий (а) и способа их разрешения (б) в баньяновом переключателе

На рис. 5.24 показан баньяновый переключатель Батчера с конфигурацией  $8 \times 8$ . Сложность операции перестановки для устройства Батчера определяется выражением  $n \log_2 n$ . Ячейки, отсортированные сетью Батчера, подаются на вход баньяновой сети, откуда они пересылаются без конфликтов.

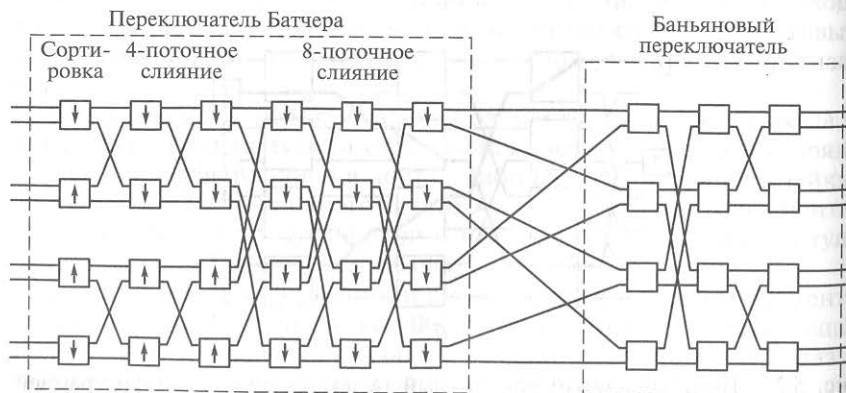


Рис. 5.24. Пример действия баньянового переключателя Батчера

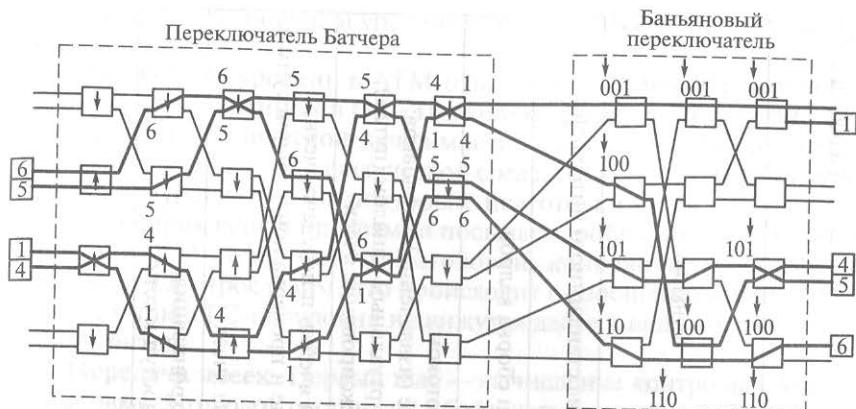


Рис. 5.25. Комбинация батчеровской и баньяновой сетей

На рис. 5.25 показан пример работы баньянового переключателя Батчера.

Известны две проблемы, которые баньяновые переключатели Батчера не могут решить:

- при возникновении коллизии на их выходе возможен только сброс;
- рассылка одной и той же ячейки сразу на несколько выходов.

Были предложены несколько вариантов промышленных переключателей этого типа, в которых по-разному преодолевались эти недостатки, однако основная идея при этом заключалась во встраивании между переключателем Батчера и баньяновой сетью специальной схемы.

### Уровень канала данных в СПД АТМ

Рассмотрим эталонную модель СПД АТМ, которая состоит из трех уровней: физического, АТМ-уровня и уровня адаптации (табл. 5.3). Поверх СПД АТМ пользователь может поместить, например стек ТСР/ІР.

Физический уровень в АТМ определяет правила передачи и приема данных в форме потока битов и преобразования их в ячейки. Носителями этого потока могут быть разные физические среды, у АТМ здесь нет ограничений.

АТМ-уровень отвечает за транспорт ячеек. Он определяет формат ячейки, заголовок, его содержимое, отвечает за установление и поддержание виртуальных соединений. Управление потоком и перегрузками также расположено здесь.

Уровень адаптации (Access Adaptation Layer — ААL) обеспечивает приложениям-пользователям возможность работы в терминах пакетов или подобных им единиц, а не ячеек.

## Уровни и подуровни СПД АТМ

Уровень OSI	Уровень АТМ	Подуровни АТМ	Функции
3/4	AAL	CS (Convergence Sublayer — подуровень сопряжения)	Предоставление стандартного интерфейса (сопряжения)
		SAR (Segmentation & Reassembly Sublayer — подуровень сегментации и сборки)	Сегментация и сборка кадров
2/3	АТМ	—	Управление потоком; формирование (извлечение) заголовков; управление виртуальным каналом (путем); (де)мультиплексирование ячеек
2	Физический	ТС (Transmission Convergence Sublayer — подуровень подготовки ячеек)	Разделение на ячейки и передача ячеек; формирование и проверка контрольной суммы заголовка; формирование ячеек
1		PMD (Physical Medium Dependent Sublayer — подуровень зависимости от физической среды)	Тактовая синхронизация; физический доступ к сети

Физический уровень и уровень адаптации имеют по два подуровня (см. табл. 5.3).

Физический уровень в АТМ охватывает физический уровень и уровень канала данных в OSI. Поскольку физический уровень АТМ на подуровне физической зависимости не предъявляет каких-то специальных требований к физической среде, то сосредоточит внимание на ТС-подуровне, т. е. на подуровне подготовки ячеек.

Когда прикладная программа посылает сообщение, оно движется вниз по АТМ-стеку, получая заголовки, концевики, разбиваясь на ячейки и т. д. Проследим, что происходит с сообщением, когда ячейки достигают ТС-подуровня и движутся далее в виде последовательности битов.

**Передача ячеек.** Первый шаг — вычисление контрольной суммы заголовка. Заголовок состоит из 5 байт, четыре из которых идентифицируют виртуальное соединение и несут контрольную информацию, а один — содержит контрольную сумму. Контрольная сумма защищает только первые четыре байта и не затрагивает данные в ячейке. Контрольная сумма вычисляется как CRC-код, т. е. как остаток от деления содержимого четырех байтов на полином  $x^8 + x^2 + x + 1$ . К этому остатку добавляется константа 01010101 для повышения надежности в случае, если заголовок содержит много нулей.

Решение защищать контрольной суммой только управляющую информацию было принято с целью сократить затраты на обработку данных на нижних уровнях. Защита собственно данных возлагается на верхние уровни, если это необходимо. Как уже отмечалось, многие приложения реального времени, например передача видео- и аудиоданных, более критичны к времени передачи, чем к степени искажения отдельных ячеек. Поскольку контрольная сумма защищает только заголовок, то этот байт так и называется НЕС (Header Error Control — контроль ошибки в заголовке).

Важным фактором, повлиявшим на выбор такой контрольной схемы, является то, что основной средой в АТМ является оптоволокно. Исследования, выполненные компанией AT&T, показали, что оптоволокно — высоконадежная среда, и единичные ошибки происходят в ней с вероятностью менее 1%. При этом схема НЕС прекрасно справляется как с однократными ошибками, так и множественными.

Для надежной передачи ячеек была предложена схема, в которой две последовательные ячейки объединяются через EXCLUSIVE OR, после чего получается новая ячейка, добавляемая в последовательность после первых двух. В результате ячейку, принятую с ошибкой или потерянную, легко можно восстановить.

После того как НЕС вычислен и добавлен в заголовок, ячейка готова к передаче. При этом среда передачи может быть как синхронной, так и асинхронной. В асинхронной среде ячейка посылается сразу, как только она готова к передаче. В синхронной среде ячейка передается в соответствии с временными соглашениями. Если ячей-

ки для передачи нет, то ТС-подуровень должен сгенерировать специальную ячейку ожидания.

Еще один вид служебных ячеек на ТС-подуровне — ОАМ (Operation And Maintenance). Эти ячейки используются АТМ-переключателями для проверки работоспособности системы.

Ячейки ожидания обрабатываются ТС-подуровнем, а ОАМ-ячейки передаются на АТМ-уровень.

Важной функцией ТС-подуровня является также генерирование ячеек в формате физической среды передачи. Это означает, что ТС-подуровень генерирует обычную АТМ-ячейку и упаковывает ее в кадр надлежащей среды передачи.

**Прием ячеек.** Итак, на выходе ТС-подуровень формирует НЕС-заголовок, преобразует ячейку в кадр, формирует АТМ-ячейки и передает поток битов на физический уровень. На противоположном конце соединении ТС-подуровень производит те же самые действия, но в обратном порядке: разбивает поток битов на кадры, выделяет ячейки, проверяет НЕС-заголовки и передает ячейки на АТМ-уровень.

Самое трудное — выделить кадр из потока битов. На уровне битов ячейка составляет  $53 \times 8 = 424$  бит. При этом нет маркеров ни начала, ни конца кадра. Как же определить границы кадра?

На ТС-подуровне имеется сдвиговый регистр на 40 бит. Если из этих 40 бит правые 8 бит представляют собой НЕС, то последующие 32 бит — это заголовок ячейки. Если это условие не выполнено, то все сдвигается на один бит и проверка повторяется. Этот процесс продолжается до тех пор, пока не будет обнаружен НЕС.

Представленная схема распознавания заголовка кадра ненадежна. Вероятность того что случайный байт будет выглядеть, как НЕС, в этом случае равна  $1/256$ . Для исправления схемы используется автомат, схема состояний которого изображена на рис. 5.26. Возможно три состояния автомата: HUNT, PRESYNC, SYNC. В состоянии HUNT автомат ищет НЕС. Как только похожий байт найден, автомат



Рис. 5.26. Схема состояний автомата для обнаружения заголовка НЕС

переходит в состояние PRESYNC и отсчитывает следующие 53 байт. Если предположить, что найденный НЕС — это начало ячейки, то сдвиг на 53 байт приведет к следующему НЕС. Проверив последовательно 8 ячеек, автомат переходит в состояние SYNC.

Если в состоянии автомата оказалось  $\alpha$  плохих последовательных ячеек, происходит переход в состояние HUNT.

## **5.5. Сотовая связь**

### **5.5.1. Сотовые и радиотелефоны**

Традиционные телефонные системы даже на основе широкополосного В-ISDN не в состоянии удовлетворить потребности в мобильной связи. Некоторым пользователям необходимы системы передачи данных, обеспечивающие доступ к сети в независимости от наличия кабеля. Категория таких пользователей имеет устойчивую тенденцию к расширению. Оконечным устройством у таких пользователей может быть и телефон, и факс, и ноутбук, и персональный помощник (PDA). Как было показано во введении, рынок этих систем огромен. Рассмотрим основные виды СПД, обеспечивающих мобильную связь.

Первые мобильные СПД появились в армии. Это были мобильные телефоны и радиостанции, которые в 1946 г. стали использоваться и в гражданских областях: в полиции, такси, скорой помощи и т. д. При этом одна станция, которая называлась базой, поддерживала связь на большой территории, например охватывала город. Как правило, база поддерживала несколько каналов, по каждому из которых можно было общаться в полудуплексном режиме. Говорящий должен был нажимать кнопку, когда говорил, и отпускать ее, чтобы слушать.

Следующий шаг — в 1960-е гг. в США появляется IMPPS (Improved Mobil telephone System), в которой уже каждый канал использовал две частоты: одну для получения сигналов, другую — для передачи. Таким образом, кнопка уже не требовалась. Эти системы могли поддерживать до 23 каналов, так что дозвониться по ним было довольно трудно.

### **Цифровая сотовая телефония**

Первые сотовые телефонные системы были аналоговыми, например система AMPS (Advanced Mobil telephone System, международный стандарт IS-41[71]). Им на смену пришли цифровые системы, которые составили второе поколение сотовых систем. В настоящее время происходит переход на сотовые системы 3G — системы третьего поколения.

Для перехода на цифровые системы было как минимум три причины:

- природа оцифрованных данных неважна, поэтому можно интегрировать в одном и том же канале и голос, и факс, и данные;
- для оцифрованных данных имеются хорошие алгоритмы сжатия, обнаружения и исправления ошибок;
- данные в цифровой форме можно шифровать в целях безопасности.

Конечно, было бы весьма желательно создать единый стандарт в области сотовой связи. Однако, как уже отмечалось в гл. 3, в области радиосвязи это невозможно. Например, в США и Японии созданы свои системы IS-54 и JDC, выделены свои диапазоны частот, отличные от европейских [65].

Европейская система GSM, которая с самого начала создавалась как цифровая, свободна от каких-либо компромиссов ради достижения совместимости с уже существующими системами. В настоящее время самая распространенная система, которая имеется и в США, правда, в несколько отличном от европейского диапазоне частот. В Европе для нее используют частоты 900 и 1800 МГц, а в США — 1900 МГц.

В 1980-е гг. только в Европе существовало пять разных сотовых аналоговых телефонных систем, поэтому, переезжая из страны в страну, пользователи вынуждены были менять и телефонные аппараты. Ясно, что это было чрезвычайно неудобно. В результате европейцы создали единую цифровую систему, известную как GSM (Global System for Mobile communications) [69], которая была введена в действие раньше американских и японских аналогов.

Идея организации любой сотовой системы связи, в том числе и сети GSM, очень проста. Вместо того чтобы охватить сразу всю необходимую территорию небольшим числом каналов, эту территорию разбивают на небольшие части — соты. В каждой соте используют свой набор каналов, но таким образом, чтобы частоты каналов соседних сот не пересекались, т. е. чтобы у них не было общих частот. Такая организация системы дает выигрыш в использовании частот вследствие возможности их повторного использования, а значит, увеличивается емкость сети — число одновременно обслуживаемых пользователей. Кроме того, в системе можно использовать маломощные сигналы, а следовательно, передатчик может быть компактным, так как не требуется мощных источников питания. Если в каких-то сотах из-за большого числа пользователей отказы в соединениях становятся слишком частыми, то эти соты можно разделить на несколько новых.

Каждая сота имеет базовую станцию (BS) — базу, состоящую из компьютера и приемно-передающей аппаратуры. Несколько BS подключаются к Центру мобильной коммутации (MSC). В небольших системах может быть достаточно одного такого центра, а в больших системах их может потребоваться несколько. MSC-центры соединяются друг с другом и с обычной наземной телефонной сетью и при необходимости коммутируют звонок с мобильного телефона на обычный телефон.

При перемещении телефона ближайшие базовые станции сравнивают уровень сигнала, поступающего от него, и та база, на которой этот уровень выше, чем на других, берет этот сигнал под свой контроль. При этом телефон получает сообщение об изменении базы.

Все каналы в соте подразделяются на следующие четыре категории:

- управляющие;
- для сообщений;
- для установки доступа и распределения каналов;
- для данных (голоса, факса и пр.).

Когда телефон включают, он начинает сканировать запрограммированный в нем список каналов управления, чтобы обнаружить наиболее мощный сигнал. По информации из управляющего канала он узнает о распределении каналов для сообщений, установки соединений и доступа, передачи данных.

Затем телефон сообщает через базовую станцию центру мобильной коммутации свою уникальную идентифицирующую информацию. Когда базовая станция получает такую информацию от телефона, она запрашивает у своего MSC-центра информацию о новом клиенте и сообщает домашнему MSC, т.е. MSC, к которому приписан этот телефон, о его текущем местоположении. Обычно такая перерегистрация телефона происходит периодически.

Чтобы позвонить, абонент набирает номер требуемого абонента и нажимает кнопку «Послать» (Send). Телефон по каналу установки доступа посылает информацию о себе и о телефоне вызываемого абонента. Получив запрос, базовая станция информирует о нем MSC. Если вызываемый абонент является абонентом компании, которой принадлежит MSC, то MSC ищет свободный канал для данных. Если такой канал найден, то MSC информирует о нем вызывающий телефон по каналу управления. Вызывающий телефон переключается на прием по указанному каналу и ждет, когда на вызываемом телефоне поднимут трубку (нажмут кнопку «Прием»).

Входящий звонок обрабатывается несколько иначе. В режиме ожидания телефон постоянно следит за каналом сообщений: т.е. не появится ли там сообщение для него. Когда вызывающий телефон сгенерировал запрос, то от MSC поступает запрос на домашний MSC вызываемого телефона, чтобы определить, в какой соте находится этот телефон. Пакет с вызовом направляется последней базовой станции, зарегистрировавшей телефон с искомым номером, например 75. Базовая станция распространяет по каналу сообщений специальное сообщение типа «75-й, ты здесь?» Вызываемый телефон отвечает по каналу управления специальным пакетом типа «Да». Тогда базовая станция шлет по каналу управления пакет типа «75-й, для вас вызов на канале 8», после чего вызываемый телефон переключается на канал 8 и начинает звонить до тех пор, пока на нем не нажмут кнопку «Прием». Такова общая схема работы сотовых систем

связи. Теперь рассмотрим эту схему применительно к стандарту GSM.

Итак, GSM — это полностью цифровая система. При этом в любой стране может быть одна или несколько функционирующих GSM-сетей, причем каждая такая сеть является региональной мобильной сетью оператора (PLMN). Зона действия каждой PLMN-сети ограничена национальными границами. Впрочем, в одной стране может быть несколько PLMN-сетей.

GSM-пользователь заключает контракт с одной из PLMN-сетей, называемой домашней, в котором указаны услуги, доступные этому пользователю. При желании пользователь во время работы может выбрать другую PLMN-сеть, если ему доступны ее услуги. Терминал пользователя, который в GSM называется мобильной станцией — MS, а в просторечье — трубкой, обеспечивает пользователю такой выбор и показывает список доступных PLMN-сетей. Выбор из этого списка пользователь может сделать сам явно или MS-терминал сделает это автоматически с помощью заложенного в него программного обеспечения.

Как и в AMPS-системе, в GSM территория разбивается на области, обслуживаемые центром мобильной коммутации (MSC). Оператор PLMN-сети абсолютно свободен в разбиении области действия MSC-станции на соты. При этом у каждой PLMN-сети есть логически единая база данных, называемая Home Location Registers (HLR), где хранится информация обо всех пользователях, для которых эта PLMN-сеть является домашней. Физически HLR-база может быть распределенной. У каждой MSC-станции имеется база данных визитеров (Visitor Location Registers — VLR). Обычно одна VLR-база обслуживает одну MSC-станцию, но она может обслуживать и несколько станций. Базы данных HLR и VLR обеспечивают отслеживание текущего местонахождения каждого MS-терминала, находящегося в зоне действия MSC-станции, запрашиваемых услуг и т. д.

Мобильная станция GSM подразделяется на две части, одна из которых обеспечивает радиоинтерфейс, а другая — интерфейс с базами HLR и VLR и содержит информацию, идентифицирующую пользователя (Subscriber Identify Module — SIM). Идентифицирует пользователя SIM-карта, а не MS-терминал, поэтому ее можно вынуть из одного MS-терминала и вставить в другой.

Каждая SIM-карта уникальна в системе GSM и связана с IMSI-идентификатором (International Mobil System Identify). На SIM-карте хранятся идентификационная информация, список услуг, список выбираемых PLMN-сетей и т. п. Она также защищена паролем (PIN — Personal Identification Number). Вставив свою SIM-карту в трубку, пользователь тем самым персонифицирует ее. Благодаря SIM-карте поддерживается роуминг, т. е. доступ к услугам связи в чужой PLMN-сети.

Теперь рассмотрим, как в GSM отслеживаются перемещения пользователей. Когда MS-терминал входит в новую область регистрации, информация о нем заносится в VLR-базу, и он получает TMSI-идентификатор (Temporary Mobil Subscriber Identify). TMSI-идентификатор короче IMSI-идентификатора, поэтому именно он передается при взаимодействии MS-терминала и VLR-базы. TMSI-идентификатор действует только в зоне MSC-станции, ассоциированной с VLR-базой, выдавшей его. IMSI и TMSI — это внутренние идентификаторы системы, связанные с SIM-картой. Для соединения с абонентом используется телефонный номер, который в GSM называется Mobil Subscriber Integrated Service Digital Network Number (MSISDNM).

MS-терминал всегда может определить, находится он в старой или в новой области регистрации. Это происходит благодаря периодически рассылаемой BS-станцией информации внутри обслуживаемой ею соты. Если MS-терминал обнаруживает, что оказался в новой области, то он инициирует запрос на обновление регистрации, в котором сообщает идентификатор предыдущей области и TMSI-идентификатор, полученный им в этой области. Этот запрос BS-станция передает в MSC-центр, который, в свою очередь, передает его в VLR-базу. Эта новая VLR-база инициирует запрос к старой VLR-базе с просьбой предоставить IMSI-идентификатор терминала, соответствующий указанному TMSI-идентификатору. Получив от старой VLR-базы необходимую информацию, новая VLR-база начинает процедуру идентификации MS-терминала по полученной информации. Если процедура идентификации прошла успешно, то новая VLR-база, используя IMSI-идентификатор терминала, определяет адрес его HLR-базы.

Эта процедура весьма близка к аналогичной процедуре в AMPS-системе (стандарт IS-41) и основное ее отличие от AMPS-аналога состоит в повышенной информационной безопасности. Так, например, идентификация пользователя и доступных ему услуг происходит здесь на основе информации, получаемой новой VLR-базой как от старой VLR-базы, так от HLR-базы идентифицируемого MS-терминала, а не только от HLR-базы, как в AMPS-системе. Процедура установления соединения в GSM-системе аналогична процедуре установления соединения в AMPS-системе. Стандарт GSM занимает более 5 000 страниц, и здесь мы приводим лишь самое общее его описание.

В большинстве стран для GSM используются частоты 900 и 1 800 МГц, а в США из-за особенностей национального распределения частот применяется другой диапазон. При этом в каждой соте выделяется до 200 каналов: 124 канала — для абонентов, а остальные — резервные и служебные. Каждый канал состоит из двух полос: входящей — от базы к мобильной станции (терминалу) и исходящей — от мобильной станции (терминала) к базе. Каждая полоса имеет ширину в 200 кГц (рис. 5.27). Каждый из 124 частотных каналов может под-

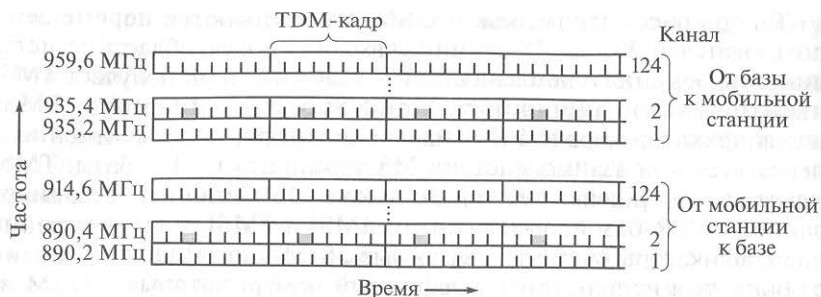


Рис. 5.27. Устройство GSM-каналов

держивать до восьми соединений, используя технику TDM-мультиплексирования. Теоретически может поддерживаться до 992 соединений одновременно.

Как уже говорилось, каждый канал поддерживает восемь разных соединений с помощью мультиплексирования с разделением по времени (TDM-метод). Каждому MS-терминалу выделяется одно соединение, т. е. один временной слот на одном из каналов.

Однако для обеспечения качества передачи и устранения помех из-за частотных конфликтов между каналами используются не все каналы. На рис. 5.28 показана иерархия кадров в GSM, которая имеет достаточно сложную структуру. Каждый TDM-кадр состоит из восьми кадров данных по 148 бит каждый. Один 1250-битовый TDM-кадр занимает 4,615 мс, а 26 TDM-кадров объединяются в мультикадр, занимающий 120 мс. Кроме того, имеется 51-кадровый мультикадр, не показанный на рис. 5.27 и используемый для нескольких каналов



Рис. 5.28. Иерархия кадров в GSM

управления на системном уровне. Например, для канала управления сотой, по которому передается информация для поддержки базы данных соты, а также для канала общего управления, который отвечает за регистрацию новых мобильных терминалов, поступивших в зону соты, выделение слотов для таких терминалов и многое другое.

В поле «Информация» на рис. 5.28 располагаются данные, закодированные кодом для обнаружения и исправления ошибок. При этом несложно подсчитать предельную пропускную способность на уровне TDM-кадра на одного пользователя:  $114 \text{ бит}/4,615 \text{ мс} = 24,7 \text{ Кбит/с}$ . Однако с учетом всех накладных расходов на синхронизацию, защиту от интерференции с другими кадрами, обнаружение и коррекцию ошибок реальная скорость передачи для пользователя составит не более 9 600 бит/с.

### **GPRS-служба**

Вполне естественно возникновение идеи по применению GSM-сетей для организации связи между компьютерами. Одним из существенных недостатков сетей сотовой связи стандарта GSM в настоящее время является низкая скорость передачи данных (максимум 9,6 Кбит/с) по одному соединению. При этом передачи данных абонент может использовать одно соединение, а оплата осуществляется, исходя из времени соединения (причем по тарифам, мало отличающимся от голосовых).

Для высокоскоростной передачи данных посредством существующих GSM-сетей была разработана служба пакетной передачи данных по радиоканалу GPRS (General Packet Radio Service). Необходимо отметить, что кроме повышения скорости (максимум составляет 171,2 Кбит/с) новая система предполагает иную схему оплаты услуги передачи данных, т.е. при использовании GPRS-службы расчет за услугу производится пропорционально объему переданной информации, а не по времени использования канала. К тому же GPRS-служба более рационально использует выделяемую полосу частот, т.е. особо не вдаваясь в технические тонкости, можно сказать, что пакеты данных передают одновременно по нескольким соединениям (именно за счет одновременного использования нескольких соединений и получается выигрыш в скорости) в паузах между передачей речи. Поскольку голосовой трафик имеет безусловный приоритет перед трафиком данных, скорость передачи информации определяется не только возможностями сетевого и абонентского оборудования, но и загрузкой сети. Ни один канал GPRS-службы не занимается под передачу данных полностью — и это является основным качественным отличием новой технологии от описанных ранее.

Разумеется, разработчики GPRS-службы приложили все усилия, для того чтобы установка новой системы «поверх» существующих GSM-сетей оказалась как можно менее обременительной (и разо-

рительной, что немаловажно) для операторов сотовой связи. Рассмотрим подробнее, какие новые блоки и связи появляются в общей архитектуре системы сотовой связи стандарта GSM с внедрением GPRS-службы.

### Внутренняя организация GPRS-службы

Доработку GSM-сети для предоставления GPRS-услуг можно условно подразделить на программную и аппаратную. Если говорить о программном обеспечении, то оно нуждается в замене или обновлении практически полностью, начиная с баз HLR и VLR и заканчивая базовыми станциями (BS). В частности, для временных кадров каналов GSM вводится режим многопользовательского доступа, а в HLR-базе появляется новый параметр — Mobile Station Multislot Capability (число соединений, которое одновременно может занимать мобильный телефон абонента).

Ядро системы GPRS (GPRS Core Network) состоит (рис. 5.29) из двух основных узлов: узла поддержки GPRS-сервиса (узел Serving GPRS Support Node — SGSN) и шлюзового узла GPRS (Gateway GPRS Support Node — GGSN).

В некотором смысле SGSN можно назвать аналогом MSC — центра мобильной коммутации сети GSM: он контролирует доставку пакетов данных пользователям, взаимодействует с HLR-базой собственных абонентов сети, проверяя разрешены ли запрашиваемые пользователями услуги, ведет мониторинг находящихся в режиме on-line пользователей, организует регистрацию вновь появившихся в зоне действия сети абонентов и т. п. Так же как и MSC-центр SGSN-узел в системе может быть не один, в этом случае каждый узел отвечает за свой участок сети.

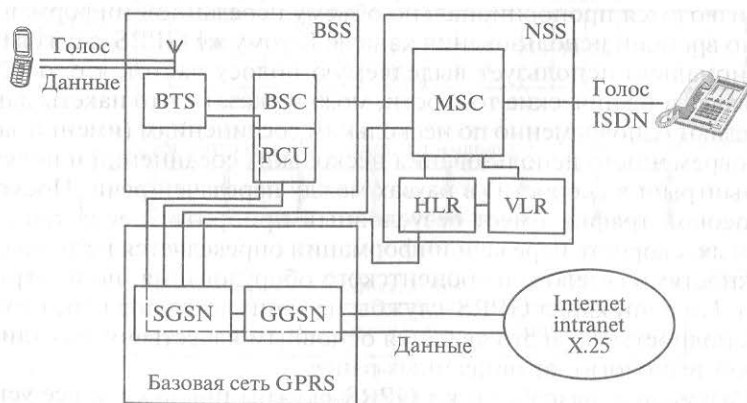


Рис. 5.29. Внутренняя организация GPRS-службы

Назначение GGSN-узла видно из его названия — это шлюз между сотовой сетью (вернее, ее частью для передачи данных через GPRS-службу) и внешними информационными магистралями (Интернетом, корпоративными интранет-сетями, другими GPRS-системами и т. д.). Основной задачей GGSN-узла является коммутация данных, идущих через SGSN-узел к абоненту и от абонента. Вторичными функциями GGSN-узла являются адресация данных, динамическая выдача адресов в Интернет (IP-адресов), а также отслеживание информации о внешних сетях и собственных абонентах (в том числе тарификация услуг).

В GPRS-службе заложена хорошая масштабируемость: при появлении новых абонентов оператор может увеличивать число SGSN-узлов, а при эскалации суммарного трафика — добавлять в систему новые GGSN-узлы.

Еще одной составной частью системы GPRS является блок контроля пакетной передачи (Packet Control Unit — PCU). Блок PCU стыкуется с контроллером базовых станций (BSC) и отвечает за направление трафика данных непосредственно от BSC к SGSN.

### Качество сервиса в GPRS

Следует отметить такой важный параметр функционирования GPRS-службы, как качество сервиса (Quality of Service — QoS). Очевидно, что видеоконференция в режиме реального времени и отправка сообщения электронной почтой предъявляют разные требования, например к задержкам на пути пакетов данных. Поэтому в GPRS существует несколько классов QoS, различающихся по следующим признакам:

- по приоритету (высокий, средний и низкий приоритет данных);
- надежности (разделение на три класса по числу возможных ошибок передачи, потерянных пакетов и т. п.);
- задержкам (задержки информации вне GPRS-сети в расчет не принимаются);
- количественным характеристикам (пиковое и среднее значения скорости).

Класс QoS выбирается индивидуально для каждой новой сессии передачи данных.

Стандарт услуги GPRS предусматривает два режима соединений:

- PTP (Point-To-Point — точка—точка);
  - PTM (Point-To-Multipoint — вещание).
- Режим PTM (вещания), в свою очередь, подразделяется на два класса:
- PTM-M (PTM-Multicast) — передача необходимой информации всем пользователям, находящимся в определенной географической зоне;
  - PTM-G (PTM-Group Call) — отправка данных определенной группе пользователей.

## Новый стандарт для 3G-сетей

Прежде чем перейти к рассмотрению стандартов для 3G-сетей, т. е. сетей третьего поколения, вспомним стандарт IS-95, в котором используется принципиально иной по сравнению с GSM-системами метод доступа. Этот метод называется разделением кодов — CDMA (Code Division Multiple Access), и он несовместим с методами, используемыми в AMPS- и GSM-системах (см. подразд. 4.3.8).

Следующим шагом на пути от GSM к сетям третьего поколения (3G-сети), или UMTS-системам (Universal Mobile Telephone System), является EDGE-служба (Enhanced Data Rates for GSM Evolution, в вольном переводе — ускоренная передача данных), позволяющая осуществлять передачу информации со скоростью до 384 Кбит/с в восьми GSM-каналах (48 Кбит/с на канал).

С EDGE-службой мобильный Интернет становится реальностью. Добавление EDGE-службы к существующим сетям второго поколения делает их совместимыми со стандартами МСЭ для 3G-сетей. EDGE-служба — это решение для 3G-сетей, которое позволяет существующей сетевой инфраструктуре предоставлять мощные современные мультимедийные услуги для мобильных терминалов. Реализация EDGE позволяет повысить и основные преимущества технологии GPRS-службы: быстрое установление соединений пакетной передачи и более высокую скорость в радиointерфейсе. Для внедрения EDGE-службы «поверх GPRS» операторам необходимо заменить аппаратуру базовых станций (BS), а пользователям — приобрести поддерживающие EDGE телефонные аппараты.

UMTS (Universal Mobile Telecommunications System) — универсальная система мобильных телекоммуникаций — это один из стандартов, разрабатываемых Европейским институтом стандартов телекоммуникаций (ETSI) для обеспечения внедрения 3G-сетей в Европе. В настоящее время основным фактором, определяющим развитие мобильной связи, является голосовая телефония. Появление GPRS и EDGE, а затем переход к UMTS-системе открывают и различные дополнительные возможности. UMTS — это высокоскоростная передача данных, мобильный Интернет, различные приложения на основе Интернета, интранета и мультимедиа (см. гл. 4 в т. 2 данного учебника).

Ключевой технологией для UMTS является широкополосный многостанционный доступ с разделением кодов — WCDMA (технология CDMA рассматривалась в гл. 4). Эта технология радиодоступа, выбранная в сентябре 1998 г. Европейским институтом стандартов телекоммуникаций, поддерживает все мультимедийные услуги 3G-сетей. Системы WCDMA/UMTS включают в себя усовершенствованную базовую сеть GSM и радиointерфейс с технологией WCDMA. Скорость передачи в радиоканале, предназначенном для мобильного абонента, достигает 2 Мбит/с. WCDMA предназначена для исполь-

зования в системах, работающих в частотном диапазоне 2 ГГц, позволяющем в полной мере использовать все преимущества этой технологии. Например, всего одна несущая WCDMA шириной 5 МГц должна обеспечить предоставление смешанных услуг со скоростями передачи от 8 Кбит/с до 2 Мбит/с, а мобильные терминалы, совместимые с WCDMA, смогут в соответствии с рекомендациями ITU обеспечивать сразу несколько услуг.

### **Услуги персональной связи**

В настоящее время предполагается, что для обеспечения услуг персональной связью у пользователя имеется только один номер, по которому он доступен, независимо от места его нахождения, т.е. в разных системах коммуникации один и тот же пользователь имеет, как правило, разные номера. Например, номер городского телефона (и не один), номер мобильного телефона (также не один), IP-адреса в сети, пейджер. Для каждого номера, как правило, имеется свой терминал со своим комплектом аксессуаров, батареей, зарядных устройств и т.д. Представьте себе выезд такого пользователя в командировку. В недалеком будущем все эти номера заменит один персональный номер. Это шаг к глобальному информационному пространству. Здесь сегодня сосредоточены усилия специалистов, и 3G-системы являются основными претендентами на эту роль.

### **5.5.2. СПД на основе WiMAX**

В гл. 3 рассматривался стандарт 802.11 — сети WiFi. Этот стандарт позволяет создавать беспроводные СПД в виде отдельных точек доступа с подключением к мощным магистральным «проводным» СПД, например к оптоволоконным. Это новая технология, позволившая развернуть множеством коммерческих СПД, в результате чего всего лишь за несколько лет сети WiFi выросли в серьезные корпоративные и публичные инфраструктуры. В настоящее время многие отели, аэропорты и вокзалы мира обладают СПД WiFi, а в некоторых странах таким образом обеспечивается обслуживание целых микрорайонов.

Безусловно, внедрение беспроводных WiFi-сетей стало революционным решением проблемы «последней мили». Однако изначально имевшиеся в стандарте ограничения по скорости обмена данными, радиусу действия, числу каналов и стоимости инфраструктуры не позволяли до недавнего времени СПД WiFi стать реальной альтернативой сотовым сетям, с одной стороны, и проводным сетям, — с другой. Даже несмотря на значительные преимущества и введение новых современных версий стандарта «врожденные» ограничения WiFi могут быть сняты только в комбинации с новыми магистральными стандартами обмена данными, такими как WiMAX.

WiMAX (Worldwide Interoperability for Microwave Access), стандартизированная институтом IEEE технология широкополосной беспроводной связи, дополняющая линии DSL и кабельные технологии в качестве альтернативного решения проблемы «последней мили» на больших расстояниях. На рис. 5.30 показано, как технология WiMAX может использоваться для реализации широкополосных соединений «последней мили», развертывания точек беспроводного доступа, организации высокоскоростной связи между филиалами компаний и решения других подобных задач.

WiMAX в версии IEEE 802.16-2004 — стандарт беспроводной связи, обеспечивающий широкополосную связь на площади радиусом до 50 км и по пропускной способности сравнимый с кабельными соединениями (до 100 Мбит/с). Технология WiMAX позволяет работать в любых условиях, в том числе в условиях плотной городской застройки, обеспечивая высокие качество связи и скорость передачи данных.

Оборудование СПД WiMAX функционирует в нескольких частотных каналах шириной 10 МГц в пределах диапазона 2...11 ГГц. Разумеется, специфическое распределение частотных диапазонов в разных странах диктует необходимость обеспечения возможности работы WiMAX на разных участках. Столь широкий разброс диапазонов выбран в целях учета специфики большинства стран мира. Так, в Северной Америке для WiMAX используются частотные диапазоны 2,5 и 5 ГГц, в Центральной и Южной Америке — 2,5, 3,5 и 5 ГГц, на Ближнем Востоке, в Африке, Западной и Восточной Европе — 3,5 и 5 ГГц, в Азиатско-Тихоокеанском регионе — 2,3, 3,5 и 5 ГГц.

В СПД WiMAX использована технология, которая обеспечивает доступ в Интернет со скоростью, производительностью и покрытием,

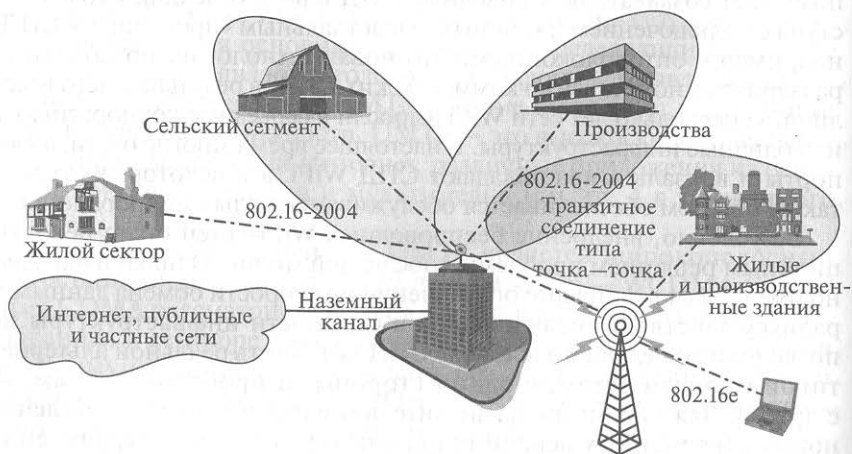


Рис. 5.30. Организация сети WiMAX

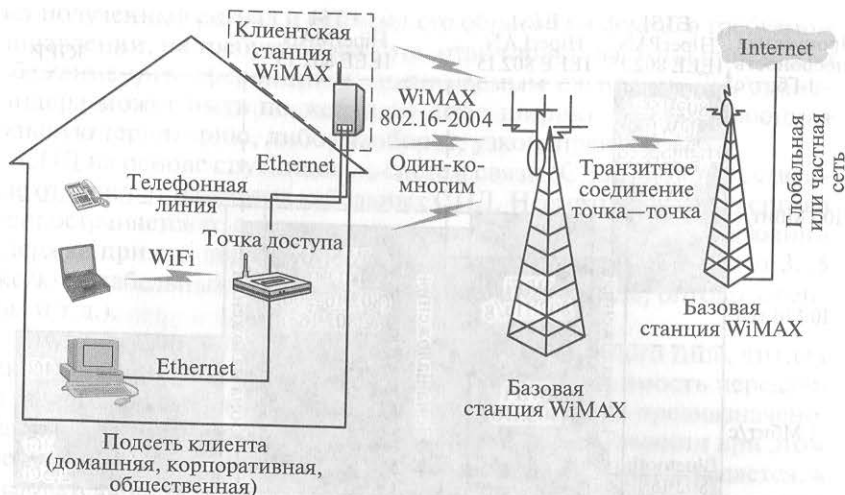


Рис. 5.31. Комбинация использования WiFi и WiMAX

гораздо большими, чем в СПД WiFi. В свою очередь, продолжением «магистральных веток» WiMAX как раз и становятся локальные СПД WiFi, различные типы бизнес- и бытовых кабельных DSL-сетей конечных пользователей. Пример подобной комбинации показан на рис. 5.31. Обеспечивая коммуникации в радиусе 10 км и более, точки WiMAX создают покрытие на значительных площадях, предоставляя пользователям достаточно гибкие условия для обеспечения этой самой пресловутой связи «последней мили».

В целом базовые характеристики стандарта 802.16 предусматривают дальность действия до 50 км, возможность работы вне прямой зоны видимости и в перспективе пиковую скорость обмена данными до 70 Мбит/с на сектор одной базовой станции при том, что типовая базовая станция будет иметь до 6 секторов покрытия.

Что касается возможностей стандарта WiMAX первого поколения — IEEE 802.16, принятого в 2004 г., в идеале по нему каждой базовой станцией обеспечивается доступ к данным на площади с радиусом до 50 км при скорости обмена данными до 35 Мбит/с. На практике ширина и соответствующая производительность канала выделяются конечному пользователю провайдером услуг.

Покрытие СПД WiMAX, в идеале напоминающее соты (только с более крупной ячейкой, чем, например, в GSM), подразумевает размещение антенно-фидерных устройств на высоких зданиях, сооружениях и мачтах. Неудивительно, что развертыванием СПД WiMAX в первую очередь заинтересовались провайдеры сотовой связи, поскольку, как бы ни была сильна конкуренция между WiMAX и сетями 3G/4G, установить и обслуживать несколько типов оборудования

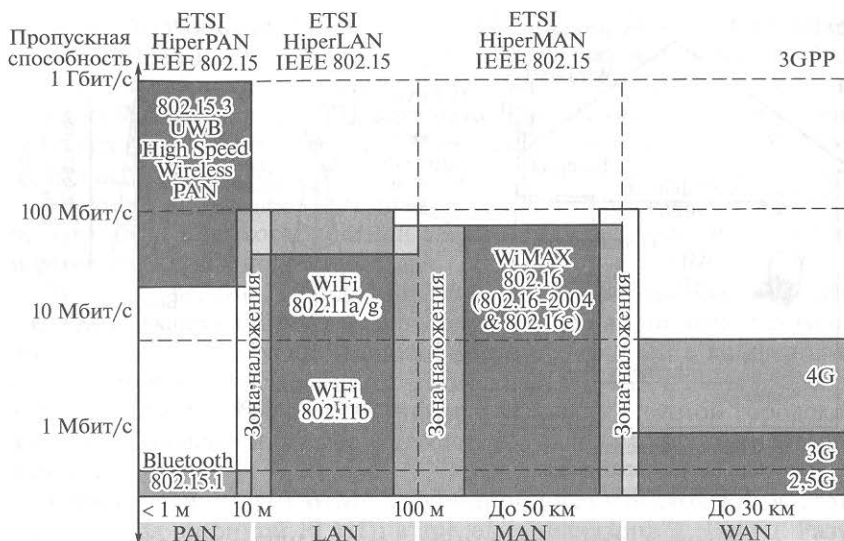


Рис. 5.32. Диаграмма соотношения стандартов Bluetooth, WiFi и WiMAX по скоростям и дальности действия

на одной мачте дешевле, нежели на нескольких, а уж потребитель сам определится с предпочтением выбора той или иной сети.

На рис. 5.32 показана диаграмма соотношения стандартов 802.15 (Bluetooth), 802.11 (WiFi) и 802.16 (WiMAX) по скоростям и дальности действия.

## 5.6. Спутниковая связь

### 5.6.1. Общие сведения

Идея создания системы связи на основе отражающего объекта, расположенного высоко над землей, давно витала в головах исследователей. Ее привлекательность состояла в том, что чем выше отражающий объект расположен над землей, тем большую часть поверхности Земли можно охватить связью при одинаковом угле обзора. Сначала пытались использовать в качестве такого объекта металлизированный воздушный шар, воздушные плотные массы и т.д. Однако сигнал возвращался настолько слабым, что практическое использование такой системы было невозможно. Первый спутник связи был запущен в СССР в 1962 г. Основное его отличие от всего предложенного ранее заключалось в том, что он усиливал сигнал прежде чем отправить его назад на Землю.

Спутник связи имеет несколько приемопередатчиков — транспондеров. Каждый транспондер слушает свою часть спектра, усили-

вает полученный сигнал и передает его обратно на Землю в требуемом направлении, на требуемой частоте, отличной от частоты приема, во избежание интерференции с принимаемым сигналом. Луч транспондера может быть по желанию либо широким, покрывающим большую территорию, либо, наоборот, узконаправленным.

СПД на основе спутниковых систем связи ( $C^3$ ) имеют существенные отличия от наземных кабельных СПД. Несмотря на то что сигнал распространяется со скоростью света, вследствие больших расстояний задержка при его передаче составляет 250...300 мс в отличие от 3...5 мкс/км в кабельных системах (в коаксиальном кабеле, оптоволоконном и т. д.).

Спутниковые системы принципиально вещательного типа, что для некоторых приложений очень важно. При этом стоимость передачи не зависит от того, скольким получателям сообщение предназначено. Однако проблема безопасности передаваемой информации при этом требует особого внимания, так как все слышат все, что передается, а следовательно, необходимо шифрование. Стоимость передачи также не зависит от расстояния.

Для справки: средняя стоимость спутниковой платформы оценивается сейчас в 150...210 млн долл. США, к чему необходимо добавить стоимость приемопередающей аппаратуры (транспондеров) и запуска, т. е. еще 150 млн долл.

По высоте и форме орбиты все  $C^3$  подразделяются на геостационарные (GEO — Geostationary Earth Orbit), высокоэллиптические (HEO — High Elliptic Orbit), средне-орбитальные (MEO — Middle Earth Orbit) и низкоорбитальные (LEO — Low Earth Orbit) [50, 71].

### **5.6.2. Геостационарные спутники**

Согласно третьему закону Кеплера период вращения спутника на высоте примерно 36 000 км над экватором равен 24 ч, причем наблюдателю на экваторе этот спутник будет казаться неподвижным. Благодаря такой неподвижности можно существенно упростить устройство наземной приемно-передающей антенной системы.

Из-за интерференции волн неразумно было бы размещать такие спутники ближе, чем на расстоянии  $2^\circ$  экваториальной плоскости друг от друга, если они работают на одинаковых частотах. Таким образом, в одно и то же время на экваториальной орбите может находиться не более 180 спутников, работающих на одной и той же частоте. Так как часть из этих орбит зарезервирована не только для целей связи, то спутников связи на самом деле меньше.

Обычно спутник связи имеет 12...20 транспондеров с полосой пропускания 36...50 МГц каждый. Транспондер с пропускной способностью 50 Мбит/с может использоваться для передачи одного потока данных со скоростью 50 Мбит/с либо для передачи 800 телефонных разговоров со скоростью 64 Кбит/с каждый, либо при каких-

то других комбинациях скорости и числа передаваемых потоков данных. При этом за счет поляризации сигнала можно сделать так, что два транспондера смогут использовать одну и ту же частоту.

В первых спутниках связи использовался один широкий луч, а в современных — используются несколько более узких лучей, пятно которых охватывает несколько сот километров поверхности Земли. Для геостационарных спутниковых систем связи (ГС<sup>3</sup>) характерны:

- большая область покрытия;
- очень большая задержка распространения сигнала;
- высокая стоимость;
- большая мощность приемопередающей аппаратуры;
- покрытие больших широт;
- стационарное размещение в пространстве относительно Земли.

Говоря о геостационарных спутниках надо также иметь в виду, что на высоте 1 500... 5 000 км и 13 000...20 000 км находятся радиационные пояса Ван Алена, которые препятствуют распространению радиосигналов и требуют дополнительной мощности передатчика для их преодоления. Эти пояса открыл в 1957 г. инженер НАСА Джеймс Ван Аллен.

Серьезную техническую проблему для ГС<sup>3</sup> долгое время представляло создание наземных терминалов. Из-за относительно малой мощности принимаемого сигнала наземные терминалы оборудовались большими антеннами (диаметром от 5 м и больше). Ориентация в пространстве на спутник таких массивных инженерных сооружений представляла собой непростую задачу. Относительно новой технологией для С<sup>3</sup> является технология малых антенн, называемых VSAT (Very Small Aperture Terminals — терминалы с очень маленькой апертурой), т.е. антенн с маленьким радиусом. Такой терминал имеет антенну диаметром 0,5...2,5 м, способную излучать сигнал мощностью 1 Вт, и может передавать данные со скоростью примерно 19,2 Кбит/с, а принимать — со скоростью 512 Кбит/с (см. подразд. 5.6.8).

В настоящее время США имеют около 30 геостационарных спутников, Канада — 8, Юго-Восточная Азия (включая Китай и Японию) — 25, Россия — 20, Западная Европа — 10; Intelsat — 25, «Интерспутник» — 11, Inmarsat — 8, Eutelsat — 8 и Arabsat — 4; кроме того, имеется около 60 военных, научных, а также теле- и радиотрансляционных спутников [52].

### **5.6.3. Спутники с высокоэллиптической орбитой**

Первой спутниковой системой с высокоэллиптической орбитой была советская «Молния», обеспечивающая трансляцию телепередач на всю территорию СССР. Обычно НЕО-спутник выводится на вытянутую эллиптическую орбиту, в одном из фокусов которой находится Земля. Поднимаясь на высоту около 40 тыс. км, а затем сни-

жаясь, спутник проводит над заданной территорией 8...12 ч в сутки, после чего быстро облетает Землю с другой стороны на высоте около 500 км. Вследствие некоторых геофизических причин существуют только две стабильные эллиптические орбиты: с наклоном 63 и 116° к экватору. При других углах наклона спутник постепенно сдвигается с заданной орбиты вследствие гравитационных возмущений Луны, неферичности Земли и других факторов.

Высокая орбита НЕО-спутника обуславливает те же проблемы, что и у геостационарных систем (слабый сигнал, большая мощность передатчика и задержка распространения сигнала), а также добавляет и множество других: необходимость наличия наземных станций с антеннами, следящими за траекторией спутника в пределах почти полусферы небосвода, и сложных приемопередающих устройств с большим динамическим диапазоном по чувствительности и выходной мощности (из-за сильного изменения дальности до спутника).

#### **5.6.4. Среднеорбитальные и низкоорбитальные спутники**

Теперь обсудим низкоорбитальные и среднеорбитальные спутниковые группировки, для которых характерны меньшие задержки, лучшие энергетические показатели и низкая стоимость наземных терминалов. МЕО-спутники запускаются на промежуточные круговые орбиты, т.е. на высоты порядка 10 тыс. км, где есть «просвет» между первым и вторым слоями Ван-Аллена.

Совершая один оборот вокруг Земли за 6...7 ч, такой спутник остается видимым из какой-либо точки поверхности не более 1,5...2,0 ч. Для обеспечения непрерывной связи создаются группы из 10...12 спутников, равномерно расставленных по нескольким орбитам, с перекрывающимися ориентациями антенн.

Поскольку МЕО-спутники почти вчетверо ближе к Земле, чем ГЕО-спутники, то благодаря обратной квадратичной зависимости рассеивания энергии от расстояния они выигрывают у последних в энергетике больше чем на порядок, а время задержки их сигналов снижается до 120...130 мс. На борту МЕО-спутников не устанавливается много транспондеров, там не требуются мощные передатчики, а значит, спутниковая платформа может быть меньше и легче (порядка 0,5 т) по сравнению с платформой ГЕО-спутников (на 1...3 т), т.е. выводить их на орбиту могут менее мощные и более дешевые ракеты.

Кроме того, МЕО-спутники могут быть запущены на полярную орбиту, чтобы закрыть и полярные зоны, которые не охватывают геостационарные спутники. Все это делает связь через МЕО-спутники, гораздо качественнее и дешевле, чем через ГЕО-спутники. Среднеорбитальные спутники имеют еще одно достоинство (уже по

сравнению с ЛЕО-спутниками): времени пребывания их «под солнцем» хватает для полной перезарядки батарей. Таким образом снижается зависимость от аккумуляторов — самых короткоживущих компонентов платформы — и повышается средний срок службы этих спутников, составляющий 10... 12 лет. Применение ядерных источников энергии пока ограничивается их массой и высоким уровнем радиации.

Среднеорбитальные системы более эффективны при построении сетей региональной связи с узловыми наземными станциями и «последней милей» в виде проводных или радиосетей, а также для организации массовой персональной связи, в том числе широкополосной. После освоения диапазонов миллиметровых волн с полосой пропускания, эквивалентной полосе пропускания хорошей оптоволоконной линии, по каналам связи можно будет осуществлять доступ к Интернету, передавать мультимедийную информацию, видеопрограммы и прочие многоканальные радио- и телеудовольствия. Такие проекты уже прорабатываются в США, например проект ICO корпорации Inmarsat (см. далее).

Хотя один МЕО-спутник намного дешевле двух трехтонных геостационарных спутников, для создания «эквивалентного» покрытия их требуется больше. Именно поэтому системы на МЕО-спутниках оказываются дороже GEO-систем, что и доказал проект ICO, расходы на который уже превысили 1,6 млрд долл.

И, наконец, низкоорбитальные, или ЛЕО-спутники, движущиеся на высотах от 500 до 1500 км. Ниже 500 км спутники не опускают, поскольку в этом случае их начинает тормозить атмосфера Земли (хотя и очень разреженная) и они начинают намного интенсивнее «сваливаться» к Земле. Малый период обращения (в среднем они делают один оборот вокруг Земли за 100...120 мин) сокращает время пребывания спутника в пределах видимости из одной точки поверхности до 10... 15 мин.

Существенно лучшие энергетические характеристики ЛЕО-спутников позволяют уменьшить наземные терминалы до размеров обычного сотового телефона или радиомодема. Однако, как и в случае с МЕО-спутниками, для обеспечения постоянной связи требуются группировки из нескольких десятков ЛЕО-спутников, цепочками вращающихся на разнесенных орбитах, при этом чем ниже орбита, тем больше требуется спутников и орбит, причем важно точно поддерживать взаимное расположение спутников.

ЛЕО-спутники проигрывают своим более «высоким» конкурентам во времени жизни из-за частого переключения энергетической системы с солнечных батарей на аккумуляторы и соответственно из-за увеличения числа циклов зарядки-разрядки батарей, вследствие чего срок их службы составляет 5... 8 лет. Обычно ЛЕО-спутник несет один транспондер, реже два или три, один из которых резервный. Однако по сравнению с GEO-спутниками на них чаще устанавливается слож-

ная электронная аппаратура коммутации потоков в целях осуществления «интеллектуальной» межспутниковой связи с четырьмя соседями, при этом число необходимых станций может быть небольшим.

Первый проект использования ЛЕО-спутников «Иридиум» выдвинула компания «Моторола» в 1990 г. Идея была очень проста: когда пятно луча одного спутника уходило из определенного места, к этому месту подлетал другой спутник, пятно которого охватывало это место. Подлетевший спутник «подхватывал» передачу-прием, которую вел улетающий спутник, и связь сохранялась. Компания подсчитала, что для реализации этой идеи потребуется 77 спутников на высоте 750 км. Позднее, после уточнения параметров проекта, это число сократилось до 66. Этот проект получил название «Иридиум» (по названию 77-го элемента из Химической таблицы Д. И. Менделеева).

Основной целью этого проекта являлось обеспечение связи с наземными средствами (даже портативными) по всей поверхности Земли. Этот проект вызвал ожесточенную конкуренцию со стороны других компаний: все захотели строить низколетящие спутниковые системы. Было предложено множество других проектов, но все они похожи на «Иридиум», поэтому мы рассмотрим его.

Проект предполагал размещение на высоте 750 км вдоль меридиана на расстоянии  $32^\circ$  друг от друга 11 спутников, таких ожерелий требуется шесть. Каждый спутник может обеспечить радиоконтакт для 48 зон. Всего система поддерживает одновременно 1 628 зон, покрывающих Землю. Поскольку площадь поверхности Земли равна 361 млн км<sup>2</sup>, нетрудно подсчитать, что одно пятно покрывает около 222 тыс. км<sup>2</sup>. Каждая сота (пятно) имеет 174 дуплексных канала на частоте обычного сотового радиотелефона. Таким образом, во всем мире поддерживаются 283 272 канала. При этом некоторые из них используются для обеспечения вещательной передачи текстовой информации (пейджинга) и для навигации, т. е. не требуют большой пропускной способности.

Итак, для низкоорбитальных систем характерны:

- малая область покрытия;
- малая задержка сигнала и низкая стоимость;
- использование маломощного сигнала;
- высокая наземная скорость спутника;
- короткое время жизни спутника (по сравнению с геостационарными).

### **5.6.5. Канальный уровень в спутниковых сетях**

Спутник связи имеет обычно несколько транспондеров. Каждый транспондер управляет лучом, покрывающим определенную часть поверхности Земли. При этом луч может создавать большую зону (до

10 000 км в поперечнике) или маленькую (до 250 км). Транспондер принимает сигналы от станций, расположенных в зоне луча, на одной частоте и может передавать на эти станции сигналы на другой частоте.

Луч нацеливается на определенную зону, антенна передает несколько кадров, и луч перемещается в другую зону. Время, в течение которого луч фиксируется в на определенной зоне, называется временем скважности.

Как и в любой СПД, важным вопросом является распределение каналов транспондеров. Из-за большой задержки передачи в канале (до 270 мс) использование несущей невозможно, и поэтому протоколы класса CSMA/CD, как, например, в Ethernet, здесь неприменимы. Здесь используются протоколы следующих пяти классов: маркерный доступ, ALOHA, FDM, TDM, CDMA, применение которых для спутниковой связи имеет некоторые особенности. В основном будем рассматривать передачу данных на спутник, поскольку при передаче со спутника имеется только один передатчик (транспондер на спутнике), и проблем распределения канала не возникает.

Обычным способом распределения одного канала между несколькими конкурирующими пользователями является объединение их каким-либо образом. Однако позволить конкурировать за свободный кадр произвольно при задержке 270 мс нельзя. Если наземные станции подключены к сети с коммутацией пакетов, имеется следующая возможность решения этой проблемы. Станции следует объединить в кольцо с маркером. При этом каждая станция должна знать своего предшественника или преемника в кольце. Передавать кадр станция может, только если она владеет маркером. Спутник ничего не знает о маркере. В случае если время передачи на спутник относительно велико, время передачи маркера мало, число станций невелико и постоянно, то такая схема работает неплохо.

Чистая ALOHA из-за низкой эффективности использования канала (18 %) обычно не применяется. Слишком дорого стоит спутник. Однако слотированная ALOHA вполне применима, т.е. одна из наземных станций берет на себя роль синхронизирующей станции и через спутник периодически транслирует синхросигналы всем станциям. Поскольку время передачи фиксированное, то легко подсчитать время начала слота  $k$  после очередного синхросигнала.

Для увеличения эффективности использования канала более чем на  $1/e$  применяют транспондер, который поддерживает два канала на разных частотах. Наземная станция выбирает один из них случайным образом. Если по обоим каналам сразу поступили кадры, то один из них буферизуют и передают позже. Такая техника за счет расширения полосы позволяет повысить эффективность использования канала до 73,6 %.

Частотное разделение (FDM-метод) по-прежнему остается одним из наиболее часто используемых методов распределения ка-

нала с множественным доступом. В этом случае канал с шириной полосы пропускания 36 МГц можно разбить примерно на 500 полос по 64 кГц каждая. Несмотря на простоту, техника FDM имеет недостатки, основной из которых заключается в том, что не вся ширина 500 полос может быть использована, так как значительная часть частот на границах полос уходит на изоляцию каналов друг от друга. В результате значительная часть полосы пропускания уходит на эти цели.

Вторым недостатком FDM-метода является необходимость контроля мощности станции. Поскольку если станция излучает слишком мощный сигнал, то часть мощности приходится на пограничные частоты между каналами, что приводит к нежелательным искажениям в соседних каналах.

Если число станций невелико и все они генерируют стабильно высокую нагрузку, то возможен статический подход к распределению FDM-канала. В противном же случае требуется динамический подход, который был реализован в системе SPADE (SPACE Dynamic Exchange) [40] и применяется на спутниках системы Intelsat. Полоса транспондера разбивается на 794 симплексных аналоговых канала с пропускной способностью каждого 64 Кбит/с и один общий канал управления с пропускной способностью 128 Кбит/с. Аналоговые каналы разбиваются на пары, образуя при этом полный дуплексный канал. В результате транспондер может передавать и принимать данные со скоростью 50 Мбит/с.

Общий канал управления (128 Кбит/с) разбивается с помощью техники TDM на слоты, и за каждой наземной станцией (их не более 50) закрепляется свой слот. Когда станция готова к передаче, она через свой слот сообщает об этом и захватывает один из 397 каналов данных. Если при захвате происходит коллизия, то станция ждет и в следующем цикле пытается опять получить канал. Закончив передачу, она с помощью управляющего канала освобождает захваченный ею канал данных.

Техника TDM, также давно используемая и хорошо освоенная, требует применения временной синхронизации для разбиения на слоты, что обычно обеспечивает специально выделенная станция. При этом для небольшого и постоянного числа станций можно использовать технику статического распределения слотов, а в случае переменного числа станций или переменной нагрузки от станций требуется применение динамической схемы распределения. Динамические схемы подразделяются на централизованные и децентрализованные.

В качестве первого примера использование централизованной схемы распределения слотов рассмотрим технологию ACTS (Advanced Communication Technology Satellite), предложенную в 1972 г. для системы из нескольких десятков станций [73]. Спутник в этом случае имел четыре канала с пропускной способностью по 110 Мбит/с, два

из которых работали на прием и два на передачу. У каждого из этих каналов имелся кадр, состоявший из 1728 слотов по 64 бит каждый, занимавший 1 мс и способный обеспечить голосовую передачу со скоростью 64 Кбит/с. Обеспечение максимального использования временных слотов каналов при передвижении луча по поверхности Земли выполняет специально выделенная главная станция управления (ГСУ), т. е. каждая наземная станция получает при необходимости слот, запрашивая его у ГСУ. При этом ГСУ имеет специальный канал, доступный всем наземным станциям без конкуренции, так как он статически разделен между ними. Работа ACTS включает в себя три этапа. На первом этапе спутник принимает 1728-слотовый кадр, на втором этапе эти 1728 слотов перераспределяются в необходимом порядке из входного буфера в выходной, а на третьем этапе выходной буфер «сбрасывается» на Землю.

Другая динамическая схема распределения слотов, предложенная Биндером в 1975 г. [73], используется, когда число станций не превышает число слотов. В этом случае за каждой станцией закрепляется свой слот. Если станции нечего передавать, она шлет сигнал ожидания в этом слоте, и все знают, что в следующем кадре этот слот можно занять по схеме ALOHA. Когда станция захочет вернуть свой слот, она просто пошлет свой кадр, вызывая коллизию. Тогда в следующем кадре этот слот уже никто не занимает, и он возвращается владельцу.

Имеется также и динамическая схема распределения, не накладывающая никаких ограничений на соотношение числа станций и числа слотов. Станции в ней конкурируют за слоты по схеме слотованной ALOHA. Если захват слота прошел успешно, то этот слот закрепляется за станцией и в следующих кадрах, т. е. до тех пор, пока она сама не освободит его.

В последней схеме последний слот в каждом кадре разбивается на мелкие слоты состязаний, и станции, желающие начать передачу, должны отметить свой подслот в предыдущем кадре, тогда в следующем кадре им будет выделен свой слот.

Несмотря на разнообразие схем и широкое применение, техника TDM имеет общие недостатки: необходимость временной синхронизации и наличие наземных станций, обеспечивающих очень высокую скорость передачи, для того чтобы уместить максимум данных во временном слоте.

Техника CDMA свободна от проблемы синхронизации и проблемы распределения канала. Однако она имеет следующие основные недостатки: во-первых, пока пропускная способность CDMA-канала ниже, чем TDM-канала; во-вторых, 128-разрядные последовательности частиц требуют наличия высокоскоростных передатчиков; в-третьих, пока число инженеров, владеющих этой техникой, недостаточно велико. Однако это, безусловно, очень перспективная техника и у нее большое будущее.

### **5.6.6. Основные категории СПД на базе С<sup>3</sup>**

Системы спутниковой связи с позиции используемого наземного терминального оборудования можно подразделить на три категории.

Первая категория включает в себя сети персональной спутниковой связи, такие как Iridium, Inmarsat, Globalstar и ICO. Терминалы персональной связи существенно отличаются от своих старших собратьев — VSAT-станций. Они более компактны, универсальны, сопрягаются с сетями сотовой связи, а самое главное — работают при движении абонента. Вместе с тем персональная связь пока неспособна обеспечить тот же комплекс и качество услуг, которые предоставляют VSAT-станции, да и тарифы в сетях персональной связи существенно выше.

Вторая категория систем спутниковой связи наиболее многочисленная. Она включает в себя корпоративные сети, базирующиеся на технологии VSAT, т. е. на использовании малогабаритных спутниковых терминалов с антеннами диаметром 1,8...2,5 м. На сегодняшний день в мире насчитывается около 300 тыс. станций VSAT.

Третья категория охватывает системы непосредственного телевизионного вещания, работающие, главным образом, в Ku-диапазоне частот (14/11 ГГц), что позволяет использовать для приема малые земные станции, стоимость которых не превышает 500 долл. Эта категория систем спутникового вещания ориентируется в первую очередь на сельское население и малые города со слаборазвитой кабельной инфраструктурой. Именно эта категория составляет большую часть населения России. Рассмотрим подробно системы первых двух категорий.

#### **Персональная спутниковая связь**

Традиционно инфраструктура связи России строилась на кабельных системах, и в настоящее время около 100 тыс. населенных пунктов нашей страны не имеют никакой оперативной связи с внешним миром, поскольку таковая до них еще «не дотянулась». Географически эти населенные пункты сосредоточены на севере страны, в Сибири и на Дальнем Востоке. В наши дни связь с этими районами можно обеспечить с помощью С<sup>3</sup>, не требующих в отличие от кабельной связи огромных средств на развертывание наземной инфраструктуры. Огромные пространства и низкая плотность населения на большей части территории нашей страны делают наземные каналы связи экономически неэффективными. Несмотря на бурный рост сотовых сетей связи различных стандартов, услуги персональной спутниковой связи в этих районах все еще предпочтительнее с финансовой точки зрения.

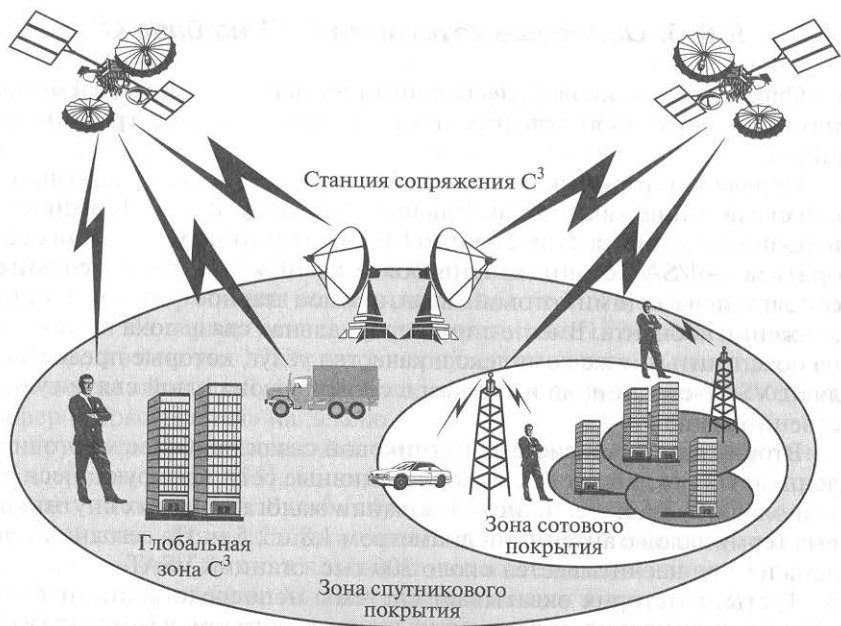


Рис. 5.33. Иллюстрация персональной спутниковой связи

Понятие персональной спутниковой связи (как в мире, так и в России) с самого начала означало не чисто спутниковую связь, а комбинацию  $S^3$  с существующими сотовыми сетями. При этом основным назначением спутниковой связи является дополнение и расширение возможностей сотовой связи за пределы ее зон покрытия, где создание инфраструктуры других видов связи по экономическим либо технологическим причинам нецелесообразно. Многорежимные абонентские терминалы при работе в зонах сотовой связи автоматически устанавливают соединение с сотовой сетью (с использованием одного из стандартов: GSM, AMPS, CDMA), а за ее пределами используют спутниковый ретранслятор (рис. 5.33).

Стационарные спутниковые абонентские терминалы особенно выгодно применять в тех районах, где связь отсутствует вообще, поскольку они обеспечивают (через спутник) подключение к наземным сетям общего пользования (в том числе и телефонным — ТфОП).

Принцип организации персональной спутниковой связи достаточно прост. Если это возможно, терминал ищет наземную сотовую сеть и работает через нее, а если наземная сотовая сеть недоступна, переключается в спутниковый режим работы. Сигналы со спутников направляются на станции сопряжения, связанные с сетями общего пользования, а глобальное покрытие позволяет организовать телефонную связь между любыми населенными пунктами России. В на-

стоящее время в нашей стране персональная телефонная связь возможна только посредством трех спутниковых систем связи: Inmarsat [22, 36], Globalstar [21] и ICO (Intermediate Circular Orbit) [70], первая и последняя из которых основаны на использовании среднеорбитальных спутников, а вторая — низкоорбитальных.

### VSAT-сети

В настоящее время VSAT-сети — наиболее динамично развивающаяся категория терминалов для С<sup>3</sup>. Если в конце 1999 г. в мире было установлено более 300 тыс. приемопередающих терминалов VSAT, то к концу 2000 г. их уже стало уже около 500 тыс. Аналитики продолжают утверждать, что рынок VSAT еще далек от насыщения даже в таких развитых странах, как США, Великобритания и Япония.

Для многих крупных и средних предприятий с филиалами, разбросанными по всему миру, электронный документооборот и другие электронные формы ведения бизнеса стали необходимой потребностью. Как показывает мировой опыт, их требованиям в наибольшей степени отвечают телекоммуникационные услуги глобальных корпоративных сетей связи. Современные глобальные корпоративные сети чаще всего базируются на технологии VSAT, т. е. на использовании малогабаритных спутниковых терминалов и антенн диаметром 1,0... 2,5 м.

Этот вид сетей широко распространен во многих странах, но особенно актуальны они в России, где наземная инфраструктура связи на значительной части территории неразвита по климатическим либо геологическим причинам. Оптимальным решением для труднодоступных районов считается сочетание магистральных каналов наземной связи и выделенных систем С<sup>3</sup>. При этом наиболее рентабельными системы С<sup>3</sup> становятся там, где развертывание наземных сетей экономически нецелесообразно или просто невозможно.

Аналитики предсказывают рост индустрии VSAT по мере развития традиционных сфер ее применения — электронной торговли, банковских и биржевых операций, обеспечения телекоммуникационными услугами жителей труднодоступных районов. Они считают, что технология VSAT постепенно станет одной из господствующих в области связи.

**Услуги.** Выделенные сети на базе VSAT-терминалов способны предоставить своим удаленным пользователям широкий спектр услуг, включая высококачественную телефонную и факсимильную связь, передачу данных с различной скоростью, организацию видеоконференций и распределение телепрограмм (рис. 5.34).

VSAT-сети телефонной и факсимильной связи могут иметь любую топологию: от простейшей двухточечной до полнодоступной схемы «каждый с каждым». Выделение спутникового канала может быть

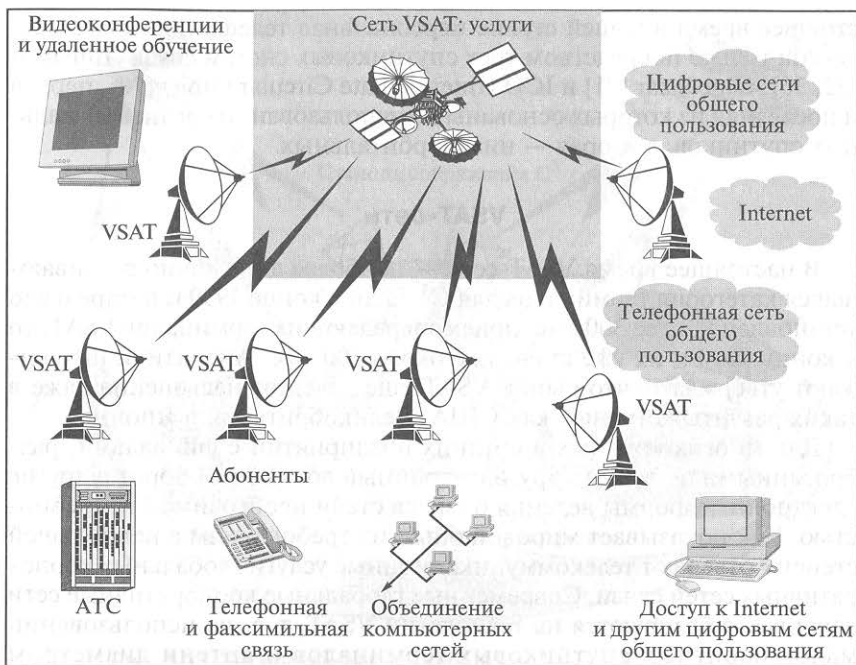


Рис. 5.34. Виды услуг, предоставляемых VSAT-системами

организовано для постоянного использования или по требованию. При создании сетей корпоративной связи (т.е. СПД предприятия) в сельской местности или при подключении удаленных станций к существующим сетям, в том числе к коммутируемой сети общего пользования (например, телефонной), данный вид услуги является приоритетным.

Современное VSAT-оборудование обеспечивает возможность подключения к наземным сетям ISDN. Типовая скорость передачи данных при таком соединении (с одним интерфейсом BRI) колеблется от 128 до 160 Кбит/с. Использование современных алгоритмов сжатия данных позволяет «упаковать» речевой канал в полосу пропускания 6,4 или 4,8 Кбит/с, благодаря чему пропускная способность спутникового канала при передаче речи повышается в 10—12 раз.

VSAT-терминалы поддерживают практически все типовые сетевые интерфейсы: RS232, RS449/422, Ethernet (IEEE 802.3), Token Ring (IEEE 802.5), и поэтому могут использоваться для объединения локальных сетей на базе наиболее популярных протоколов IP, IPX, Net-BIOS. Кроме того, применение многопротокольной среды и технологии Frame Relay (см. подразд. 5.3) позволяет создавать сети с гибкой сменой скоростей и качества услуг передачи. Например, скорость передачи в этих сетях может изменяться от 64 Кбит/с до

8,448 Мбит/с. Основными потребителями таких услуг высокоскоростной передачи данных и мультимедиа являются банки и страховые компании, средства массовой информации, государственные учреждения.

Технология VSAT допускает также создание корпоративных многоцелевых сетей с коммутацией пакетов и большим числом удаленных станций. Скорость передачи в этих сетях обычно не превышает 64 Кбит/с, а передача данных осуществляется с использованием стандартных протоколов X.25, LAP-B, HDLC. Такие сети с множеством узлов характеризуются асимметричным трафиком с лавинообразной или непредсказуемой нагрузкой. Однако VSAT-технология позволяет организовать постоянный или дополнительный канал «по требованию» и обеспечить приоритизацию трафика. В качестве примеров можно привести сети бензозаправочных станций с проверкой кредитных карточек в режиме реального времени, сети контроля за банкоматами, сети сбора и обработки телеметрической и метеорологической информации и т. п.

**Система С<sup>3</sup> «Ямал» РАО «Газпром».** В качестве примера корпоративного использования С<sup>3</sup> рассмотрим систему «Ямал» [32, 37]. В настоящее время РАО «Газпром» владеет сетью газопроводов протяженностью более 140 тыс. км, и значительная часть этих сетей расположена в местах полного отсутствия проводной наземной связи. Для обеспечения российских предприятий газовой промышленности современными видами связи и была создана спутниковая система «Ямал». С данной задачей системы С<sup>3</sup> РАО «Газпром» сопряжено решение еще одной задачи — контроля за состоянием потенциально опасных объектов.

С самого начала основные усилия разработчиков системы «Ямал» были направлены на создание собственного космического сегмента и развертывание на его базе корпоративных сетей связи для отделений «Газпрома». Земной сегмент системы «Ямал» включает в себя три типа земных станций (ЗС) (рис. 5.35), имеющих возможность наращивания числа каналов (без отключения рабочих) и оснащенных автоматическим управлением:

- узловые станции сопряжения с пропускной способностью до 8 448 Кбит/с, с мощностью передатчиков 125... 700 Вт и с антеннами диаметром 4,5... 7,0 м;

- абонентские станции VSAT, обеспечивающие скорость передачи до 2 048 Кбит/с, имеющие передатчики мощностью 2... 40 Вт и антенны диаметром 2,5... 3,7 м;

- малогабаритные возимые, стационарные и носимые станции с передатчиками мощностью до 5 Вт и с антеннами диаметром 0,6... 1,5 м, позволяющие передавать данные со скоростью до 64 Кбит/с.

Общее число наземных станций в системе «Ямал» — около 60. Ретранслятор космического аппарата (КА) обеспечивает обмен данными с ЗС, расположенными в девяти зонах, с помощью девяти лучей.

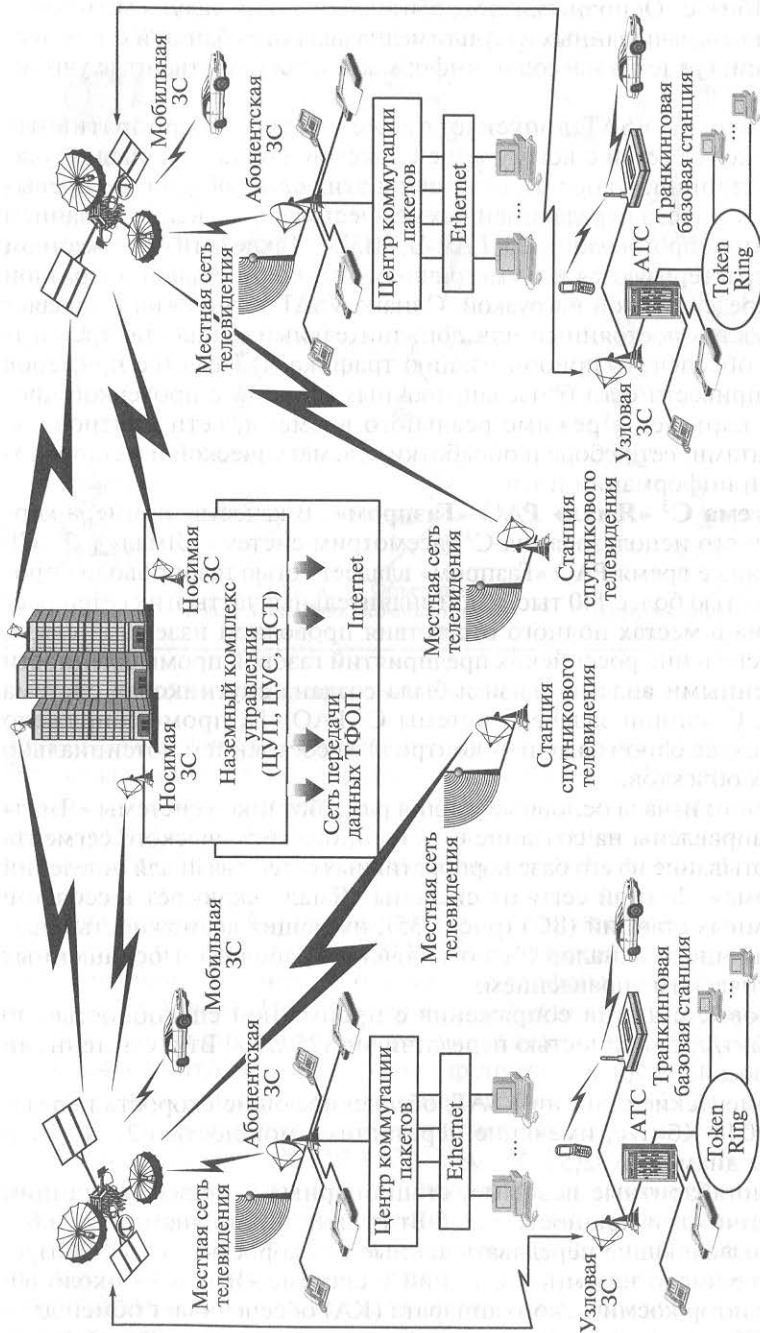


Рис. 5.35. Взаимодействие спутникового и наземного сегментов в сети «Ямал»

Переключение стволов\* транспондера с одного луча на другой производится по командам с Земли. Формирование лучей транспондера выполняется на этапе создания КА. Адаптация к возможным изменениям трафика производится в процессе эксплуатации посредством переконмутации части стволы транспондера по лучам.

Система  $S^3$  «Ямал» представляет собой СПД, объединяющую в единое информационное пространство существующие выделенные СПД предприятий газовой промышленности и сеть аварийной радиосвязи. Система передачи данных связывает вычислительные комплексы РАО «Газпром» в единую сеть (центр—регион и регион—регион), а также обеспечивает связь регионов с сетями передачи данных России и международными сетями. Используемое в системе  $S^3$  «Ямал» каналообразующее оборудование позволяет организовывать как синхронные (скорость передачи 9,6...2 048,0 Кбит/с), так и асинхронные (0,075...19,200 Кбит/с) цифровые каналы.

Описанная СПД на основе  $S^3$  обеспечивает необходимые услуги по передаче данных для разрабатываемых в ОАО «Газпром» систем экологического мониторинга, управления буровыми работами, контроля и управления электроснабжением, сбора геофизической информации.

### **5.6.7. Высокоскоростные спутниковые системы связи**

Рассмотрим перспективные проекты спутниковых систем высокоскоростной связи. Эти проекты нацелены, прежде всего, на реализацию концепции информационного общества через персональный доступ в Интернет. Согласно этой концепции каждый человек должен иметь доступ к необходимой ему информации в любой точке Земли. Большинство из этих проектов находятся еще на стадии реализации и развития. Все технические данные этих проектов собраны в табл. 5.4.

**Система спутниковой связи и передачи данных Astrolink [13]** использует девять геостационарных искусственных спутников Земли (ИСЗ), которые формируют практически глобальную зону обслуживания. Данная система предусматривает цифровую телефонную связь, передачу данных и трансляцию широкополосной видеоинформации для медицинских учреждений, правительственных организаций, транспортных и туристических компаний. Предусматриваются также организация распространения электронных версий различных изданий, дистанционное обучение, передача медицинских топографических данных и решение многих других задач, требующих передачи больших объемов информации.

Земной сегмент системы включает в себя стационарные и передвижные абонентские станции с антеннами диаметром 65, 85 и 120 см.

\* Стволы транспондера называется цифровой канал в определенном диапазоне частот.

Таблица 5.4  
**Технические данные сверхформативных спутниковых систем на основе геостационарных ИСЗ**

Характеристики	ASTROLINK	SpaceWay	Skybridge	Teledesic
Назначение	ТЛФ, ПД	ТЛФ, ПД, видеоТЛФ	ТЛФ, ПД, видеоТЛФ	ТЛФ, ПД, сверхширокополосная ПД
Зона обслуживания	Глобальная	Глобальная	Глобальная (64° ю. ш. — 64° с. ш.)	Глобальная
Год запуска первого ИСЗ	2000	2002	2001	1998
Год начала эксплуатации системы	2003	2004	2003	Нет данных
Число ИСЗ	9 (GEO)	17 (GEO)	64 (LEO)	288 (LEO)
Срок службы ИСЗ, лет	12	5	8	10
Мощность солнечных батарей, кВт	10,5	11	3	11,6
Масса ИСЗ (сухая), кг	2 185	2 000	800	800
Рабочий диапазон частот	Ка (20/30 ГГц)	Ка, Ку	Ку (14/11 ГГц)	Ка
Число стволлов транспондера	50	48 (Ка) + 24 (Ку)		
Число лучей транспондера	194	48	45	64
Пропускная способность ИСЗ, Гбит/с	9,6	4,4	1	13,3
Рабочий диапазон частот межспутниковой радиолинии, ГГц	60	60	Отсутствует	60
Пропускная способность спутника, Гбит/с	1,0	1,0		1,531
Стоимость системы, млрд долл.	4	5,1	5,1	9

Абонентские станции предусматривают систему автоматического поддержания уровня излучаемой мощности и рассчитаны на работу в ISDN-сетях и сетях, использующих технологию АТМ. Абонентские станции для крупных пользователей обеспечивают те же возможности, но диаметры их антенн составляют 1,2...2,4 м, и обеспечивают возможность коллективного доступа к ресурсам системы. Центральные региональные станции имеют выход в наземные телефонные сети общего пользования (диаметр их антенны 2,4 м).

**Межрегиональная система спутниковой связи и передачи данных Spaceway** предназначена для организации международных видеотелефонных сетей и высокоинформативных сетей передачи данных в глобальном масштабе [13, 57].

Космический сегмент по проекту данной системы предусматривает использование 17 геостационарных спутников. Все спутники связаны между собой межспутниковыми линиями. Многолучевые антенны спутников создают следующие региональные рабочие зоны:

- регион 1 — Северная Америка;
- регион 2 — Центральная Америка, Южная Америка;
- регион 3 — Африка, Средний Восток, Европа;
- регион 4 — Австралия, Океания, Дальний Восток.

Каждый регион обслуживают четыре спутника, образующие кластер в соответствующей точке геостационарной орбиты. Один спутник (175° в.д.) выделен для обеспечения трафика между США и Азиатско-Тихоокеанским регионом. Рабочие зоны формируются многолучевыми антеннами. Каждый из 48 лучей поддерживает передачу цифрового потока со скоростью 92 Мбит/с. На Земле используются различные типы абонентских станций VSAT с антенной диаметром 66 см и передатчиками примерно 2 Вт. Параллельно рассматривается концепция создания дополнительной космической группировки на основе среднеорбитальных ИСЗ при сокращении числа геостационарных ИСЗ.

**Система C<sup>3</sup> Skybridge** [9] предусматривает интеграцию наземных СПД (включая сотовые) и предоставляет следующие виды услуг:

- работа в сети Интернет в режимах обмена и доступа к электронным базам данных;
- оплата покупок, рекламируемых в телевизионных программах;
- дистанционное обучение, проведение видеоконференций, пересылка файлов, электронная почта;
- видеотелефонная связь;
- развлекательные телевизионные программы по заказу абонента, интерактивные компьютерные игры;
- передача информации медицинской диагностики, дистанционные медицинские консультации.

Предусматривается практически глобальная зона обслуживания, ограниченная 68° ю.ш. и 68° с.ш. Космический сегмент состоит из

64 спутников, расположенных на круговых орбитах с высотой 1 475 км, которые разбиты на две подгруппы. В каждой подгруппе по 32 спутника, расположенных по четыре в каждой из восьми орбитальных плоскостей. Столь сложное построение орбитальной группировки связано с оптимизацией системы Skybridge по критерию совместимости работы с геостационарными системами в диапазоне частот 10...18 ГГц при условии наилучшего обслуживания малонаселенных регионов Земли.

В рассматриваемой системе применяется многостанционный доступ CDMA/TDMA. Канальная скорость передачи данных на линии ИСЗ—Земля составляет 41,5 Мбит/с, а на линии Земля—ИСЗ—5,2 Мбит/с. Рабочая полоса частот передающего канала составляет 22,6 МГц на линии ИСЗ—Земля и 2,93 МГц—на линии Земля—ИСЗ.

**Система С<sup>3</sup> Teledesic** принципиально отличается от других систем спутниковой связи и по назначению, и по предполагаемым техническим решениям. В первую очередь, она предназначалась для обеспечения не только фиксированных, но и подвижных абонентов высококачественной телефонной связью, а также других служб, нуждающихся в обмене широкополосной информацией в глобальном масштабе. По своей потенциальной пропускной способности система сравнима с волоконнооптической линией и в проекте рассчитана на их совместную эксплуатацию в магистральных линиях связи.

Основные идейные создатели данной системы—фирма McCaw Cellular Communications, специализирующаяся на проводных сетях связи, и фирма Microsoft. Проектные работы были начаты в 1990 г. Первоначально предполагалось, что с 2001 г. начнется коммерческая эксплуатация системы, однако ее начало было перенесено на 2003 г. (запуск первого экспериментального ИСЗ произведен 27 февраля 1998 г.). Из-за банкротства Iridium строительство Teledesic в 2002 г. было заморожено. Однако как бы ни сложилась ситуация с Teledesic в дальнейшем, не стоит недооценивать перспективность некоторых идей, положенных в основу этого проекта. Поэтому мы решили дать материал, раскрывающий некоторые его технические детали.

Космический сегмент системы планировался в виде группировки из 288 ИСЗ, расположенных на круговых орбитах высотой 1 375 км в 12 плоскостях с наклоном 98,142°...98,182°. На каждой орбите планировалось иметь 24 спутника. Пространственное разнесение орбит в плоскости экватора составляло примерно 18°.

Для обеспечения глобальной зоны обслуживания в системе Teledesic предусматриваются межспутниковые радиолинии. Общая зона обслуживания разбита на 20 000 локальных зон. Каждая локальная зона включает в себя девять парциальных зон (ячеек) размером 53,3 × 53,3 км. Каждый из ИСЗ создает рабочую область, включающую в себя 64 локальные зоны (диаметром 1 400 км, по 576 ячеек в каждой зоне).

При движении ИСЗ вдоль орбиты изменяется пространственная ориентация 64 лучей антенной системы, обеспечивая стационарность расположения ячеек. За каждой ячейкой закреплен определенный заранее ресурс пропускной способности ИСЗ. В результате можно достаточно точно описать границы обслуживаемых территорий, достоверно учесть плотность распределения потребителей и соответственно рационально использовать пропускную способность каждого ИСЗ. Межспутниковые радиолинии работают в диапазоне частот 60 ГГц, что обеспечивает помехозащищенность системы. Максимальная дальность межспутниковой радиолинии — 2 586 км, пропускная способность — 1,531 Гбит/с.

Земной сегмент системы состоит из различных терминалов. Для фиксированных абонентов предусматриваются терминалы с антеннами диаметром 0,16...1,80 м, а для мобильных — диаметром 0,08 м. Мощность передающих устройств 0,01...4,70 Вт. Скорость передачи в зависимости от типа терминала и его комплектации составляет от 16 Кбит/с до 2,048 Мбит/с. Для организации высокоскоростных линий связи используются терминалы с антеннами диаметром от 0,28 до 1,60 м при мощности передатчиков от 1 до 49 Вт в зависимости от требуемой скорости потока, которая составляет от 155,5 Мбит/с до 1,24416 Гбит/с.

Каждый ИСЗ может поддерживать работу 16 высокоскоростных терминалов, находящихся в его рабочей зоне. Внутри отдельной ячейки предусмотрена возможность организации сетей с пропускной способностью 1 400 каналов по 16 Кбит/с или 15 каналов по 1,544 Мбит/с (возможна эквивалентная комбинация каналов). Между центральными станциями системы и специальными государственными пользователями предусматривается возможность организации сверхскоростных каналов от 155 Мбит/с до 2 Гбит/с.

### **5.6.8. Характерные особенности современных спутниковых систем связи**

Анализ технических параметров перспективных спутниковых систем связи (см. табл. 5.4) позволяет выявить общие характерные особенности их технической реализации.

Практически все заявленные спутниковые системы работают или будут работать в Ка-диапазоне частот (20/30 ГГц). Многочисленные эксперименты и начало внедрения этого диапазона в практику к настоящему времени уже проведены.

Другой существенной особенностью является наличие межспутниковых радиолиний как для систем, основанных на низкоорбитальных ИСЗ, так и на геостационарных. Причем во всех без исключения случаях используется диапазон частот 60 ГГц. Интересно, что, несмотря на активное предложение использовать в межспутниковых радиолиниях оптический диапазон частот, при переходе к практиче-

ской реализации предпочтение было отдано диапазону 60 ГГц. Применение межспутниковых линий связи открывает интересную возможность коммутации потоков данных между спутниковыми группировками на разных орбитах. Действительно, несложно представить себе ситуацию, когда вместо того чтобы передавать пакет данных от ЛЕО-спутника к ЛЕО-спутнику было бы выгодно «перебросить» этот пакет на GEO- или МЕО-спутник, с которого затем «сбросить» его на ближайший в этот момент к получателю ЛЕО-спутник.

Новым техническим решением, которое предусмотрено во всех системах, является использование на GEO-спутниках антенн с десятками лучей. Как правило, лучи имеют ширину диаграммы направленности (ДН)  $1 \dots 2^\circ$  и обеспечивают «плотное» покрытие рабочей зоны. Для каждого луча выделен свой частотный ствол (стволы) ретранслятора. Смежные лучи развязаны по частоте, а несмежные лучи с совпадающими частотами должным образом поляризованы.

Для реализации антенных систем ЛЕО-спутников также предусматривается многолучевая технология, но она имеет принципиально отличную от используемой на геостационарных ИСЗ основу — фазированные антенные решетки. Такая антенна представляет собой решетку из отдельных антенн, диаграмму направленности каждой из которых можно формировать и управлять независимо с помощью компьютера.

Ретрансляционная аппаратура перспективных ИСЗ, как правило, предполагает коммутацию каналов, обеспечивающую полносвязность системы (связь «каждый с каждым»). При этом разделение каналов обычно осуществляется традиционным способом: на линии Земля—ИСЗ используется режим FDMA, а на линии ИСЗ—Земля — режим TDMA (либо модификации этого режима в сочетании с CDMA). Представленные системы принципиально отличаются от существующих в настоящее время как по пропускной способности, так и по экономической эффективности.

По-видимому в ближайшие несколько лет будут заявлены и новые сверхинформативные спутниковые системы. Уже сегодня активно идет процесс их системной интеграции (например, системное объединение космических группировок геостационарных, среднеорбитальных и низкоорбитальных ИСЗ).

Начало эксплуатации сверхинформативных систем позволит предоставить абонентам принципиально новые услуги связи, например видеотелефонную связь, формирование пакета телевизионных программ по заказу абонента и многое другое. Из этого конечно же не следует, что в XXI в. не будут развиваться глобальные, континентальные и национальные спутниковые системы, действующие в настоящее время. Однако уже в начале XXI в. постепенное насыщение рынка телекоммуникаций приводит к необходимости пересмотра их организационной структуры, стратегических планов развития и взаимной технической и коммерческой координации в целях оптималь-

ного участия в формировании и создании единого мирового информационного пространства.

Уже сейчас идет работа над Межпланетарным Интернетом [56]. В мае 2009 г. на международной космической станции успешно прошли испытания нового стека протоколов, реализующего технологию сетей, адаптирующихся к задержкам — DTN (Delay Tolerant Networking). DTN-протоколы позволяют распространить наземный Интернет в космос. Они решают целый ряд серьезных проблем, например уменьшают большую задержку пакета при его перемещении по космическим каналам связи, изменчивость этой задержки вследствие изменения взаимного расположения узлов космической сети на орбитах и неравномерность сетевого трафика и высокого уровня помех в канале вследствие солнечной радиации.

По-видимому в недалеком будущем развитие средств связи в целом приведет к иной форме восприятия мира и новому этапу развития цивилизации.

## СПИСОК ЛИТЕРАТУРЫ

1. Блейхут Р. Теория и практика кодов, контролирующих ошибки / Р. Блейхут. — М.: Мир, 1986. — 576 с.
2. Бобровский С. Изобретатель компьютера. — [Электронный ресурс]. — Режим доступа: [www.COMPUTER-MUSEUM.ru/galglory/2.htm](http://www.COMPUTER-MUSEUM.ru/galglory/2.htm)
3. Вютрих Х.А. Виртуализация как возможный путь развития управления / Х.А. Вютрих, А.Ф. Филипп // Проблемы теории и практики управления. — 1999. — № 5.
4. Гордиевский О. КГБ. История внешнеполитических операций от Ленина до Горбачева / О. Гордиевский, К. Эндрю. — М.: Nota Bene, 1992. — 352 с.
5. Городская вычислительная сеть. Википедия. — [Электронный ресурс]. — Режим доступа: [http://ru.wikipedia.org/wiki/Городская\\_сеть](http://ru.wikipedia.org/wiki/Городская_сеть).
6. ГОСТ Р 1.0—92. Государственная система стандартизации Российской Федерации. Основные положения. — М.: Госстандарт России: Изд-во стандартов, 1993.
7. Громов Г.Р. От гиперкниги к гипермозгу: информационные технологии эпохи Интернета: эссе, диалоги, очерки / Г.Р. Громов. — М.: Радио и связь, 2004. — 204 с.
8. Дайджест катастроф. — [Электронный ресурс]. — Электронный журнал. — Режим доступа: <http://catless.ncl.ac.uk/Risks>
9. Дорнан Э. Последние пятьсот миль / Э. Дорнан // Журнал сетевых решений LAN. — 2001. — № 5.
10. Заболотнов И. Как это работает: xDSL / И. Заболотнов // Независимый обзор провайдеров. — [Электронный ресурс]. — 2007. — Июль. — Режим доступа: <http://www.provider.net.ru/library.php?article=1132>
11. Закон Мура. Википедия. — [Электронный ресурс]. — Режим доступа: [http://ru.wikipedia.org/wiki/Закон\\_Мура](http://ru.wikipedia.org/wiki/Закон_Мура)
12. Клейнрок Л. Теория массового обслуживания / Л. Клейнрок. — М.: Машиностроение, 1979. — 432 с.
13. Колюбякин В.С. Спутниковые широкополосные мультимедийные проекты / В.С. Колюбякин // Телемультимедия. — [Электронный ресурс]. — 2000. — 01 февр. — Режим доступа: <http://www.telemultimedia.ru/art.php?id=25&rid=14>
14. Конрад Цузе. Википедия. — [Электронный ресурс]. — Режим доступа: [www.ru.wikipedia.org/wiki/Конрад\\_Цузе](http://www.ru.wikipedia.org/wiki/Конрад_Цузе)
15. Лынов С. Интернет как наркотик для человека и человечества / С. Лынов // Практическая психология. — [Электронный ресурс]. — Режим доступа: <http://www.sunhome.ru/psychology/11769>

16. *Мак-Вильямс Ф. Дж.* Теория кодов, исправляющих ошибки / Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн. — М.: Радио и связь, 1979. — 744 с.
17. *Малиновский Б. Н.* Из мировой истории цифровой вычислительной техники / Б. Н. Малиновский // Виртуальный компьютерный музей. — [Электронный ресурс]. — Режим доступа: <http://www.computer-museum.ru/frgnhist/malinovs.htm>
18. Метрология, сертификация, стандартизация. — [Электронный ресурс]. — Режим доступа: <http://sapr.mgsu.ru/biblio/metrolog/main.files/right.html>
19. *Морелос-Сарагоса Р.* Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение / Р. Морелос-Сарагоса. — М.: Техносфера, 2005. — 320 с.
20. *Новичков А. Н.* Одна частная история Ethernet / А. Н. Новичков // Сети и система связи. — 2008. — № 3. — С. 14—16.
21. О системе Globalstar. — [Электронный ресурс]. — Режим доступа: <http://www.globalstar.ru/>
22. О системе Inmarsat. — [Электронный ресурс]. — Режим доступа: <http://www.inmarsat.ru/>
23. Обнаружение и исправление ошибок. Википедия. — [Электронный ресурс]. — Режим доступа: [http://ru.wikipedia.org/wiki/Коррекция\\_ошибок](http://ru.wikipedia.org/wiki/Коррекция_ошибок)
24. Оптический компьютер из замороженного света. — [Электронный ресурс]. — Режим доступа: [www.3dnews.ru/news/opticheskiy\\_komputer\\_iz\\_zamorozhennogo\\_sveta](http://www.3dnews.ru/news/opticheskiy_komputer_iz_zamorozhennogo_sveta)
25. Оптический компьютер. Википедия. — [Электронный ресурс]. — Режим доступа: [www.wikipedia.org/wiki/Оптический\\_компьютер](http://www.wikipedia.org/wiki/Оптический_компьютер)
26. Основы организации и технологии стандартизации. — [Электронный ресурс]. — Режим доступа: <http://sapr.mgsu.ru/biblio/metrolog/main.files/text3.files/2.2.html>
27. Основы организации и технологии стандартизации. — [Электронный ресурс]. — Режим доступа: <http://sapr.mgsu.ru/biblio/metrolog/main.files/text3.files/1.1.html>
28. *Парамонов В.* Вычислительному комплексу ENIAC 60 лет / Парамонов В. — [Электронный ресурс]. — Режим доступа: <http://hard.compulenta.ru/252780/>
29. *Патюрель Р.* Создание сетевых организационных структур / Р. Патюрель // Проблемы теории и практики управления. — 1997. — № 3. — С. 76—81.
30. *Питерсон У.* Коды, исправляющие ошибки / У. Питерсон. — М.: Мир, 1964. — 340 с.
31. *Питерсон У.* Коды / У. Питерсон, Э. Уэлдон. — М.: Мир, 1976. — 595 с.
32. *Севастьянов Д. Н.* Космическая информационная система «Ямал»: Новые возможности / Д. Н. Севастьянов // Газовая промышленность. — 2006. — № 9. — С. 39—41.
33. *Семенов Ю. А.* Сети FDDI / Ю. А. Семенов. — [Электронный ресурс]. — Режим доступа: [http://www.citforum.ru/nets/semenov/4/41/fddi\\_416.shtml](http://www.citforum.ru/nets/semenov/4/41/fddi_416.shtml)
34. Сервис-ориентированная архитектура. Википедия. — [Электронный ресурс]. — Режим доступа: <http://ru.wikipedia.org/wiki>
35. Сетевой этикет. — [Электронный ресурс]. — Режим доступа: <http://netiquette.narod.ru>

36. Система Inmarsat. — [Электронный ресурс]. — Режим доступа: <http://www.connect.ru/article.asp?id=5088>
37. Система спутниковой связи «Ямал». Каталог продукции. — [Электронный ресурс]. — Режим доступа: <http://www.gazprom.ru/child/gzcom00.shtml#s03>
38. Сухомлин В.А. Введение в анализ информационных технологий / В.А. Сухомлин. — М.: Горячая линия — Телеком, 2003. — 457 с.
39. Тарасов В. Причины возникновения и особенности организации предприятия нового типа / В.Тарасов // Проблемы теории и практики управления. — 1998. — № 1. — С. 87—90.
40. Тенненбаум Э.С. Компьютерные сети / Э.С.Тенненбаум. — СПб.: Питер, 2007. — 992 с.
41. Технология Jini — [Электронный ресурс]. — Режим доступа: <http://ru.sun.com/java/jini/tech.htm>
42. Тоффлер Э. Третья волна / Э.Тоффлер. — М.: АСТ, 2002. — 781 с.
43. Тоффлер Э. Шок будущего / Э.Тоффлер. — М.: АСТ, 2003. — 557 с.
44. Уоррен Г.С. Алгоритмические трюки для программистов / Г.С.Уоррен. — М.: Вильямс, 2007. — 288 с.
45. Уэстерман Дж. Сервис-ориентированная архитектура сегодня: введение в SOA / Дж.Уэстерман. — [Электронный ресурс]. — Режим доступа: <http://www.citforum.ru/internet/webservice/soa/>
46. Ферми Л. Атомы у нас дома / Л.Ферми. — М.: Иностранная литература, 1959. — 328 с.
47. Флоренский Ю. Первая ЭВМ была уничтожена по приказу Черчилля / Ю.Флоренский // Наука и жизнь. — [Электронный ресурс]. — Электрон. журн. — Режим доступа: <http://nauka.relis.ru/06/9710/06710034.htm>
48. Хантингтон С. Столкновение цивилизаций / С.Хантингтон; пер. с англ. — М.: ООО «Изд-во АСТ», 2003. — 603 с.
49. Черняк Е.Б. Пять столетий тайной войны. Из истории секретной дипломатии и разведки / Е.Б.Черняк. — М.: Международные отношения, 1991. — 376 с.
50. Черняк Л. Дойти до линии горизонта / Е.Б.Черняк. — [Электронный ресурс]. — Режим доступа: [www.osp.ru/cw/2006142/3488076](http://www.osp.ru/cw/2006142/3488076)
51. Шафер Э. Жулничество в Интернете / Э.Шафер. — [Электронный ресурс]. — Режим доступа: [http://www.masternewmedia.org/ru/internet\\_fraud/internet\\_deception\\_research/internet\\_fraud\\_phishing\\_pharming\\_research\\_study\\_20051001.htm](http://www.masternewmedia.org/ru/internet_fraud/internet_deception_research/internet_fraud_phishing_pharming_research_study_20051001.htm)
52. Шильников Е. GEO, НЕО, МЕО и LEO / Е.Шильников // Компьютеры. — 1999. — № 42.
53. Электросвязь. — 1997. — № 11. — С. 13.
54. Элементы оптических компьютеров будут выращивать в бактериях. — [Электронный ресурс]. — Режим доступа: [www.membrana.ru/lenta/?4120/](http://www.membrana.ru/lenta/?4120/)
55. Юнг Р. Ярче тысячи солнц / Р.Юнг. — М.: Госатомиздат, 1961. — 280 с.
56. Ackerman E. Interplanetary Internet Tested / E.Ackerman // IEEE Spectrum. — V. 46. — №. 7. — P. 9—10.
57. Bandwidth-on-Demand. — [Electronic resource]. — Mode access: <http://www.boeing.com/defense-space/space/bss/factsheets/702/spaceway/spaceway.htm.1>

58. *Batcher K. E.* Sorting Networks and Their Applications / K. E. Batcher // AFIPS Spring Joint Computer Conf. — 1968. — V.32. — P. 307—315.
59. Bertsekas D. Gallager R. Data networks. Prentice Hall, 1992.
60. Bluetooth. Википедия. — [Электронный ресурс]. — Режим доступа: [http://en.wikipedia.org/wiki/Bluetooth#Bluetooth\\_profiles](http://en.wikipedia.org/wiki/Bluetooth#Bluetooth_profiles)
61. *Cioffi J. M.* Asymmetric Digital Subscriber Line / J. M. Cioffi // The Communication Handbook. Ed. CRC Press. — 1997. — P. 450—479.
62. *Clos C.* A Study of Non-Blocking Switching Networks / C. Clos // Bell System Tech. — 1956. — J. V.32. — P. 406—424.
63. Colossus computer. Википедия. — [Электронный ресурс]. — Режим доступа: [http://en.wikipedia.org/wiki/Colossus\\_computer](http://en.wikipedia.org/wiki/Colossus_computer)
64. *Davidow W. H.* The Virtual Corporation: Structuring and Revitalising Corporation for The 21 century / W. H. Davidow, M. S. Malone. — New York: HarpereCollins, 1992. — 287 p.
65. *Delpart M.* Second Generation Systems / M. Delpart, V. Kumar // The Communication Handbook. Ed. CRC Press, 1997. — P. 1208—1223.
66. *Faucheux C.* How virtual organizing is transforming management science / C. Faucheux // Association for Computing Machinery. Communications of the ACM. — 1997. — V. 40. — № 69.
67. *Gilder G.* Microcosm: The Quantum Revolution in Economics and Technology / G. Gilder. — New York: Touchstone, 1990. — 426 p.
68. *Hamel G.* Leading the Revolution / G. Hamel. — Boston: HBS Press, 2002. — P. 358.
69. *Hanzo L.* The Pan-European Cellular System / L. Hanzo // The Communication Handbook. Ed. CRC Press, 1997. — P. 1226—1247.
70. ICO Global Communications. — [Electronic resource]. — Mode access: <http://www.ico.com/>
71. *Jain R.* Location Strategies for Personal Communications Services / R. Jain, Lin Yi-Bing, S. Mohan // The Communication Handbook. Ed. CRC Press. — 1997. — P. 1116—1147.
72. *Karol M. J.* Input versus Output Queuing on a Spaiice-Division Packet Switch / M. J. Karol, M. J. Hluchyj, S. P. Morgan // IEEE Trans on Comm, 1987. — V. 35. — P. 1347—1356.
73. *Maral G.* Satellite Communications Systems: Systems, Techniques and Technology / G. Maral. 4th Edition. Wiley. — 2002. — 784 p.
74. *Mowshowitz A.* Virtual organization / A. Mowshowitz // Association for Computing Machinery. Communications of the ACM. — 1997. — V. 40. — № 9.
75. *Paulson E.* Inside Cisco / E. Paulson. — San Francisco: John Wiley & Sous, 2001. — 312 p.
76. *Roberts L. G.* ALOHA packet system with and without slots and capture / L. G. Roberts // Computer Communication Review. — 1972. — V. 5. — № 2. — P. 28—42.
77. *Ross A.* CDMA Technology / A. Ross, K. Gilhousen // The Communication Handbook. Ed. CRC Press. — 1997. — P. 1257—1276.
78. *Singh S.* The CODE BOOK / S. Singh. — London: 4th Estate, 2000. — 402 p.
79. *Waters J. K.* Chambers and the Cisco Way: Navigating through Volatilidy / J. K. Waters. — San Francisco: John Wiley & Sous, 2002.

## ОГЛАВЛЕНИЕ

Предисловие.....	3
<b>Глава 1. Введение в предмет.....</b>	<b>6</b>
1.1. Шок будущего.....	6
1.2. Предпосылки появления сетей ЭВМ и развития информационных технологий.....	6
1.2.1. Появление технически сложных систем.....	6
1.2.2. Повышение эффективности управления.....	8
1.3. Три движущие силы информационных технологий.....	10
1.3.1. Некоторые факты из истории компьютеров.....	10
1.3.2. Микроэлектроника и закон Мура.....	11
1.3.3. Компьютеры на основе микропроцессоров.....	12
1.3.4. Телекоммуникации и закон Гилдера.....	13
1.4. Кто, как и для чего использует сеть Интернет.....	15
1.4.1. Общие сведения.....	15
1.4.2. Интранет.....	16
1.4.3. Взаимодействие с другими предприятиями.....	17
1.4.4. Виртуальные предприятия.....	18
1.4.5. Взаимодействие с конечным потребителем.....	20
1.4.6. Электронное правительство.....	20
1.4.7. Использование Сети в индивидуальных целях.....	22
1.5. Сетевая этика.....	23
1.6. Инженерия программного обеспечения.....	24
1.7. Сервис-ориентированные архитектуры web-сервисы.....	27
<b>Глава 2. Основные понятия, модели и примеры компьютерных сетей.....</b>	<b>30</b>
2.1. Организация компьютерных сетей.....	30
2.1.1. Общие сведения.....	30
2.1.2. Системы передачи данных.....	31
2.1.3. Сопряжение транспортных сред.....	36
2.2. Классификация сетей ЭВМ.....	36
2.3. Сетевое программное обеспечение.....	38
2.3.1. Иерархия протоколов.....	38
2.3.2. Основные понятия.....	39
2.3.3. Интерфейсы и сервис.....	40
2.3.4. Примитивы сервиса.....	41
2.3.5. Сервисы с соединением и без соединения.....	43
2.3.6. Основные вопросы организации уровней.....	45
2.4. Модель системы передачи данных.....	46
2.4.1. Общие сведения.....	46
2.4.2. Физический уровень.....	47
2.4.3. Канальный уровень.....	48

2.4.4. Сетевой уровень .....	49
2.5. Примеры СПД.....	50
2.5.1. СПД на основе стандарта Bluetooth .....	50
2.5.2. СПД на основе стандарта X.25 .....	51
2.5.3. СПД на основе Frame Relay.....	52
2.5.4. Универсальные СПД и асинхронный способ передачи.....	52
2.5.5. Сравнение различных СПД.....	53
2.6. Стандартизация .....	54
2.6.1. Стандарты .....	54
2.6.2. Кто и как вводит стандарты.....	54
2.6.3. Международная организация по стандартизации.....	55
2.6.4. Международная электротехническая комиссия .....	56
2.6.5. Международный союз электросвязи.....	57
2.6.6. Региональные межправительственные организации по стандартизации.....	58
2.6.7. Промышленные консорциумы и профессиональные ассоциации .....	60
2.6.8. Национальные организации по стандартизации .....	61
<b>Глава 3. Физический уровень .....</b>	<b>63</b>
3.1. Теоретические основы передачи данных .....	63
3.1.1. Общие сведения .....	63
3.1.2. Разные формы представления сигнала .....	64
3.1.3. Сигналы, данные, передача.....	65
3.1.4. Взаимосвязь пропускной способности канала и его полосы пропускания .....	68
3.1.5. Сигналы с ограниченной полосой пропускания .....	69
3.2. Представление данных на физическом уровне .....	69
3.2.1. Общие сведения.....	69
3.2.2. Цифровые данные — цифровой сигнал.....	71
3.2.3. Цифровые данные — аналоговый сигнал .....	76
3.2.4. Аналоговые данные — цифровой сигнал .....	79
3.2.5. Аналоговые данные — аналоговый сигнал .....	82
3.3. Физические среды для передачи данных.....	84
3.3.1. Магнитные носители .....	84
3.3.2. Витая пара.....	85
3.3.3. Коаксиальные кабели.....	86
3.3.4. Оптоволокно.....	87
3.3.5. Физический уровень в сетях IEEE 802.3.....	91
3.4. Беспроводная связь.....	101
3.4.1. Общие сведения.....	101
3.4.2. Электромагнитный спектр .....	102
3.4.3. Радиопередача .....	105
3.4.4. Микроволновая передача .....	106
3.4.5. Инфракрасные и миллиметровые волны .....	107
3.4.6. Видимое излучение .....	107
3.4.7. Стандарт беспроводных локальных сетей IEEE 802.11 .....	107
<b>Глава 4. Канальный уровень.....</b>	<b>111</b>
4.1. Основы передачи данных на канальном уровне.....	111
4.1.1. Сервис, предоставляемый сетевому уровню .....	111
4.1.2. Разбиение на кадры.....	113

4.1.3.	Сохранение последовательности кадров.....	115
4.1.4.	Управление потоком.....	116
4.1.5.	Обнаружение и исправление ошибок.....	116
4.1.6.	Коды с исправлением ошибок.....	117
4.1.7.	Коды с обнаружением ошибок.....	119
4.2.	Протоколы для каналов типа точка—точка.....	122
4.2.1.	Простейшие протоколы канала данных.....	122
4.2.2.	Симплекс-протокол без ограничений.....	124
4.2.3.	Симплексный старт-стопный протокол.....	125
4.2.4.	Симплексный протокол для канала с шумом.....	126
4.2.5.	Протоколы скользящего окна.....	129
4.2.6.	Протокол с возвратом на <i>n</i> кадров и протокол с выборочным повтором.....	133
4.2.7.	Протокол HDLC.....	134
4.2.8.	Протокол типа точка—точка—PPP.....	136
4.3.	Протоколы множественного доступа.....	139
4.3.1.	Общие сведения.....	139
4.3.2.	Статические методы доступа к каналу.....	139
4.3.3.	Базовая модель динамического предоставления доступа к каналу.....	141
4.3.4.	Методы множественного доступа ALOHA.....	142
4.3.5.	Протоколы множественного доступа с обнаружением несущей.....	146
4.3.6.	Бесконфликтные протоколы.....	148
4.3.7.	Протоколы с ограниченным числом конфликтов.....	150
4.3.8.	Множественный доступ к беспроводным каналам.....	153
4.4.	Канальный уровень стандарта IEEE 802 для локальных и муниципальных сетей.....	157
4.4.1.	Стандарт IEEE 802.3 и Ethernet.....	157
4.4.2.	Канальный уровень в сетях IEEE 802.11.....	162
4.5.	Стандарт IEEE 802.2: управление логическим каналом.....	164
4.5.1.	Общие сведения.....	164
4.5.2.	Три типа процедур уровня LLC.....	164
4.5.3.	Структура кадров LLC. Процедура с восстановлением кадров LLC2.....	165
4.6.	Мосты в ЛВС.....	169
4.6.1.	Общие сведения.....	169
4.6.2.	Мосты СПД IEEE 802.x в СПД IEEE 802.x.....	171
4.6.3.	Прозрачные мосты.....	172
4.6.4.	Мосты с маршрутизацией от источника.....	175
4.6.5.	Сравнение мостов для СПД IEEE 802.3.....	176
4.7.	Сетевые коммутаторы.....	178
4.7.1.	Общие сведения.....	178
4.7.2.	Функционирование сетевого коммутатора.....	179
4.7.3.	Структурирование трафика.....	179
4.7.4.	Сравнение коммутаторов и мостов.....	180
4.8.	Виртуальные сети.....	180
4.8.1.	Понятие виртуальной сети.....	180
4.8.2.	Типы виртуальных сетей.....	181
<b>Глава 5.</b>	<b>Примеры систем передачи данных.....</b>	<b>188</b>
5.1.	Телефонные сети.....	188
5.1.1.	Общие сведения.....	188

5.1.2. Немного истории.....	188
5.1.3. Структура телефонной сети.....	190
5.1.4. Абонентская линия.....	193
5.1.5. Технологии семейства xDSL.....	197
5.1.6. Магистралы и мультиплексирование.....	200
5.1.7. Коммутация.....	208
5.2. Системы FDDI.....	212
5.2.1. Основы технологии FDDI.....	212
5.2.2. Протоколы технологии FDDI.....	214
5.2.3. Типы узлов и правила их соединения.....	215
5.2.4. Функции MAC-подуровня.....	215
5.3. СПД Frame Relay.....	223
5.3.1. Общие сведения.....	223
5.3.2. Архитектура Frame Relay.....	224
5.3.3. Канальный уровень FR.....	225
5.3.4. Управление качеством сервиса.....	229
5.3.5. Управление доступом.....	232
5.3.6. Использование СПД Frame Relay.....	233
5.4. Цифровые сети с интегрированным сервисом.....	235
5.4.1. Общие сведения.....	235
5.4.2. Принципы организации СПД ISDN.....	236
5.4.3. Архитектура СПД ISDN.....	237
5.4.4. Подключение оборудования пользователей.....	239
5.4.5. Адресация в СПД ISDN.....	240
5.4.6. Стек протоколов в СПД N-ISDN.....	242
5.4.7. Высокоскоростные ISDN-сети и ATM-сети.....	243
5.4.8. Виртуальные каналы в сравнении с коммутируемыми каналами.....	244
5.4.9. Передача в ATM-сетях.....	244
5.5. Сотовая связь.....	255
5.5.1. Сотовые и радиотелефоны.....	255
5.5.2. СПД на основе WiMAX.....	265
5.6. Спутниковая связь.....	268
5.6.1. Общие сведения.....	268
5.6.2. Геостационарные спутники.....	269
5.6.3. Спутники с высокоэллиптической орбитой.....	270
5.6.4. Среднеорбитальные и низкоорбитальные спутники.....	271
5.6.5. Канальный уровень в спутниковых сетях.....	273
5.6.6. Основные категории СПД на базе C <sup>3</sup> .....	277
5.6.7. Высокоскоростные спутниковые системы связи.....	283
5.6.8. Характерные особенности современных спутниковых систем связи.....	287
Список литературы.....	290

*Учебное издание*

**Смелянский Руслан Леонидович**

## **КОМПЬЮТЕРНЫЕ СЕТИ**

**Том 1**

**Системы передачи данных**

**Учебник**

Редактор *В. Н. Махова*

Технический редактор *Е. Ф. Коржуева*

Компьютерная верстка: *Л. А. Смирнова*

Корректоры *А. П. Сизова, О. И. Лыкова*

Изд. № 101112604. Подписано в печать 27.10.2010. Формат 60×90/16.  
Гарнитура «Ньютон». Бумага офсетная. Печать офсетная. Усл. печ. л. 19,0.  
Тираж 2 000 экз. Заказ № 30832.

Издательский центр «Академия». [www.academia-moscow.ru](http://www.academia-moscow.ru)  
125252, Москва, ул. Зорге, д. 15, корп. 1, пом. 26б.

Адрес для корреспонденции: 129085, Москва, пр-т Мира, 101В, стр. 1, а/я 48.  
Тел./факс: (495) 648-0507, 616-0029.

Санитарно-эпидемиологическое заключение № 77.99.60.953.Д.007831.07.09 от 06.07.2009.

Отпечатано в соответствии с качеством предоставленных издательством  
электронных носителей в ОАО «Саратовский полиграфкомбинат».  
410004, г. Саратов, ул. Чернышевского, 59. [www.sarpk.ru](http://www.sarpk.ru)