ИНТЕРНЕТ УНИВЕРСИТЕТ
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

# Основы локальных сетей

**Курс лекций. Учебное пособие**

**Ю.В. Новиков, С.В. Кондратенко**

**Рекомендовано для студентов высших учебных заведений, обучающихся по специальностям в области информационных технологий**

**Серия «Основы информационных технологий»**

**Книга издана при финансовой поддержке компании РМ ТЕЛЕКОМ**

**РМ Телеком®**

**Интернет-Университет Информационных Технологий**
**www.intuit.ru**
**Москва, 2005**

УДК 004.43(075.8)
Н-73
ББК 32.973.202я73-2

Н-73 Основы локальных сетей: курс лекций: учеб. пособие : для студентов вузов, обучающихся по специальностям в обл. информ. технологий / Ю. В. Новиков, С. В. Кондратенко. — М. : Интернет — Ун-т Информ. Технологий, 2005. - 360 с. — (Серия «Основы информационных технологий»/Интернет ун-т информ. технологий). — ISBN 5-9556-0032-9.

Книга представляет собой краткое учебное пособие по локальным компьютерным сетям, в котором рассматриваются ключевые принципы, лежащие в основе архитектуры локальных сетей, базовые функции локальных сетей, а также алгоритмы реализации этих функций. Приводятся рекомендации по проектированию наиболее распространенных сетей Ethernet и Fast Ethernet. Также разбираются вопросы подключения локальных сетей к глобальной сети Интернет с помощью модемов.

**Рекомендовано для студентов высших учебных заведений, обучающихся по специальностям в области информационных технологий.**

Библиогр. 55

Издание осуществлено при финансовой поддержки «РМ Телеком»

**РМ Телеком®**

Курс лекций по информационным технологиям
Интернет-Университета Информационных Технологий
www.intuit.ru
Руководитель проекта – А. В. Шкред

## Основы локальных сетей
### Курс лекций. Учебное пособие
### Серия «Основы информационных технологий»

Формат $60 \times 90^1/_{16}$. Усл. печ. л. 22,5. Бумага офсетная.
Подписано в печать 10.03.2005. Тираж 2000 экз. Заказ № 5409.

ООО «ИНТУИТ.ру» Интернет-Университет Информационных Технологий, www.intuit.ru, 123056, Москва, Электрический пер., 8, стр. 3.

Отпечатано с готовых диапозитивов на ФГУП ордена «Знак Почета» Смоленская областная типография им. В.И. Смирнова. 214000, г. Смоленск, проспект им. Ю. Гагарина, д. 2.



**ISBN 5-9556-0032-9**

# О проекте

Интернет-Университет Информационных Технологий – это первое в России высшее учебное заведение, которое предоставляет возможность получить дополнительное образование во Всемирной сети. Web-сайт университета находится по адресу www.intuit.ru.

Мы рады, что вы решили расширить свои знания в области компьютерных технологий. Современный мир – это мир компьютеров и информации. Компьютерная индустрия – самый быстрорастущий сектор экономики, и ее рост будет продолжаться еще долгое время. Во времена жесткой конкуренции от уровня развития информационных технологий, достижений научной мысли и перспективных инженерных решений зависит успех не только отдельных людей и компаний, но и целых стран. Вы выбрали самое подходящее время для изучения компьютерных дисциплин. Профессионалы в области информационных технологий сейчас востребованы везде: в науке, экономике, образовании, медицине и других областях, в государственных и частных компаниях, в России и за рубежом. Анализ данных, прогнозы, организация связи, создание программного обеспечения, построение моделей процессов – вот далеко не полный список областей применения знаний для компьютерных специалистов.

Обучение в университете ведется по собственным учебным планам, разработанным ведущими российскими специалистами на основе международных образовательных стандартов Computer Curricula 2001 Computer Science. Изучать учебные курсы можно самостоятельно по учебникам или на сайте Интернет-Университета, задания выполняются только на сайте. Для обучения необходимо зарегистрироваться на сайте университета. Удостоверение об окончании учебного курса или специальности выдается при условии выполнения всех заданий к лекциям и успешной сдачи итогового экзамена.

Книга, которую вы держите в руках, – очередная в многотомной серии «Основы информационных технологий», выпускаемой Интернет-Университетом Информационных Технологий. В этой серии будут выпущены учебники по всем базовым областям знаний, связанным с компьютерными дисциплинами.

Добро пожаловать в Интернет-Университет Информационных Технологий!

**Анатолий Шкред**
***anatoli@shkred.ru***

# Предисловие

Локальные сети в последнее время из модного дополнения к компьютерам постепенно превращаются в обязательную принадлежность компаний, имеющих больше одного компьютера. Совершенствование аппаратуры и программных средств достигло такого уровня, что установить и эксплуатировать простейшую сеть может практически любой более или менее грамотный пользователь. Кроме того, предлагается множество книг, подробно описывающих процесс установки и обслуживания сетей. А наиболее распространенная операционная система Microsoft Windows изначально содержит в себе довольно развитые сетевые средства, так что даже покупать специальное сетевое программное обеспечение совсем не обязательно. И то, что раньше было доступно только посвященным, специально обученным профессионалам, теперь легко может проделать каждый.

Однако не всякий пользователь, который имеет дело с сетью, удовлетворяется той поверхностной информацией, которая содержится в большинстве популярных книг, отличающихся к тому же многословием и неизменным стремлением охватить все вопросы разом. Некоторым недостаточно знаний о том, как подключить сетевой адаптер к компьютеру, соединить кабелем адаптер с концентратором и запустить программу совместного использования диска. Им интересно также знать, что происходит внутри сети, как взаимодействуют между собой сетевые средства, какие алгоритмы они используют, чем отличаются друг от друга.

Но книг, посвященных этим специфическим вопросам, пока что явно недостаточно. Значительная часть выходящей сейчас литературы по сетям рассматривает главным образом особенности новых версий популярных сетевых программных средств, оставляя практически без внимания вопросы взаимодействия на нижних уровнях архитектуры. Именно эти пробелы и призвана восполнить данная книга.

В отличие от многих других изданий она содержит информацию, которая не скоро устареет. Ни появление новых программных средств, ни выпуск более эффективных и производительных аппаратных средств не отменят ключевых принципов, лежащих в основе сетевых технологий. Именно на этих принципах и сделан акцент в книге.

Кроме того, поверхностное знакомство с сетями породило немало ложных стереотипов, вольных или невольных заблуждений. Например, неправильное понимание терминологии, некритичное отношение к наиболее распространенным решениям, боязнь творчества. Преодоление подобных стереотипов также входит в задачу данной работы.

Книга в значительной мере самодостаточна. С одной стороны, она не требует от читателя каких-либо глубоких специальных знаний. С дру-

гой – она достаточно подробно рассматривает основные вопросы, связанные с локальными сетями. Книга может служить самоучителем и закладывает хорошую базу для дальнейшего, более глубокого изучения частных, узкоспециальных проблем.

Книга написана преподавателями Московского государственного инженерно-физического института (МИФИ) на основе личного опыта авторов, а также учебных курсов, читаемых в настоящее время на кафедре Электроники.

Главы 1, 2, 3, 4, 5, 8, 9, 10 написаны к.т.н., доцентом Ю.В. Новиковым, главы 6, 7 и 12 – к.т.н., доцентом С.В. Кондратенко, глава 11 – совместно обоими авторами.

В первых четырех главах рассматриваются общие принципы, лежащие в основе всех локальных сетей, разъясняются основные понятия и правила обмена.

Пятая глава посвящена особенностям наиболее распространенных и перспективных стандартных локальных сетей, их сравнению между собой по различным параметрам и вопросам применения.

В шестой главе кратко излагаются основные методы и алгоритмы шифрования информации в сетях, а также соответствующие программные средства.

Главы с седьмой по одиннадцатую посвящены наиболее популярной сети Ethernet/Fast Ethernet, алгоритмам ее работы, особенностям оборудования, правилам выбора топологии и проектирования сложных сетей.

Наконец, в двенадцатой главе описаны принципы подключения локальной сети к глобальной через модемы, алгоритмы работы модемов, их разновидности и стандарты.

В приложении содержатся сведения об основных организациях, занимающихся стандартизацией в области сетевых технологий.

В конце книги приведен подробный словарь терминов и сокращений, наиболее часто встречающихся в литературе по сетям.

# Об авторах

**Новиков Юрий Витальевич**

Кандидат технических наук, доцент факультета автоматики и электроники МИФИ, автор пяти книг по электронике и компьютерным локальным сетям: «Разработка устройств сопряжения для персонального компьютера типа IBM PC», «Аппаратура локальных сетей: функции, выбор, разработка», «Локальные сети: архитектура, алгоритмы, проектирование», «Основы цифровой схемотехники. Базовые элементы и схемы, методы проектирования», «Основы микропроцессорной техники».

**Кондратенко Сергей Владимирович**

Кандидат технических наук, доцент факультета автоматики и электроники МИФИ, автор книги «Локальные сети: архитектура, алгоритмы, проектирование».

# Лекции

# Содержание

**Внимание!**

**На сайте Интернет-университета информационных технологий Вы можете пройти тестирование по каждой лекции и курсу в целом.**

**Добро пожаловать на наш сайт:**

**www.intuit.ru**

# Глава 1. Определение локальных сетей и их топология

## Лекция 1. Определение локальных сетей и их топология

**В этой лекции говорится о базовой терминологии сетевых технологий, назначении и роли локальных сетей, применяемых сетевых структурах, их достоинствах и недостатках.**

**Ключевые слова**: локальная сеть, линии связи, абонент, сервер, клиент, топология, обмен информацией, устойчивость к отказам.

## Место и роль локальных сетей

### Немного истории компьютерной связи

Связь на небольшие расстояния в компьютерной технике существовала еще задолго до появления первых персональных компьютеров.

К большим компьютерам (mainframes), присоединялись многочисленные терминалы (или «интеллектуальные дисплеи»). Правда, интеллекта в этих терминалах было очень мало, практически никакой обработки информации они не делали, и основная цель организации связи состояла в том, чтобы разделить интеллект («машинное время») большого мощного и дорогого компьютера между пользователями, работающими за этими терминалами. Это называлось *режимом разделения времени*, так как большой компьютер последовательно во времени решал задачи множества пользователей. В данном случае достигалось совместное использование самых дорогих в то время ресурсов — вычислительных (рис. 1.1).

Затем были созданы микропроцессоры и первые микрокомпьютеры. Появилась возможность разместить компьютер на столе у каждого пользователя, так как вычислительные, интеллектуальные ресурсы подешевели. Но зато все остальные ресурсы оставались еще довольно дорогими. А что значит голый интеллект без средств хранения информации и ее документирования? Не будешь же каждый раз после включения питания заново набирать выполняемую программу или хранить ее в маловместительной постоянной памяти. На помощь снова пришли средства связи. Объединив несколько микрокомпьютеров, можно было организовать совместное ис-

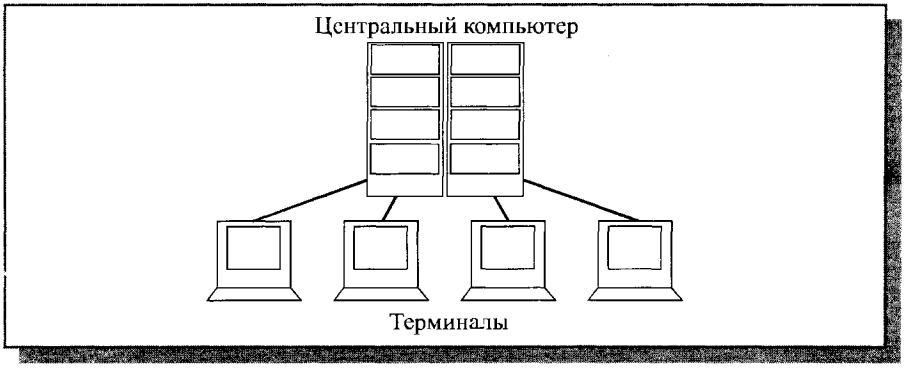



**Рис. 1.1.** Подключение терминалов к центральному компьютеру

пользование ими компьютерной периферии (магнитных дисков, магнитной ленты, принтеров). При этом вся обработка информации проводилась на месте, но ее результаты передавались на централизованные ресурсы. Здесь опять же совместно использовалось самое дорогое, что есть в системе, но уже совершенно по-новому. Такой режим получил название режима *обратного разделения времени* (рис. 1.2). Как и в первом случае, средства связи снижали стоимость компьютерной системы в целом.

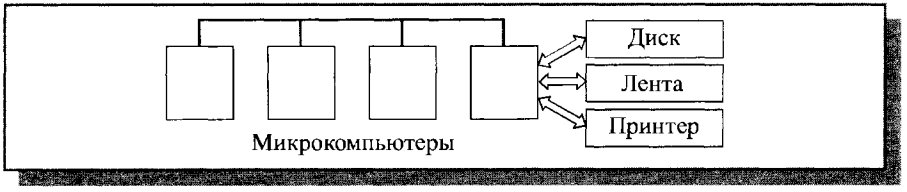



**Рис. 1.2.** Объединение в сеть первых микрокомпьютеров

Затем появились персональные компьютеры, которые отличались от первых микрокомпьютеров тем, что имели полный комплект достаточно развитой для полностью автономной работы периферии: магнитные диски, принтеры, не говоря уже о более совершенных средствах интерфейса пользователя (мониторы, клавиатуры, мыши и т.д.). Периферия подешевела и по цене стала вполне сравнима с компьютером. Казалось бы, зачем теперь соединять персональные компьютеры (рис. 1.3)? Что им разделять, когда и так уже все разделено и находится на столе у каждого пользователя? Интеллекта на месте хватает, периферии тоже. Что же может дать сеть в этом случае?

Самое главное — это опять же совместное использование ресурса. То самое обратное разделение времени, но уже на принципиально другом уровне. Здесь уже оно применяется не для снижения стоимости системы, а с целью более эффективного использования ресурсов, имеющихся в

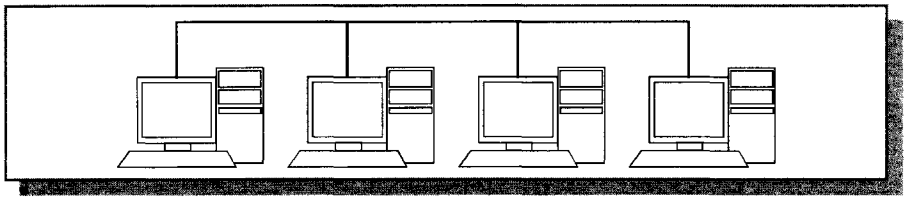


**Рис 1.3.** Объединение в сеть персональных компьютеров

распоряжении компьютеров. Например, сеть позволяет объединить объем дисков всех компьютеров, обеспечив доступ каждого из них к дискам всех остальных как к своим собственным.

Но нагляднее всего преимущества сети проявляются в том случае, когда все пользователи активно работают с единой базой данных, запрашивая информацию из нее и занося в нее новую (например, в банке, в магазине, на складе). Никакими дискетами тут уже не обойдешься: пришлось бы целыми днями переносить данные с каждого компьютера на все остальные, содержать целый штат курьеров. А с сетью все очень просто: любые изменения данных, произведенные с любого компьютера, тут же становятся видными и доступными всем. В этом случае особой обработки на месте обычно не требуется, и в принципе можно было бы обойтись более дешевыми терминалами (вернуться к первой рассмотренной ситуации), но персональные компьютеры имеют несравнимо более удобный интерфейс пользователя, облегчающий работу персонала. К тому же воз-

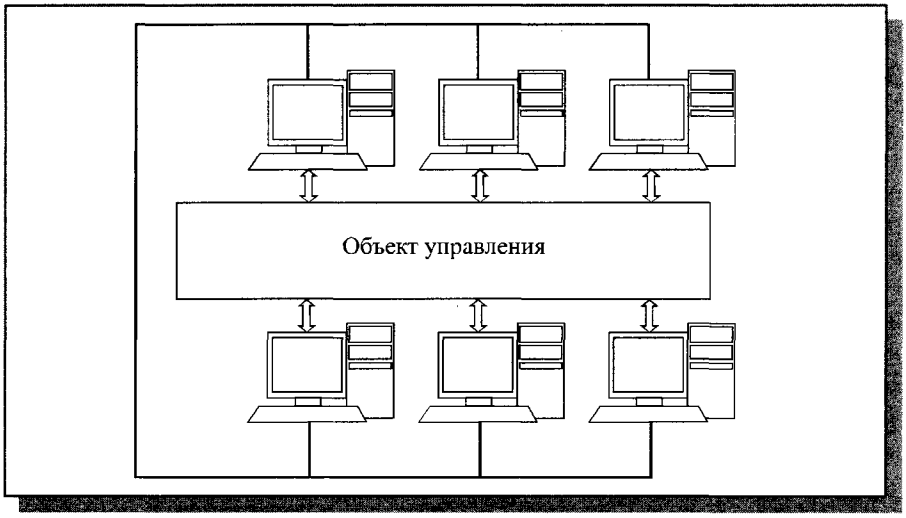



**Рис. 1.4.** Использование локальной сети для организации совместной работы компьютеров

можность сложной обработки информации на месте часто может заметно уменьшить объем передаваемых данных.

Без сети также невозможно обойтись в том случае, когда необходимо обеспечить согласованную работу нескольких компьютеров. Эта ситуация чаще всего встречается, когда эти компьютеры используются не для вычислений и работы с базами данных, а в задачах управления, измерения, контроля — там, где компьютер сопрягается с теми или иными внешними устройствами (рис. 1.4). Примерами могут служить различные производственные технологические системы, а также системы управления научными установками и комплексами. Здесь сеть позволяет синхронизовать действия компьютеров, распараллелить и соответственно ускорить процесс обработки данных, то есть сложить уже не только периферийные ресурсы, но и интеллектуальную мощь.

Именно указанные преимущества локальных сетей и обеспечивают их популярность и все более широкое применение, несмотря на все неудобства, связанные с их установкой и эксплуатацией.

## Определение локальной сети

Способов и средств обмена информацией за последнее время предложено множество: от простейшего переноса файлов с помощью дискеты до всемирной компьютерной сети Интернет, способной объединить все компьютеры мира. Какое же место в этой иерархии отводится локальным сетям?

Чаще всего термин «локальные сети» или «локальные вычислительные сети» (LAN, Local Area Network) понимают буквально, то есть это такие сети, которые имеют небольшие, локальные размеры, и соединяют близко расположенные компьютеры. Однако достаточно посмотреть на характеристики некоторых современных локальных сетей, чтобы понять, что такое определение не точно. Например, некоторые локальные сети легко обеспечивают связь на расстоянии нескольких десятков километров. Это уже размеры не комнаты, не здания, не близко расположенных зданий, но, может быть, даже целого города. С другой стороны, по глобальной сети (WAN, Wide Area Network или GAN, Global Area Network) вполне могут связываться компьютеры, находящиеся на соседних столах в одной комнате, но ее почему-то никто не называет локальной сетью. Близко расположенные компьютеры могут также связываться с помощью кабеля, соединяющего разъемы внешних интерфейсов (RS232-C, Centronics) или даже без кабеля по инфракрасному каналу (IrDA). Но такая связь тоже почему-то не называется локальной.

Неверно и довольно часто встречающееся определение локальной сети как малой сети, которая объединяет небольшое количество компьютеров. Действительно, как правило, локальная сеть связывает от двух до

нескольких десятков компьютеров. Но предельные возможности современных локальных сетей гораздо выше: максимальное число абонентов может достигать тысячи. Называть такую сеть малой неправильно.

Некоторые авторы определяют локальную сеть как «систему для непосредственного соединения многих компьютеров». При этом подразумевается, что информация передается от компьютера к компьютеру без каких-либо посредников и по единой среде передачи. Однако говорить о единой среде передачи в современной локальной сети не приходится. Например, в пределах одной сети могут использоваться как электрические кабели различных типов (витая пара, коаксиальный кабель), так и оптоволоконные кабели. Определение передачи «без посредников» также не корректно — ведь в современных локальных сетях используются репитеры, трансиверы, концентраторы, коммутаторы, маршрутизаторы, мосты, которые порой производят довольно сложную обработку передаваемой информации. Не совсем понятно, можно ли считать их посредниками или нет, и можно ли считать подобную сеть локальной.

Наверное, наиболее точно было бы назвать локальной такую сеть, которая позволяет пользователям не замечать связи. Еще можно сказать, что локальная сеть должна обеспечивать *прозрачную* связь. По сути, компьютеры, связанные локальной сетью объединяются, в один виртуальный компьютер, ресурсы которого могут быть доступны всем пользователям, причем этот доступ не менее удобен, чем доступ к ресурсам, входящим непосредственно в каждый отдельный компьютер. Под удобством в данном случае понимается высокая реальная скорость доступа, скорость обмена информацией между приложениями, практически не заметная для пользователя. При таком определении становится понятно, что ни медленные глобальные сети, ни медленная связь через последовательный или параллельный порты не подпадают под понятие локальной сети.

Из данного определения следует, что скорость передачи по локальной сети обязательно должна расти по мере роста быстродействия наиболее распространенных компьютеров. Именно это и наблюдается: если еще десять лет назад вполне приемлемой считалась скорость обмена в 10 Мбит/с, то сейчас уже среднескоростной считается сеть, имеющая пропускную способность 100 Мбит/с, активно разрабатываются, а кое-где используются средства для скорости 1000 Мбит/с и даже больше. Без этого уже нельзя, иначе связь станет слишком узким местом, будет чрезмерно замедлять работу объединенного сетью виртуального компьютера, и снижать удобство доступа к сетевым ресурсам.

Таким образом, главное отличие локальной сети от любой другой — высокая скорость передачи информации по сети. Но это еще не все, не менее важны и другие факторы.

В частности, принципиально необходим низкий уровень ошибок передачи, вызванных как внутренними, так и внешними факторами. Ведь даже очень быстро переданная информация, которая искажена ошибками, просто не имеет смысла, ее придется передавать еще раз. Поэтому локальные сети обязательно используют специально прокладываемые высококачественные и хорошо защищенные от помех линии связи.

Особое значение имеет и такая характеристика сети, как возможность работы с большими нагрузками, то есть с высокой интенсивностью обмена (или, как еще говорят, с большим трафиком). Ведь если механизм управления обменом, используемый в сети, не слишком эффективен, то компьютеры могут подолгу ждать своей очереди на передачу. И даже если эта передача будет производиться затем на высочайшей скорости и безошибочно, для пользователя сети такая задержка доступа ко всем сетевым ресурсам неприемлема. Ему ведь не важно, почему приходится ждать.

Механизм управления обменом может гарантированно успешно работать только в том случае, когда заранее известно, сколько компьютеров (или, как еще говорят, абонентов, узлов) допустимо подключить к сети. Иначе всегда можно включить столько абонентов, что вследствие перегрузки забуксует любой механизм управления. Наконец, сетью можно назвать только такую систему передачи данных, которая позволяет объединять до нескольких десятков компьютеров, но никак не два, как в случае связи через стандартные порты.

Таким образом, сформулировать отличительные признаки локальной сети можно следующим образом:

- Высокая скорость передачи информации, большая пропускная способность сети. Приемлемая скорость сейчас — не менее 10 Мбит/с.
- Низкий уровень ошибок передачи (или, что то же самое, высококачественные каналы связи). Допустимая вероятность ошибок передачи данных должна быть порядка $10^{-8}$ — $10^{-12}$.
- Эффективный, быстродействующий механизм управления обменом по сети.
- Заранее четко ограниченное количество компьютеров, подключаемых к сети.

При таком определении понятно, что глобальные сети отличаются от локальных прежде всего тем, что они рассчитаны на неограниченное число абонентов. Кроме того, они используют (или могут использовать) не слишком качественные каналы связи и сравнительно низкую скорость передачи. А механизм управления обменом в них не может быть гарантированно быстрым. В глобальных сетях гораздо важнее не качество связи, а сам факт ее существования.

Нередко выделяют еще один класс компьютерных сетей — городские, региональные сети (MAN, Metropolitan Area Network), которые обычно по

своим характеристикам ближе к глобальным сетям, хотя иногда все-таки имеют некоторые черты локальных сетей, например, высококачественные каналы связи и сравнительно высокие скорости передачи. В принципе городская сеть может быть локальной со всеми ее преимуществами.

Правда, сейчас уже нельзя провести четкую границу между локальными и глобальными сетями. Большинство локальных сетей имеет выход в глобальную. Но характер передаваемой информации, принципы организации обмена, режимы доступа к ресурсам внутри локальной сети, как правило, сильно отличаются от тех, что приняты в глобальной сети. И хотя все компьютеры локальной сети в данном случае включены также и в глобальную сеть, специфики локальной сети это не отменяет. Возможность выхода в глобальную сеть остается всего лишь одним из ресурсов, разделяемых пользователями локальной сети.

По локальной сети может передаваться самая разная цифровая информация: данные, изображения, телефонные разговоры, электронные письма и т.д. Кстати, именно задача передачи изображений, особенно полноцветных динамических, предъявляет самые высокие требования к быстродействию сети. Чаще всего локальные сети используются для разделения (совместного использования) таких ресурсов, как дисковое пространство, принтеры и выход в глобальную сеть, но это всего лишь незначительная часть тех возможностей, которые предоставляют средства локальных сетей. Например, они позволяют осуществлять обмен информацией между компьютерами разных типов. Полноценными абонентами (узлами) сети могут быть не только компьютеры, но и другие устройства, например, принтеры, плоттеры, сканеры. Локальные сети дают также возможность организовать систему параллельных вычислений на всех компьютерах сети, что многократно ускоряет решение сложных математических задач. С их помощью, как уже упоминалось, можно управлять работой технологической системы или исследовательской установки с нескольких компьютеров одновременно.

Однако сети имеют и довольно существенные недостатки, о которых всегда следует помнить:

- Сеть требует дополнительных, иногда значительных материальных затрат на покупку сетевого оборудования, программного обеспечения, на прокладку соединительных кабелей и обучение персонала.
- Сеть требует приема на работу специалиста (администратора сети), который будет заниматься контролем работы сети, ее модернизацией, управлением доступом к ресурсам, устранением возможных неисправностей, защитой информации и резервным копированием. Для больших сетей может понадобиться целая бригада администраторов.
- Сеть ограничивает возможности перемещения компьютеров, подключенных к ней, так как при этом может понадобиться перекладка соединительных кабелей.

- Сети представляют собой прекрасную среду для распространения компьютерных вирусов, поэтому вопросам защиты от них придется уделять гораздо больше внимания, чем в случае автономного использования компьютеров. Ведь достаточно инфицировать один — и все компьютеры сети будут поражены.
- Сеть резко повышает опасность несанкционированного доступа к информации с целью ее кражи или уничтожения. Информационная защита требует проведения целого комплекса технических и организационных мероприятий.

Ничто не дается даром. И надо хорошо подумать, стоит ли подключать к сети все компьютеры компании, или часть из них лучше оставить автономными. Возможно, что сеть вообще не нужна, так как породит гораздо больше проблем, чем позволит решить.

Здесь же следует упомянуть о таких важнейших понятиях теории сетей, как абонент, сервер, клиент.

**Абонент** (узел, хост, станция) — это устройство, подключенное к сети и активно участвующее в информационном обмене. Чаще всего абонентом (узлом) сети является компьютер, но абонентом также может быть, например, сетевой принтер или другое периферийное устройство, имеющее возможность напрямую подключаться к сети. Далее в тексте книги вместо термина «абонент» для простоты будет использоваться термин «компьютер».

**Сервером** называется абонент (узел) сети, который предоставляет свои ресурсы другим абонентам, но сам не использует их ресурсы. Таким образом, он обслуживает сеть. Серверов в сети может быть несколько, и совсем не обязательно, что сервер —самый мощный компьютер. *Выделенный* (dedicated) сервер — это сервер, занимающийся только сетевыми задачами. *Невыделенный* сервер может помимо обслуживания сети выполнять и другие задачи. Специфический тип сервера — это сетевой принтер.

**Клиентом** называется абонент сети, который только использует сетевые ресурсы, но сам свои ресурсы в сеть не отдает, то есть сеть его обслуживает, а он ей только пользуется. Компьютер-клиент также часто называют *рабочей станцией*. В принципе каждый компьютер может быть одновременно как клиентом, так и сервером.

Под сервером и клиентом часто понимают также не сами компьютеры, а работающие на них программные приложения. В этом случае то приложение, которое только отдает ресурс в сеть, является сервером, а то приложение, которое только пользуется сетевыми ресурсами — клиентом.

## Топология локальных сетей

Под топологией (компоновкой, конфигурацией, структурой) компьютерной сети обычно понимается физическое расположение компьютеров сети друг относительно друга и способ соединения их линиями связи. Важно отметить, что понятие топологии относится, прежде всего, к локальным сетям, в которых структуру связей можно легко проследить. В глобальных сетях структура связей обычно скрыта от пользователей и не слишком важна, так как каждый сеанс связи может производиться по собственному пути.

Топология определяет требования к оборудованию, тип используемого кабеля, допустимые и наиболее удобные методы управления обменом, надежность работы, возможности расширения сети. И хотя выбирать топологию пользователю сети приходится нечасто, знать об особенностях основных топологий, их достоинствах и недостатках надо.

Существует три базовые топологии сети:

- *Шина* (bus) — все компьютеры параллельно подключаются к одной линии связи. Информация от каждого компьютера одновременно передается всем остальным компьютерам (рис. 1.5).

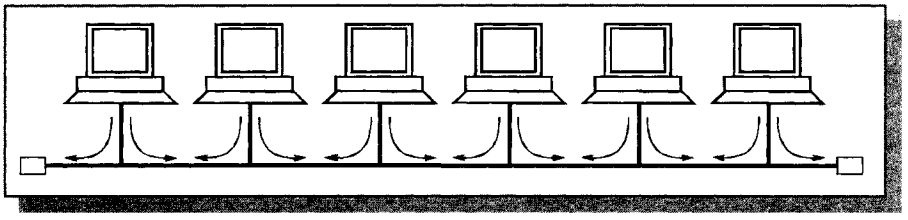


**Рис. 1.5.** Сетевая топология «шина»

- *Звезда* (star) — к одному центральному компьютеру присоединяются остальные периферийные компьютеры, причем каждый из них использует отдельную линию связи (рис. 1.6). Информация от периферийного компьютера передается только центральному компьютеру, от центрального — одному или нескольким периферийным.
- *Кольцо* (ring) — компьютеры последовательно объединены в кольцо. Передача информации в кольце всегда производится только в одном направлении. Каждый из компьютеров передает информацию только одному компьютеру, следующему в цепочке за ним, а получает информацию только от предыдущего в цепочке компьютера (рис. 1.7).

На практике нередко используют и другие топологии локальных сетей, однако большинство сетей ориентировано именно на три базовые топологии.

Прежде чем перейти к анализу особенностей базовых сетевых топологий, необходимо выделить некоторые важнейшие факторы, влияющие

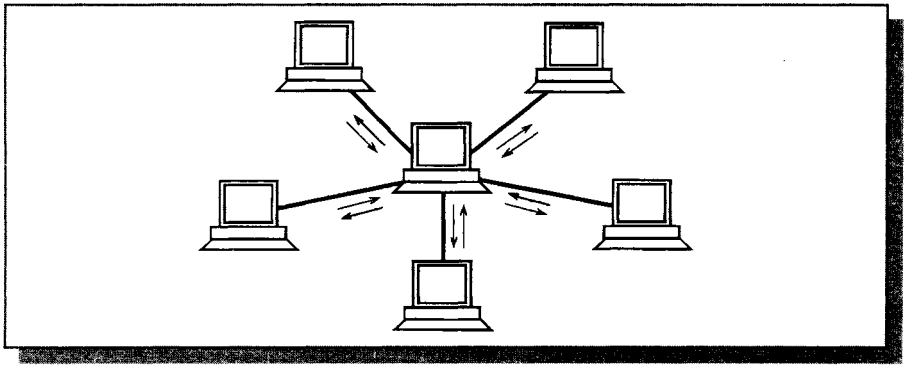


**Рис. 1.6.** Сетевая топология звезда

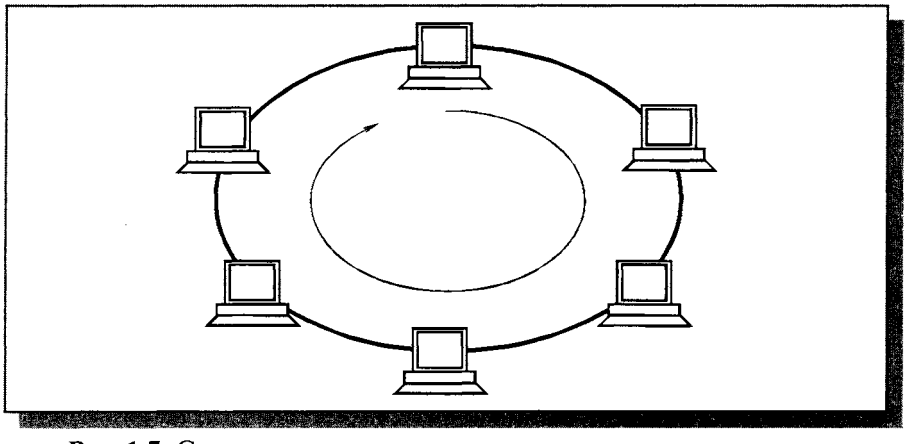


**Рис. 1.7.** Сетевая топология кольцо

на физическую работоспособность сети и непосредственно связанные с понятием топология.

- Исправность компьютеров (абонентов), подключенных к сети. В некоторых случаях поломка абонента может заблокировать работу всей сети. Иногда неисправность абонента не влияет на работу сети в целом, и не мешает остальным абонентам обмениваться информацией.
- Исправность сетевого оборудования, то есть технических средств, непосредственно подключенных к сети (адаптеры, трансиверы, разъемы и т.д.). Выход из строя сетевого оборудования одного из абонентов может сказаться на всей сети, но может нарушить обмен только с одним абонентом.
- Целостность кабеля сети. При обрыве кабеля сети (например, из-за механических воздействий) может нарушиться обмен информацией

во всей сети или в одной из ее частей. Для электрических кабелей столь же критично короткое замыкание в кабеле.

- Ограничение длины кабеля, связанное с затуханием распространяющегося по нему сигнала. Как известно, в любой среде при распространении сигнал ослабляется (затухает). И чем большее расстояние проходит сигнал, тем больше он затухает (рис. 1.8). Необходимо следить, чтобы длина кабеля сети не была больше предельной длины $L_{пр}$, при превышении которой затухание становится уже неприемлемым (принимающий абонент не распознает ослабевший сигнал).

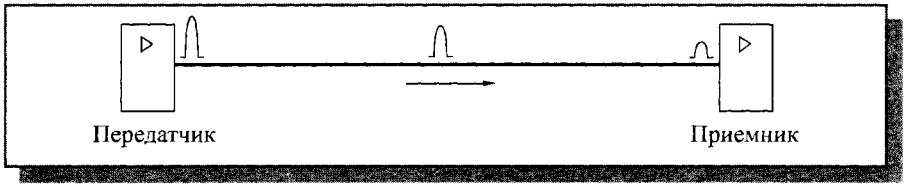



**Рис. 1.8.** Затухание сигнала при распространении по сети

## Топология «шина»

Топология «шина» (или, как ее еще называют, общая шина) самой своей структурой предполагает идентичность сетевого оборудования компьютеров, а также равноправие всех абонентов по доступу к сети. Компьютеры в шине могут передавать только по очереди, так как линия связи в данном случае единственная. Если несколько компьютеров будут передавать информацию одновременно, она исказится в результате наложения (*конфликта*, *коллизии*). В шине всегда реализуется режим так называемого *полудуплексного* (half duplex) обмена (в обоих направлениях, но по очереди, а не одновременно).

В топологии «шина» отсутствует явно выраженный центральный абонент, через которого передается вся информация, что увеличивает ее надежность (ведь при отказе центра перестает функционировать вся управляемая им система). Добавление новых абонентов в шину довольно просто и обычно возможно даже во время работы сети. В большинстве случаев при использовании шины требуется минимальное количество соединительного кабеля по сравнению с другими топологиями.

Поскольку центральный абонент отсутствует, разрешение возможных конфликтов в данном случае ложится на сетевое оборудование каждого отдельного абонента. В связи с этим сетевая аппаратура при топологии шина сложнее, чем при других топологиях. Тем не менее из-за широкого распространения сетей с топологией «шина» (прежде всего наиболее популярной сети Ethernet) стоимость сетевого оборудования не слишком высока.

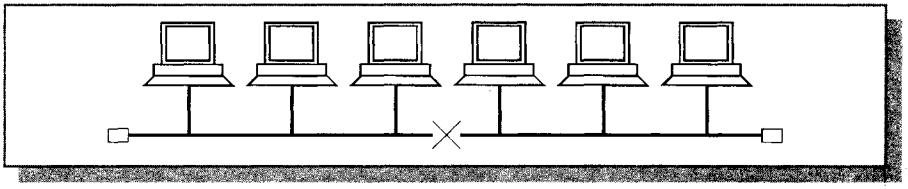


**Рис. 1.9.** Обрыв кабеля в сети с топологией шина

Важное преимущество шины состоит в том, что при отказе любого из компьютеров сети исправные машины смогут нормально продолжать обмен.

Казалось бы, при обрыве кабеля получаются две вполне работоспособные шины (рис. 1.9). Однако надо учитывать, что из-за особенностей распространения электрических сигналов по длинным линиям связи необходимо предусматривать включение на концах шины специальных согласующих устройств, *терминаторов*, показанных на рис. 1.5 и 1.9 в виде прямоугольников. Без включения терминаторов сигнал отражается от конца линии и искажается так, что связь по сети становится невозможной. В случае разрыва или повреждения кабеля нарушается согласование линии связи, и прекращается обмен даже между теми компьютерами, которые остались соединенными между собой. Подробнее о согласовании будет изложено в специальном разделе книги. Короткое замыкание в любой точке кабеля шины выводит из строя всю сеть.

Отказ сетевого оборудования любого абонента в шине может вывести из строя всю сеть. К тому же такой отказ довольно трудно локализовать, поскольку все абоненты включены параллельно, и понять, какой из них вышел из строя, невозможно.

При прохождении по линии связи сети с топологией *шина* информационные сигналы ослабляются и никак не восстанавливаются, что накладывает жесткие ограничения на суммарную длину линий связи. Причем каждый абонент может получать из сети сигналы разного уровня в зависимости от расстояния до передающего абонента. Это предъявляет дополнительные требования к приемным узлам сетевого оборудования.

Если принять, что сигнал в кабеле сети ослабляется до предельно допустимого уровня на длине $L_{пр}$, то полная длина шины не может превышать величины $L_{пр}$. В этом смысле шина обеспечивает наименьшую длину по сравнению с другими базовыми топологиями.

Для увеличения длины сети с топологией «шина» часто используют несколько *сегментов* (частей сети, каждый из которых представляет собой шину), соединенных между собой с помощью специальных усилителей и восстановителей сигналов — *репитеров* или *повторителей* (на рис. 1.10 показано соединение двух сегментов. Предельная длина сети в этом случае возрастает до 2 $L_{пр}$, так как каждый из сегментов может быть длиной $L_{пр}$).

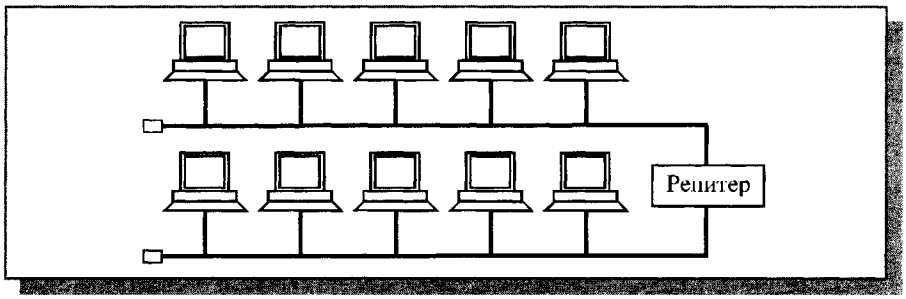



**Рис. 1.10.** Соединение сегментов сети типа шина с помощью репитера

Однако такое наращивание длины сети не может продолжаться бесконечно. Ограничения на длину связаны с конечной скоростью распространения сигналов по линиям связи.

## Топология звезда

Звезда — это единственная топология сети с явно выделенным центром, к которому подключаются все остальные абоненты. Обмен информацией идет исключительно через центральный компьютер, на который ложится большая нагрузка, поэтому ничем другим, кроме сети, он, как правило, заниматься не может. Понятно, что сетевое оборудование центрального абонента должно быть существенно более сложным, чем оборудование периферийных абонентов. О равноправии всех абонентов (как в шине) в данном случае говорить не приходится. Обычно центральный компьютер — самый мощный, именно на него возлагаются все функции по управлению обменом. Никакие конфликты в сети с топологией «звезда» в принципе невозможны, так как управление полностью централизовано.

Если говорить об устойчивости звезды к отказам компьютеров, то выход из строя периферийного компьютера или его сетевого оборудования никак не отражается на функционировании оставшейся части сети, зато любой отказ центрального компьютера делает сеть полностью неработоспособной. В связи с этим должны приниматься специальные меры по повышению надежности центрального компьютера и его сетевой аппаратуры.

Обрыв кабеля или короткое замыкание в нем при топологии «звезда» нарушает обмен только с одним компьютером, а все остальные компьютеры могут нормально продолжать работу.

В отличие от шины, в звезде на каждой линии связи находятся только два абонента: центральный и один из периферийных. Чаще всего для их соединения используется две линии связи, каждая из которых передает информацию в одном направлении, то есть на каждой линии связи имеется только один приемник и один передатчик. Это так называемая

передача *точка-точка*. Все это существенно упрощает сетевое оборудование по сравнению с шиной и избавляет от необходимости применения дополнительных, внешних терминаторов.

Проблема затухания сигналов в линии связи также решается в звезде проще, чем в случае шины — ведь каждый приемник всегда получает сигнал одного уровня. Предельная длина сети с топологией «звезда» может быть вдвое больше, чем в шине (то есть 2 $L_{пр}$), так как каждый из кабелей, соединяющий центр с периферийным абонентом, может иметь длину $L_{пр}$.

Серьезный недостаток топологии «звезда» состоит в жестком ограничении количества абонентов. Обычно центральный абонент может обслуживать не более 8–16 периферийных абонентов. В этих пределах подключение новых абонентов довольно просто, но за ними оно просто невозможно. В звезде допустимо подключение еще одного центрального абонента вместо переферийного(в результате получается топология из нескольких соединенных между собой звезд).

Звезда, показанная на рис. 1.6, носит название активной или истинной звезды. Существует также топология, называемая пассивной звездой, которая только внешне похожа на звезду (рис. 1.11). В настоящее время она распространена гораздо более широко, чем активная звезда. Достаточно сказать, что она используется в наиболее популярной сегодня сети Ethernet.

В центре сети с данной топологией помещается не компьютер, а специальное устройство — концентратор или, как его еще называют, хаб (hub), которое выполняет ту же функцию, что и репитер, то есть восстанавливает приходящие сигналы и пересылает их во все другие линии связи.

Получается, что хотя схема прокладки кабелей подобна истинной или активной звезде, фактически речь идет о шинной топологии, так как информация от каждого компьютера одновременно передается ко всем остальным компьютерам, а никакого центрального абонента не существует. Безусловно, пассивная звезда дороже обычной шины, так как в этом

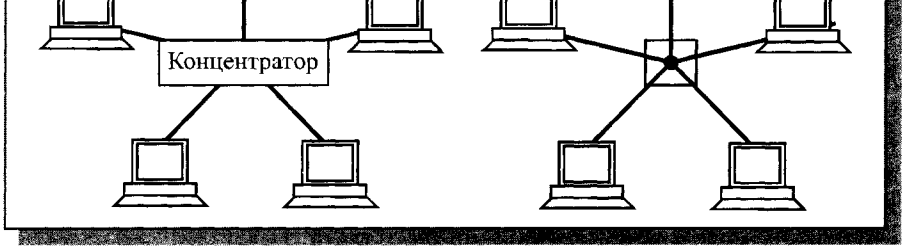



**Рис. 1.11.** Топология пассивная звезда и ее эквивалентная схема

случае требуется еще и концентратор. Однако она предоставляет целый ряд дополнительных возможностей, связанных с преимуществами звезды, в частности, упрощает обслуживание и ремонт сети. Именно поэтому в последнее время пассивная звезда все больше вытесняет истинную шину, которая считается малоперспективной топологией.

Можно выделить также промежуточный тип топологии между активной и пассивной звездой. В этом случае концентратор не только ретранслирует поступающие на него сигналы, но и производит управление обменом, однако сам в обмене не участвует (так сделано в сети 100VG-AnyLAN).

Большое достоинство звезды (как активной, так и пассивной) состоит в том, что все точки подключения собраны в одном месте. Это позволяет легко контролировать работу сети, локализовать неисправности путем простого отключения от центра тех или иных абонентов (что невозможно, например, в случае шинной топологии), а также ограничивать доступ посторонних лиц к жизненно важным для сети точкам подключения. К периферийному абоненту в случае звезды может подходить как один кабель (по которому идет передача в обоих направлениях), так и два (каждый кабель передает в одном из двух встречных направлений), причем последнее встречается гораздо чаще.

Общим недостатком для всех топологий типа «звезда» (как активной, так и пассивной) является значительно больший, чем при других топологиях, расход кабеля. Например, если компьютеры расположены в одну линию (как на рис. 1.5), то при выборе топологии «звезда» понадобится в несколько раз больше кабеля, чем при топологии «шина». Это существенно влияет на стоимость сети в целом и заметно усложняет прокладку кабеля.

### Топология кольцо

*Кольцо* — это топология, в которой каждый компьютер соединен линиями связи с двумя другими: от одного он получает информацию, а другому передает. На каждой линии связи, как и в случае звезды, работает только один передатчик и один приемник (связь типа точка-точка). Это позволяет отказаться от применения внешних терминаторов.

Важная особенность кольца состоит в том, что каждый компьютер ретранслирует (восстанавливает, усиливает) приходящий к нему сигнал, то есть выступает в роли репитера. Затухание сигнала во всем кольце не имеет никакого значения, важно только затухание между соседними компьютерами кольца. Если предельная длина кабеля, ограниченная затуханием, составляет $L_{пр}$, то суммарная длина кольца может достигать $NL_{пр}$, где N — количество компьютеров в кольце. Полный размер сети в пределе будет $NL_{пр}/2$, так как кольцо придется сложить вдвое. На практике размеры кольцевых сетей достигают десятков километров (например, в

сети FDDI). Кольцо в этом отношении существенно превосходит любые другие топологии.

Четко выделенного центра при кольцевой топологии нет, все компьютеры могут быть одинаковыми и равноправными. Однако довольно часто в кольце выделяется специальный абонент, который управляет обменом или контролирует его. Понятно, что наличие такого единственного управляющего абонента снижает надежность сети, так как выход его из строя сразу же парализует весь обмен.

Строго говоря, компьютеры в кольце не являются полностью равноправными (в отличие, например, от шинной топологии). Ведь одни из них обязательно получают информацию от компьютера, ведущего передачу в данный момент, раньше, а другие — позже. Именно на этой особенности топологии и строятся методы управления обменом по сети, специально рассчитанные на кольцо. В таких методах право на следующую передачу (или, как еще говорят, на захват сети) переходит последовательно к следующему по кругу компьютеру. Подключение новых абонентов к кольцу выполняется достаточно просто, хотя и требует обязательной остановки работы всей сети на время подключения. Как и в случае шины, максимальное количество абонентов в кольце может быть довольно велико (до тысячи и больше). Кольцевая топология обычно обладает высокой устойчивостью к перегрузкам, обеспечивает уверенную работу с большими потоками передаваемой по сети информации, так как в ней, как правило, нет конфликтов (в отличие от шины), а также отсутствует центральный абонент (в отличие от звезды), который может быть перегружен большими потоками информации.

Сигнал в кольце проходит последовательно через все компьютеры сети, поэтому выход из строя хотя бы одного из них (или же его сетевого

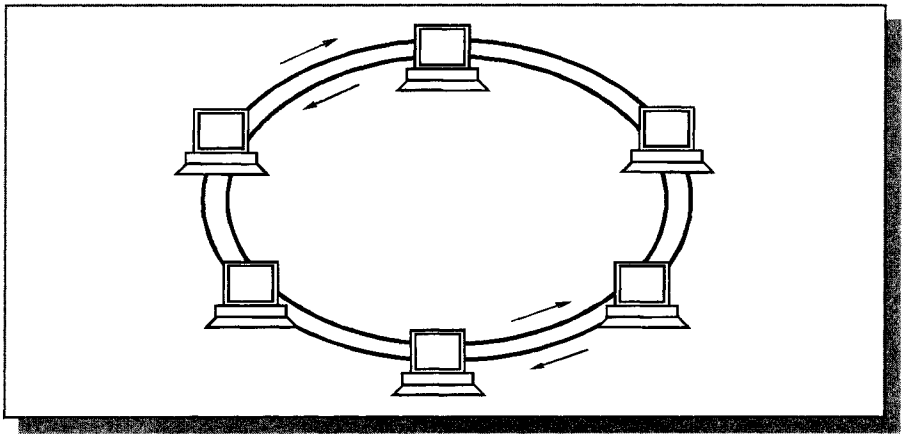


**Рис. 1.12.** Сеть с двумя кольцами

оборудования) нарушает работу сети в целом. Это существенный недостаток кольца.

Точно так же обрыв или короткое замыкание в любом из кабелей кольца делает работу всей сети невозможной. Из трех рассмотренных топологий «кольцо» наиболее уязвимо к повреждениям кабеля, поэтому в случае топологии кольцо обычно предусматривают прокладку двух (или более) параллельных линий связи, одна из которых находится в резерве.

Иногда сеть с топологией «кольцо» выполняется на основе двух параллельных кольцевых линий связи, передающих информацию в противоположных направлениях (рис. 1.12). Цель подобного решения — увеличение (в идеале — вдвое) скорости передачи информации по сети. К тому же при повреждении одного из кабелей сеть может работать с другим кабелем (правда, предельная скорость уменьшится).

### Другие топологии

Кроме трех рассмотренных базовых топологий нередко применяется также сетевая топология дерево (tree), которую можно рассматривать как комбинацию нескольких звезд. Причем, как и в случае звезды, дерево может быть активным или истинным (рис. 1.13) и пассивным (рис. 1.14). При активном дереве в центрах объединения нескольких линий связи находятся центральные компьютеры, а при пассивном — концентраторы (хабы).

Довольно часто применяются комбинированные топологии, среди которых наиболее распространены звездно-шинная (рис. 1.15) и звездно-кольцевая (рис. 1.16).

В звездно-шинной (star-bus) топологии используется комбинация шины и пассивной звезды. К концентратору подключаются как отдельные компьютеры, так и целые шинные сегменты. На самом деле реализуется физическая топология «шина», включающая все компьютеры сети. В дан-

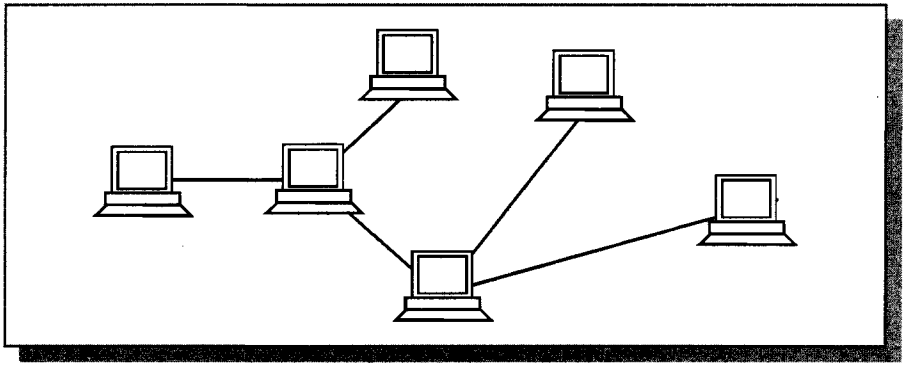


**Рис. 1.13.** Топология активное дерево

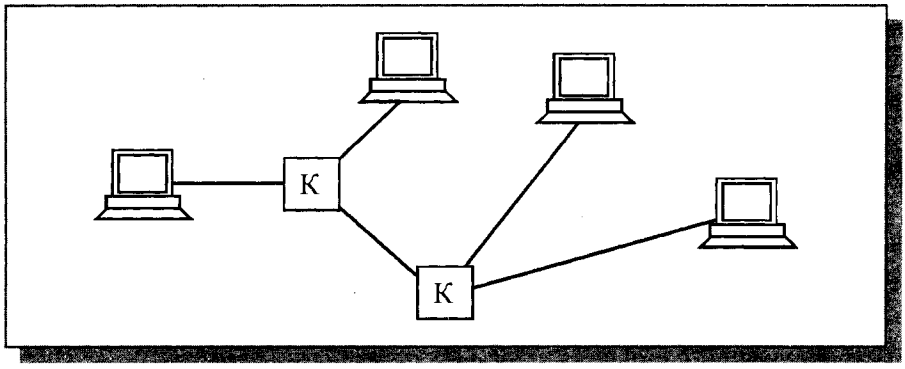



**Рис. 1.14.** Топология пассивное дерево. К — концентраторы

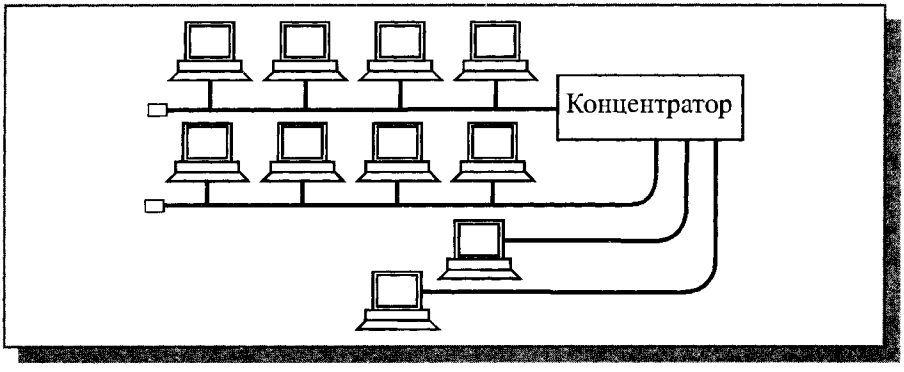



**Рис. 1.15.** Пример звездно-шинной топологии

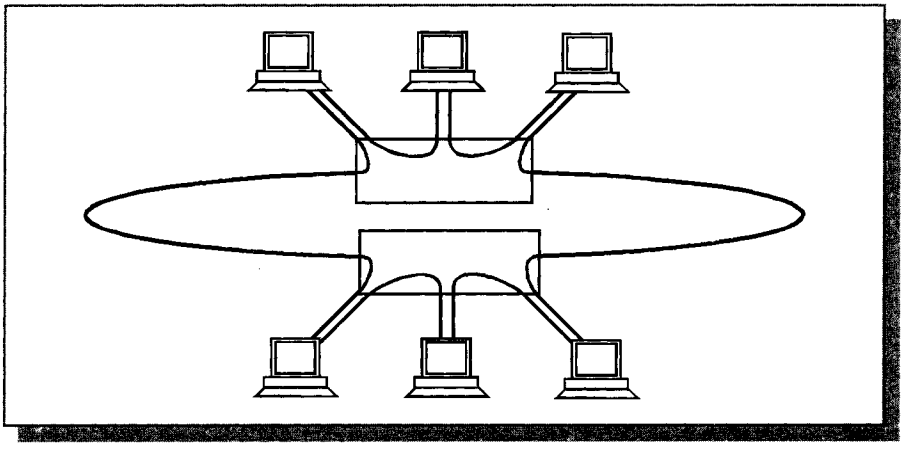


**Рис. 1.16.** Пример звездно-кольцевой топологии

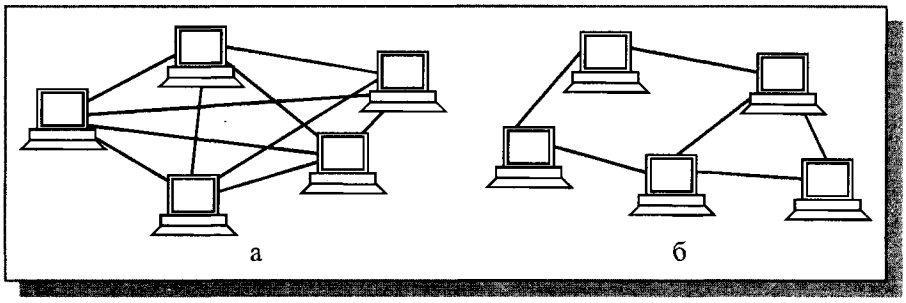



**Рис. 1.17.** Сеточная топология: полная (а) и частичная (б)

ной топологии может использоваться и несколько концентраторов, соединенных между собой и образующих так называемую магистральную, опорную шину. К каждому из концентраторов при этом подключаются отдельные компьютеры или шинные сегменты. В результате получается звездно-шинное дерево. Таким образом, пользователь может гибко комбинировать преимущества шинной и звездной топологий, а также легко изменять количество компьютеров, подключенных к сети. С точки зрения распространения информации данная топология равноценна классической шине.

В случае звездно-кольцевой (star-ring) топологии в кольцо объединяются не сами компьютеры, а специальные концентраторы (изображенные на рис. 1.16 в виде прямоугольников), к которым в свою очередь подключаются компьютеры с помощью звездообразных двойных линий связи. В действительности все компьютеры сети включаются в замкнутое кольцо, так как внутри концентраторов линии связи образуют замкнутый контур (как показано на рис. 1.16). Данная топология дает возможность комбинировать преимущества звездной и кольцевой топологий. Например, концентраторы позволяют собрать в одно место все точки подключения кабелей сети. Если говорить о распространении информации, данная топология равноценна классическому кольцу.

В заключение надо также сказать о сеточной топологии (mesh), при которой компьютеры связываются между собой не одной, а многими линиями связи, образующими сетку (рис. 1.17).

В полной сеточной топологии каждый компьютер напрямую связан со всеми остальными компьютерами. В этом случае при увеличении числа компьютеров резко возрастает количество линий связи. Кроме того, любое изменение в конфигурации сети требует внесения изменений в сетевую аппаратуру всех компьютеров, поэтому полная сеточная топология не получила широкого распространения.

Частичная сеточная топология предполагает прямые связи только для самых активных компьютеров, передающих максимальные объемы информации. Остальные компьютеры соединяются через промежуточные узлы.

Сеточная топология позволяет выбирать маршрут для доставки информации от абонента к абоненту, обходя неисправные участки. С одной стороны, это увеличивает надежность сети, с другой же – требует существенного усложнения сетевой аппаратуры, которая должна выбирать маршрут.

### Многозначность понятия топологии

Топология сети указывает не только на физическое расположение компьютеров, как часто считают, но, что гораздо важнее, на характер связей между ними, особенности распространения информации, сигналов по сети. Именно характер связей определяет степень отказоустойчивости сети, требуемую сложность сетевой аппаратуры, наиболее подходящий метод управления обменом, возможные типы сред передачи (каналов связи), допустимый размер сети (длина линий связи и количество абонентов) необходимость электрического согласования и многое другое.

Более того, физическое расположение компьютеров, соединяемых сетью, почти не влияет на выбор топологии. Как бы ни были расположены компьютеры, их можно соединить с помощью любой заранее выбранной топологии (рис. 1.18).

В том случае, если соединяемые компьютеры расположены по контуру круга, они могут соединяться, как звезда или шина. Когда компьютеры расположены вокруг некоего центра, их допустимо соединить с помощью топологий «щина» или «кольцо».

Наконец когда компьютеры расположены в одну линию, они могут соединяться звездой или кольцом. Другое дело, какова будет требуемая длина кабеля.

Строго говоря, в литературе при упоминании о топологии сети авторы могут подразумевать четыре совершенно разные понятия, относящиеся к различным уровням сетевой архитектуры:

- Физическая топология (географическая схема расположения компьютеров и прокладки кабелей). В этом смысле, например, пассивная звезда ничем не отличается от активной, поэтому ее нередко называют просто звездой.
- Логическая топология (структура связей, характер распространения сигналов по сети). Это наиболее правильное определение топологии.
- Топология управления обменом (принцип и последовательность передачи права на захват сети между отдельными компьютерами).
- Информационная топология (направление потоков информации, передаваемой по сети).

Например, сеть с физической и логической топологией «шина» может в качестве метода управления использовать эстафетную передачу

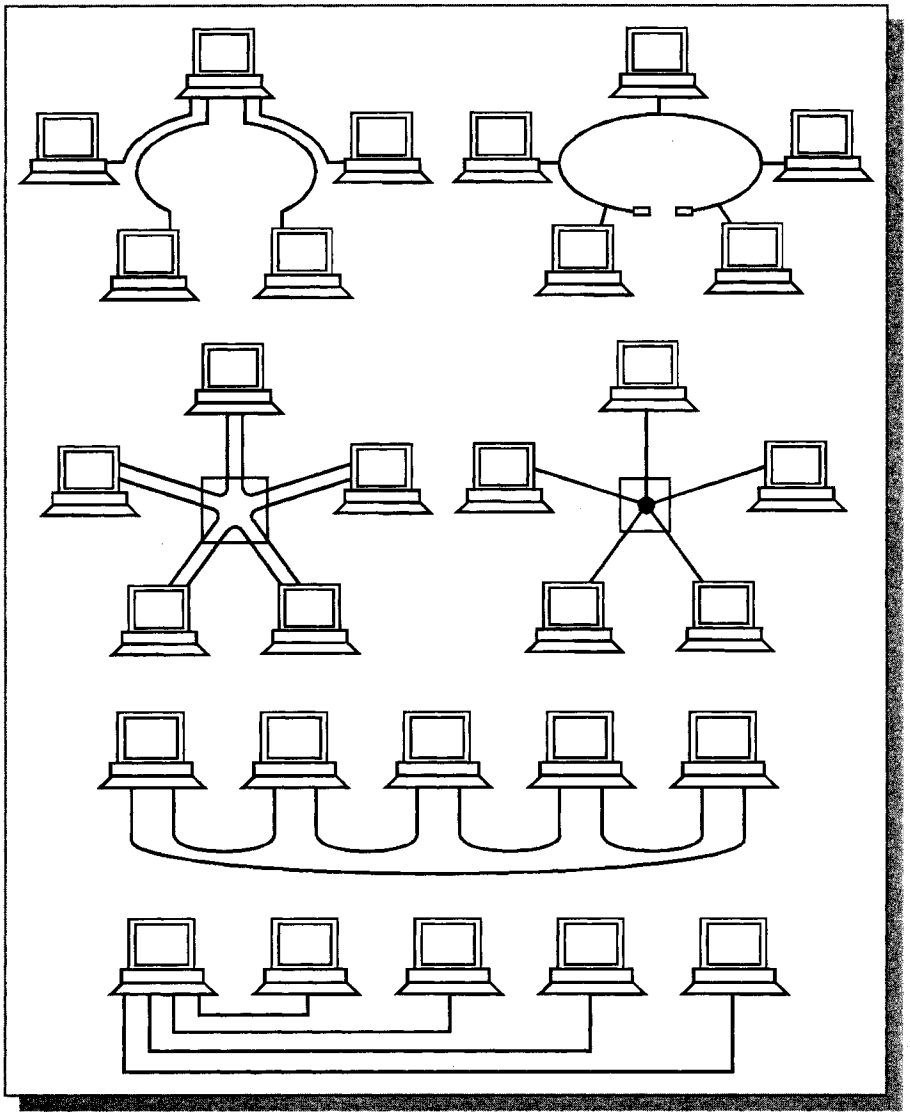


**Рис. 1.18.** Примеры использования разных топологий

права захвата сети (быть в этом смысле кольцом) и одновременно передавать всю информацию через выделенный компьютер (быть в этом смысле звездой). Или сеть с логической топологией шина может иметь физическую топологию «звезда» (пассивная) или «дерево» (пассивное).

Сеть с любой физической топологией, логической топологией, топологией управления обменом может считаться звездой в смысле информационной топологии, если она построена на основе одного сервера и нескольких клиентов, общающихся только с этим сервером. В данном случае справедливы все рассуждения о низкой отказоустойчивости сети к неполадкам центра (сервера). Точно так же любая сеть может быть названа шиной в информационном смысле, если она построена из компьютеров, являющихся одновременно как серверами, так и клиентами. Такая сеть будет мало чувствительна к отказам отдельных компьютеров.

Заканчивая обзор особенностей топологий локальных сетей, необходимо отметить, что топология все-таки не является основным фактором при выборе типа сети. Гораздо важнее, например, уровень стандартизации сети, скорость обмена, количество абонентов, стоимость оборудования, выбранное программное обеспечение. Но, с другой стороны, некоторые сети позволяют использовать разные топологии на разных уровнях. Этот выбор уже целиком ложится на пользователя, который должен учитывать все перечисленные в данном разделе соображения.

# Глава 2. Среды передачи информации локальных сетей

## Лекция 2. Типы линий связи локальных сетей

**В этой лекции говорится о типах, особенностях, принципах функционирования, достоинствах и недостатках, правилах использования линий связи, применяемых в локальных сетях.**

**Ключевые слова:** среда передачи, задержка распространения, затухание сигнала, полоса пропускания, коаксиальный кабель, витая пара, оптоволоконный кабель, радиоканал.

Средой передачи информации называются те линии связи (или каналы связи), по которым производится обмен информацией между компьютерами. В подавляющем большинстве компьютерных сетей (особенно локальных) используются проводные или кабельные каналы связи, хотя существуют и беспроводные сети, которые сейчас находят все более широкое применение, особенно в портативных компьютерах.

Информация в локальных сетях чаще всего передается в последовательном коде, то есть бит за битом. Такая передача медленнее и сложнее, чем при использовании параллельного кода. Однако надо учитывать то, что при более быстрой параллельной передаче (по нескольким кабелям одновременно) увеличивается количество соединительных кабелей в число раз, равное количеству разрядов параллельного кода (например, в 8 раз при 8-разрядном коде). Это совсем не мелочь, как может показаться на первый взгляд. При значительных расстояниях между абонентами сети стоимость кабеля вполне сравнима со стоимостью компьютеров и даже может превосходить ее. К тому же проложить один кабель (реже — два разнонаправленных) гораздо проще, чем 8, 16 или 32. Значительно дешевле обойдется также поиск повреждений и ремонт кабеля.

Но это еще не все. Передача на большие расстояния при любом типе кабеля требует сложной передающей и приемной аппаратуры, так как при этом необходимо формировать мощный сигнал на передающем конце и детектировать слабый сигнал на приемном конце. При последовательной передаче для этого требуется всего один передатчик и один приемник. При параллельной же количество требуемых передатчиков и приемников возрастает пропорционально разрядности используемого параллельного кода. В связи с этим, даже если разрабатывается сеть незначительной длины (порядка десятка метров), чаще всего выбирают последовательную передачу.

К тому же при параллельной передаче чрезвычайно важно, чтобы длины отдельных кабелей были точно равны друг другу. Иначе в результате прохождения по кабелям разной длины между сигналами на приемном конце образуется временной сдвиг, который может привести к сбоям в работе или даже к полной неработоспособности сети. Например, при скорости передачи 100 Мбит/с и длительности бита 10 нс этот временной сдвиг не должен превышать 5–10 нс. Такую величину сдвига дает разница в длинах кабелей в 1–2 метра. При длине кабеля 1000 метров это составляет 0,1–0,2%.

Надо отметить, что в некоторых высокоскоростных локальных сетях все-таки используют параллельную передачу по 2–4 кабелям, что позволяет при заданной скорости передачи применять более дешевые кабели с меньшей полосой пропускания. Но допустимая длина кабелей при этом не превышает сотни метров. Примером может служить сегмент 100BASE-T4 сети Fast Ethernet.

Промышленностью выпускается огромное количество типов кабелей, например, только одна крупнейшая кабельная компания Belden предлагает более 2000 их наименований. Но все кабели можно разделить на три большие группы:

- электрические (медные) кабели на основе *витых пар* проводов (twisted pair), которые делятся на экранированные (shielded twisted pair, STP) и неэкранированные (unshielded twisted pair, UTP);
- электрические (медные) *коаксиальные* кабели (coaxial cable);
- *оптоволоконные* кабели (fiber optic).

Каждый тип кабеля имеет свои преимущества и недостатки, так что при выборе надо учитывать как особенности решаемой задачи, так и особенности конкретной сети, в том числе и используемую топологию.

Можно выделить следующие основные параметры кабелей, принципиально важные для использования в локальных сетях:

- *Полоса пропускания* кабеля (частотный диапазон сигналов, пропускаемых кабелем) и затухание сигнала в кабеле. Два этих параметра тесно связаны между собой, так как с ростом частоты сигнала растет затухание сигнала. Надо выбирать кабель, который на заданной частоте сигнала имеет приемлемое затухание. Или же надо выбирать частоту сигнала, на которой затухание еще приемлемо. Затухание измеряется в децибелах и пропорционально длине кабеля.
- *Помехозащищенность* кабеля и обеспечиваемая им *секретность* передачи информации. Эти два взаимосвязанных параметра показывают, как кабель взаимодействует с окружающей средой, то есть, как он реагирует на внешние помехи, и насколько просто прослушать информацию, передаваемую по кабелю.

- *Скорость распространения сигнала* по кабелю или обратный параметр – *задержка сигнала* на метр длины кабеля. Этот параметр имеет принципиальное значение при выборе длины сети. Типичные величины скорости распространения сигнала – от 0,6 до 0,8 от скорости распространения света в вакууме. Соответственно типичные величины задержек – от 4 до 5 нс/м.
- Для электрических кабелей очень важна величина *волнового сопротивления* кабеля. Волновое сопротивление важно учитывать при согласовании кабеля для предотвращения отражения сигнала от концов кабеля. Волновое сопротивление зависит от формы и взаиморасположения проводников, от технологии изготовления и материала диэлектрика кабеля. Типичные значения волнового сопротивления – от 50 до 150 Ом.

В настоящее время действуют следующие стандарты на кабели:

- EIA/TIA 568 (Commercial Building Telecommunications Cabling Standard) – американский;
- ISO/IEC IS 11801 (Generic cabling for customer premises) – международный;
- CENELEC EN 50173 (Generic cabling systems) – европейский.

Эти стандарты описывают практически одинаковые кабельные системы, но отличаются терминологией и нормами на параметры. В данной работе предлагается придерживаться терминологии стандарта EIA/TIA 568.

## Кабели на основе витых пар

Витые пары проводов используются в дешевых и сегодня, пожалуй, самых популярных кабелях. Кабель на основе витых пар представляет собой несколько пар скрученных попарно изолированных медных проводов в единой диэлектрической (пластиковой) оболочке. Он довольно гибкий и удобный для прокладки. Скручивание проводов позволяет свести к минимуму индуктивные наводки кабелей друг на друга и снизить влияние переходных процессов.

Обычно в кабель входит две (рис. 2.1) или четыре витые пары.

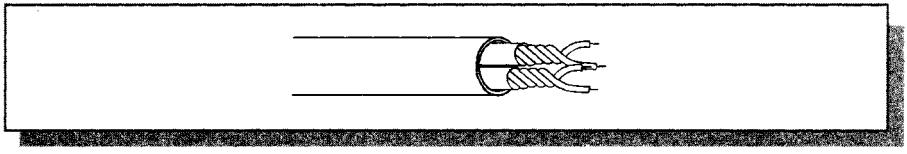


**Рис. 2.1.** Кабель с витыми парами

Неэкранированные витые пары характеризуются слабой защищенностью от внешних электромагнитных помех, а также от подслушивания, которое может осуществляться с целью, например, промышленного шпионажа. Причем перехват передаваемой по сети информации возможен как с помо-

щью контактного метода (например, посредством двух иголок, воткнутых в кабель), так и с помощью бесконтактного метода, сводящегося к радиоперехвату излучаемых кабелем электромагнитных полей. Причем действие помех и величина излучения вовне увеличивается с ростом длины кабеля. Для устранения этих недостатков применяется экранирование кабелей.

В случае экранированной витой пары STP каждая из витых пар помещается в металлическую оплетку-экран для уменьшения излучений кабеля, защиты от внешних электромагнитных помех и снижения взаимного влияния пар проводов друг на друга (crosstalk – перекрестные наводки). Для того чтобы экран защищал от помех, он должен быть обязательно заземлен. Естественно, экранированная витая пара заметно дороже, чем неэкранированная. Ее использование требует специальных экранированных разъемов. Поэтому встречается она значительно реже, чем неэкранированная витая пара.

Основные достоинства неэкранированных витых пар – простота монтажа разъемов на концах кабеля, а также ремонта любых повреждений по сравнению с другими типами кабеля. Все остальные характеристики у них хуже, чем у других кабелей. Например, при заданной скорости передачи затухание сигнала (уменьшение его уровня по мере прохождения по кабелю) у них больше, чем у коаксиальных кабелей. Если учесть еще низкую помехозащищенность, то понятно, почему линии связи на основе витых пар, как правило, довольно короткие (обычно в пределах 100 метров). В настоящее время витая пара используется для передачи информации на скоростях до 1000 Мбит/с, хотя технические проблемы, возникающие при таких скоростях, крайне сложны.

Согласно стандарту EIA/TIA 568, существуют пять основных и две дополнительные категории кабелей на основе неэкранированной витой пары (UTP):

- Кабель категории 1 – это обычный телефонный кабель (пары проводов — не витые), по которому можно передавать только речь. Этот тип кабеля имеет большой разброс параметров (волнового сопротивления, полосы пропускания, перекрестных наводок).
- Кабель категории 2 – это кабель из витых пар для передачи данных в полосе частот до 1 МГц. Кабель не тестируется на уровень перекрестных наводок. В настоящее время он используется очень редко. Стандарт EIA/TIA 568 не различает кабели категорий 1 и 2.
- Кабель категории 3 – это кабель для передачи данных в полосе часто до 16 МГц, состоящий из витых пар с девятью витками проводов на метр длины. Кабель тестируется на все параметры и имеет волновое сопротивление 100 Ом. Это самый простой тип кабелей, рекомендованный стандартом для локальных сетей. Еще недавно он был самым распространенным, но сейчас повсеместно вытесняется кабелем категории 5.

- Кабель категории 4 – это кабель, передающий данные в полосе частот до 20 МГц. Используется редко, так как не слишком заметно отличается от категории 3. Стандартом рекомендуется вместо кабеля категории 3 переходить сразу на кабель категории 5. Кабель категории 4 тестируется на все параметры и имеет волновое сопротивление 100 Ом. Кабель был создан для работы в сетях по стандарту IEEE 802.5.
- Кабель категории 5 – в настоящее время самый совершенный кабель, рассчитанный на передачу данных в полосе частот до 100 МГц. Состоит из витых пар, имеющих не менее 27 витков на метр длины (8 витков на фут). Кабель тестируется на все параметры и имеет волновое сопротивление 100 Ом. Рекомендуется применять его в современных высокоскоростных сетях типа Fast Ethernet и TPFDDI. Кабель категории 5 примерно на 30–50% дороже, чем кабель категории 3.
- Кабель категории 6 – перспективный тип кабеля для передачи данных в полосе частот до 200 (или 250) МГц.
- Кабель категории 7 – перспективный тип кабеля для передачи данных в полосе частот до 600 МГц.

Согласно стандарту EIA/TIA 568, полное волновое сопротивление наиболее совершенных кабелей категорий 3, 4 и 5 должно составлять 100 Ом±15% в частотном диапазоне от 1 МГц до максимальной частоты кабеля. Требования не очень жесткие: величина волнового сопротивления может находиться в диапазоне от 85 до 115 Ом. Здесь же следует отметить, что волновое сопротивление экранированной витой пары STP по стандарту должно быть равным 150 Ом±15%. Для согласования сопротивлений кабеля и оборудования в случае их несовпадения применяют согласующие трансформаторы (Balun). Существует также экранированная витая пара с волновым сопротивлением 100 Ом, но используется она довольно редко.

Второй важнейший параметр, задаваемый стандартом, – это максимальное затухание сигнала, передаваемого по кабелю, на разных частотах. В таблице 2.1 приведены предельные значения величины затухания в децибелах для кабелей категорий 3, 4 и 5 на расстояние 1000 футов (то есть 305 метров) при нормальной температуре окружающей среды 20°С.

Из таблицы видно, что величины затухания на частотах, близких к предельным, для всех кабелей очень значительны. Даже на небольших расстояниях сигнал ослабляется в десятки и сотни раз, что предъявляет высокие требования к приемникам сигнала.

Еще один специфический параметр, определяемый стандартом, это величина так называемой перекрестной наводки на ближнем конце (NEXT – Near End CrossTalk). Он характеризует влияние разных проводов в кабеле друг на друга. Суть данного параметра иллюстрируется на рис. 2.2. Сигнал, передаваемый по одной из витых пар кабеля (верхняя пара), наводит индуктивную помеху на другую (нижнюю) витую пару кабеля. Две витые пары в сети обычно пе-

**Табл. 2.1.** Максимальное затухание в кабелях

| Частота, МГц | Максимальное затухание, дБ | | |
|---|---|---|---|
| | Категория 3 | Категория 4 | Категория 5 |
| 0,064 | 2,8 | 2,3 | 2,2 |
| 0,256 | 4,0 | 3,4 | 3,2 |
| 0,512 | 5,6 | 4,6 | 4,5 |
| 0,772 | 6,8 | 5,7 | 5,5 |
| 1,0 | 7,8 | 6,5 | 6,3 |
| 4,0 | 17 | 13 | 13 |
| 8,0 | 26 | 19 | 18 |
| 10,0 | 30 | 22 | 20 |
| 16,0 | 40 | 27 | 25 |
| 20,0 | — | 31 | 28 |
| 25,0 | — | — | 32 |
| 31,25 | — | — | 36 |
| 62,5 | — | — | 52 |
| 100 | — | — | 67 |

редают информацию в разные стороны, поэтому наиболее важна наводка на ближнем конце воспринимающей пары (нижней на рисунке), так как именно там находится приемник информации. Перекрестная наводка на дальнем конце (FEXT – Far End CrossTalk) не имеет такого большого значения.

В таблице 2.2 представлены значения допустимой перекрестной наводки на ближнем конце для кабелей категорий 3, 4 и 5 на различных ча-

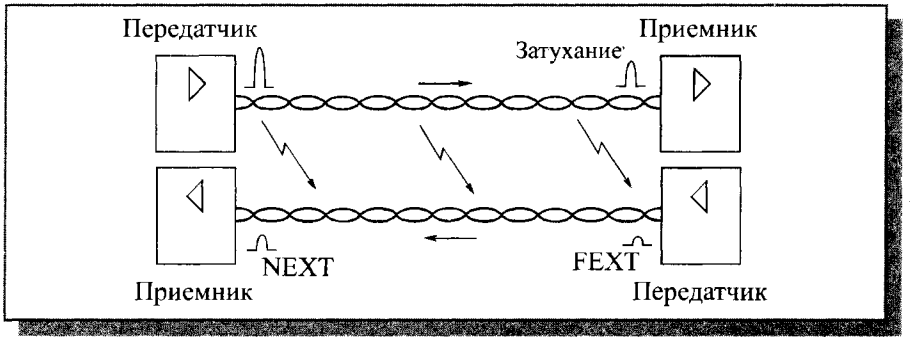



**Рис. 2.2.** Перекрестные помехи в кабелях на витых парах

**Табл. 2.2.** Допустимые уровни перекрестных наводок NEXT

| Частота, МГц | Перекрестная наводка на ближнем конце, дБ | | |
|---|---|---|---|
| | Категория 3 | Категория 4 | Категория 5 |
| 0,150- | 54 | -68 | -74 |
| 0,772 | -43 | -58 | -64 |
| 1,0 | -41 | -56 | -62 |
| 4,0 | -32 | -47 | -53 |
| 8,0 | -28 | -42 | -48 |
| 10,0 | -26 | -41 | -47 |
| 16,0 | -23 | -38 | -44 |
| 20,0 | — | -36 | -42 |
| 25,0 | — | — | -41 |
| 31,25 | — | — | -40 |
| 62,5 | — | — | -35 |
| 100,0 | — | — | -32 |

стотах сигнала. Естественно, более качественные кабели обеспечивают меньшую величину перекрестной наводки.

Стандарт определяет также максимально допустимую величину рабочей емкости каждой из витых пар кабелей категории 4 и 5. Она должна составлять не более 17 нФ на 305 метров (1000 футов) при частоте сигнала 1 кГц и температуре окружающей среды 20°С.

Для присоединения витых пар используются разъемы (коннекторы) типа RJ-45, похожие на разъемы, используемые в телефонах (RJ-11), но несколько большие по размеру. Разъемы RJ-45 имеют восемь контактов вместо четырех в случае RJ-11. Присоединяются разъемы к кабелю с помощью специальных обжимных инструментов. При этом золоченые игольчатые контакты разъема прокалывают изоляцию каждого провода, входят между его жилами и обеспечивают надежное и качественное соединение. Надо учитывать, что при установке разъемов стандартом допускается расплетение витой пары кабеля на длину не более одного сантиметра.

Чаще всего витые пары используются для передачи данных в одном направлении (точка-точка), то есть в топологиях типа «звезда» или «кольцо». Топология «шина» обычно ориентируется на коаксиальный кабель. Поэтому внешние терминаторы, согласующие неподключенные концы кабеля, для витых пар практически никогда не применяются.

Кабели выпускаются с двумя типами внешних оболочек:

- Кабель в поливинилхлоридной (ПВХ, PVC) оболочке дешевле и предназначен для работы в сравнительно комфортных условиях эксплуатации.
- Кабель в тефлоновой оболочке дороже и предназначен для более жестких условий эксплуатации.

Кабель в ПВХ–оболочке называется еще non-plenum, а в тефлоновой – plenum. Термин plenum обозначает в данном случае пространство под фальшполом и над подвесным потолком, где удобно размещать кабели сети. Для прокладки в этих скрытых от глаз пространствах как раз удобнее кабель в тефлоновой оболочке, который, в частности, горит гораздо хуже, чем ПВХ–кабель, и не выделяет при этом ядовитых газов в большом количестве.

Еще один важный параметр любого кабеля, который жестко не определяется стандартом, но может существенно повлиять на работоспособность сети, – это скорость распространения сигнала в кабеле или, другими словами, задержка распространения сигнала в кабеле в расчете на единицу длины.

Производители кабелей иногда указывают величину задержки на метр длины, а иногда – скорость распространения сигнала относительно скорости света (или NVP – Nominal Velocity of Propagation, как ее часто называют в документации). Связаны эти две величины простой формулой:

$$t_з = 1/(3 \times 10^{10} \times NVP)$$

где $t_з$ – величина задержки на метр длины кабеля в наносекундах. Например, если $NVP = 0,65$ (65% от скорости света), то задержка $t_з$ будет равна 5,13 нс/м. Типичная величина задержки большинства современных кабелей составляет около 4–5 нс/м.

В таблице 2.3 приведены величины NVP и задержек на метр длины (в наносекундах) для некоторых типов кабеля двух самых известных компаний-производителей AT&T и Belden.

Стоит также отметить, что каждый из проводов, входящих в кабель на основе витых пар, как правило, имеет свой цвет изоляции, что существенно упрощает монтаж разъемов, особенно в том случае, когда концы кабеля находятся в разных комнатах, и контроль с помощью приборов затруднен.

Примером кабеля с экранированными витыми парами может служить кабель STP IBM типа 1, который включает в себя две экранированные витые пары AWG типа 22. Волновое сопротивление каждой пары составляет 150 Ом. Для этого кабеля применяются специальные разъемы, отличающиеся от разъемов для неэкранированной витой пары (например, DB9). Имеются и экранированные версии разъема RJ-45.

## Коаксиальные кабели

Коаксиальный кабель представляет собой электрический кабель, состоящий из центрального медного провода и металлической оплетки (эк-

дарт EIA/TIA-568 включает в себя только один тип коаксиального кабеля, применяемый в сети Ethernet.

Основное применение коаксиальный кабель находит в сетях с топологией типа «шина». При этом на концах кабеля обязательно должны устанавливаться терминаторы для предотвращения внутренних отражений сигнала, причем один (и только один!) из терминаторов должен быть заземлен. Без заземления металлическая оплетка не защищает сеть от внешних электромагнитных помех и не снижает излучение передаваемой по сети информации во внешнюю среду. Но при заземлении оплетки в двух или более точках из строя может выйти не только сетевое оборудование, но и компьютеры, подключенные к сети. Терминаторы должны быть обязательно согласованы с кабелем, необходимо, чтобы их сопротивление равнялось волновому сопротивлению кабеля. Например, если используется 50-омный кабель, для него подходят только 50-омные терминаторы.

Реже коаксиальные кабели применяются в сетях с топологией «звезда» (например, пассивная звезда в сети Arcnet). В этом случае проблема согласования существенно упрощается, так как внешних терминаторов на свободных концах не требуется.

Волновое сопротивление кабеля указывается в сопроводительной документации. Чаще всего в локальных сетях применяются 50-омные (RG-58, RG-11, RG-8) и 93-омные кабели (RG-62). Распространенные в телевизионной технике 75-омные кабели в локальных сетях не используются. Марок коаксиального кабеля немного. Он не считается особо перспективным. Не случайно в сети Fast Ethernet не предусмотрено применение коаксиальных кабелей. Однако во многих случаях классическая шинная топология (а не пассивная звезда) очень удобна. Как уже отмечалось, она не требует применения дополнительных устройств – концентраторов.

Существует два основных типа коаксиального кабеля:

- тонкий (thin) кабель, имеющий диаметр около 0,5 см, более гибкий;
- толстый (thick) кабель, диаметром около 1 см, значительно более жесткий. Он представляет собой классический вариант коаксиального кабеля, который уже почти полностью вытеснен современным тонким кабелем.

Тонкий кабель используется для передачи на меньшие расстояния, чем толстый, поскольку сигнал в нем затухает сильнее. Зато с тонким кабелем гораздо удобнее работать: его можно оперативно проложить к каждому компьютеру, а толстый требует жесткой фиксации на стене помещения. Подключение к тонкому кабелю (с помощью разъемов BNC байонетного типа) проще и не требует дополнительного оборудования. А для подключения к толстому кабелю надо использовать специальные довольно дорогие устройства, прокалывающие его оболочки и устанавливающие контакт как с центральной жилой, так и с экраном. Толстый кабель примерно вдвое дороже, чем тонкий, поэтому тонкий кабель применяется гораздо чаще.

**Табл. 2.3.** Временные характеристики некоторых кабелей

| Фирма | Марка | Категория | Оболочка | NVP | Задержка |
|---|---|---|---|---|---|
| AT&T | 1010 | 3 | non-plenum | 0,67 | 4,98 |
| AT&T | 1041 | 4 | non-plenum | 0,70 | 4,76 |
| AT&T | 1061 | 5 | non-plenum | 0,70 | 4,76 |
| AT&T | 2010 | 3 | plenum | 0,70 | 4,76 |
| AT&T | 2041 | 4 | plenum | 0,75 | 4,44 |
| AT&T | 2061 | 5 | plenum | 0,75 | 4,44 |
| Belden | 1229A | 3 | non-plenum | 0,69 | 4,83 |
| Belden | 1455A | 4 | non-plenum | 0,72 | 4,63 |
| Belden | 1583A | 5 | non-plenum | 0,72 | 4,63 |
| Belden | 1245A2 | 3 | plenum | 0,69 | 4,83 |
| Belden | 1457A | 4 | plenum | 0,75 | 4,44 |
| Belden | 1585A | 5 | plenum | 0,75 | 4,44 |

рана), разделенных между собой слоем диэлектрика (внутренней изоляции) и помещенных в общую внешнюю оболочку (рис. 2.3).

Коаксиальный кабель до недавнего времени был очень популярен, что связано с его высокой помехозащищенностью (благодаря металлической оплетке), более широкими, чем в случае витой пары, полосами пропускания (свыше 1ГГц), а также большими допустимыми расстояниями передачи (до километра). К нему труднее механически подключиться для несанкционированного прослушивания сети, он дает также заметно меньше электромагнитных излучений вовне. Однако монтаж и ремонт коаксиального кабеля существенно сложнее, чем витой пары, а стоимость его выше (он дороже примерно в 1,5–3 раза). Сложнее и установка разъемов на концах кабеля. Сейчас его применяют реже, чем витую пару. Стан-

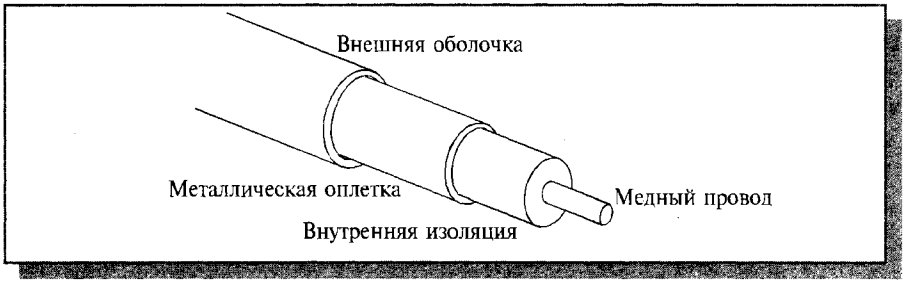



**Рис. 2.3.** Коаксиальный кабель

Как и в случае витых пар, важным параметром коаксиального кабеля является тип его внешней оболочки. Точно так же в данном случае применяются как non-plenum (PVC), так и plenum–кабели. Естественно, тефлоновый кабель дороже поливинилхлоридного. Обычно тип оболочки можно отличить по окраске (например, для PVC кабеля фирма Belden использует желтый цвет, а для тефлонового – оранжевый).

Типичные величины задержки распространения сигнала в коаксиальном кабеле составляют для тонкого кабеля около 5 нс/м, а для толстого – около 4,5 нс/м.

Существуют варианты коаксиального кабеля с двойным экраном (один экран расположен внутри другого и отделен от него дополнительным слоем изоляции). Такие кабели имеют лучшую помехозащищенность и защиту от прослушивания, но они немного дороже обычных.

В настоящее время считается, что коаксиальный кабель устарел, в большинстве случаев его вполне может заменить витая пара или оптоволоконный кабель. И новые стандарты на кабельные системы уже не включают его в перечень типов кабелей.

## Оптоволоконные кабели

Оптоволоконный (он же волоконно-оптический) кабель – это принципиально иной тип кабеля по сравнению с рассмотренными двумя типами электрического или медного кабеля. Информация по нему передается не электрическим сигналом, а световым. Главный его элемент – это прозрачное стекловолокно, по которому свет проходит на огромные расстояния (до десятков километров) с незначительным ослаблением.

Структура оптоволоконного кабеля очень проста и похожа на структуру коаксиального электрического кабеля (рис. 2.4). Только вместо центрального медного провода здесь используется тонкое (диаметром около 1–10 мкм) стекловолокно, а вместо внутренней изоляции – стеклянная или пластиковая оболочка, не позволяющая свету выходить за пределы стекловолокна. В данном случае речь идет о режиме так называемого пол-

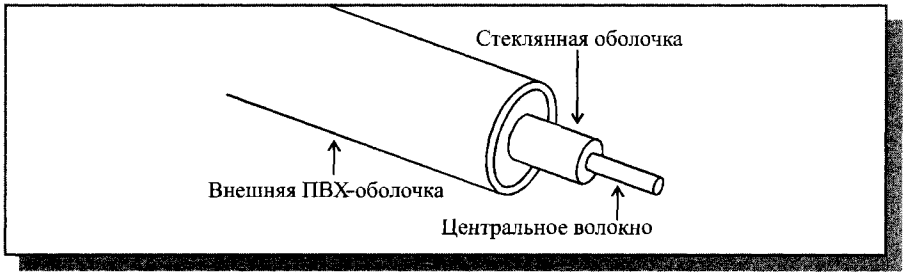



**Рис. 2.4.** Структура оптоволоконного кабеля

ного внутреннего отражения света от границы двух веществ с разными коэффициентами преломления (у стеклянной оболочки коэффициент преломления значительно ниже, чем у центрального волокна). Металлическая оплетка кабеля обычно отсутствует, так как экранирование от внешних электромагнитных помех здесь не требуется. Однако иногда ее все-таки применяют для механической защиты от окружающей среды (такой кабель иногда называют броневым, он может объединять под одной оболочкой несколько оптоволоконных кабелей).

Оптоволоконный кабель обладает исключительными характеристиками по помехозащищенности и секретности передаваемой информации. Никакие внешние электромагнитные помехи в принципе не способны исказить световой сигнал, а сам сигнал не порождает внешних электромагнитных излучений. Подключиться к этому типу кабеля для несанкционированного прослушивания сети практически невозможно, так как при этом нарушается целостность кабеля. Теоретически возможная полоса пропускания такого кабеля достигает величины $10^{12}$ Гц, то есть 1000 ГГц, что несравнимо выше, чем у электрических кабелей. Стоимость оптоволоконного кабеля постоянно снижается и сейчас примерно равна стоимости тонкого коаксиального кабеля.

Типичная величина затухания сигнала в оптоволоконных кабелях на частотах, используемых в локальных сетях, составляет от 5 до 20 дБ/км, что примерно соответствует показателям электрических кабелей на низких частотах. Но в случае оптоволоконного кабеля при росте частоты передаваемого сигнала затухание увеличивается очень незначительно, и на больших частотах (особенно свыше 200 МГц) его преимущества перед электрическим кабелем неоспоримы, у него просто нет конкурентов.

Однако оптоволоконный кабель имеет и некоторые недостатки.

Самый главный из них – высокая сложность монтажа (при установке разъемов необходима микронная точность, от точности скола стекловолокна и степени его полировки сильно зависит затухание в разъеме). Для установки разъемов применяют сварку или склеивание с помощью специального геля, имеющего такой же коэффициент преломления света, что и стекловолокно. В любом случае для этого нужна высокая квалификация персонала и специальные инструменты. Поэтому чаще всего оптоволоконный кабель продается в виде заранее нарезанных кусков разной длины, на обоих концах которых уже установлены разъемы нужного типа. Следует помнить, что некачественная установка разъема резко снижает допустимую длину кабеля, определяемую затуханием.

Также надо помнить, что использование оптоволоконного кабеля требует специальных оптических приемников и передатчиков, преобразующих световые сигналы в электрические и обратно, что порой существенно увеличивает стоимость сети в целом.

Оптоволоконные кабели допускают разветвление сигналов (для этого производятся специальные пассивные *разветвители* (couplers) на 2–8 каналов), но, как правило, их используют для передачи данных только в одном направлении между одним передатчиком и одним приемником. Ведь любое разветвление неизбежно сильно ослабляет световой сигнал, и если разветвлений будет много, то свет может просто не дойти до конца сети. Кроме того, в разветвителе есть и внутренние потери, так что суммарная мощность сигнала на выходе меньше входной мощности.

Оптоволоконный кабель менее прочен и гибок, чем электрический. Типичная величина допустимого радиуса изгиба составляет около 10–20 см, при меньших радиусах изгиба центральное волокно может сломаться. Плохо переносит кабель и механическое растяжение, а также раздавливающие воздействия.

Чувствителен оптоволоконный кабель и к ионизирующим излучениям, из-за которых снижается прозрачность стекловолокна, то есть увеличивается затухание сигнала. Резкие перепады температуры также негативно сказываются на нем — стекловолокно может треснуть.

Применяют оптоволоконный кабель только в сетях с топологией «звезда» и «кольцо». Никаких проблем согласования и заземления в данном случае не существует. Кабель обеспечивает идеальную гальваническую развязку компьютеров сети. В будущем этот тип кабеля, вероятно, вытеснит электрические кабели или, во всяком случае, сильно потеснит их. Запасы меди на планете истощаются, а сырья для производства стекла более чем достаточно.

Существуют два различных типа оптоволоконного кабеля:

- *многомодовый* или *мультимодовый* кабель, более дешевый, но менее качественный;
- *одномодовый* кабель, более дорогой, но имеет лучшие характеристики по сравнению с первым.

Суть различия между этими двумя типами сводится к разным режимам прохождения световых лучей в кабеле.

В одномодовом кабеле практически все лучи проходят один и тот же путь, в результате чего они достигают приемника одновременно, и форма сигнала почти не искажается (рис. 2.5). Одномодовый кабель имеет диаметр центрального волокна около 1,3 мКм и передает свет только с такой же длиной волны (1,3 мКм). Дисперсия и потери сигнала при этом очень незначительны, что позволяет передавать сигналы на значительно большее

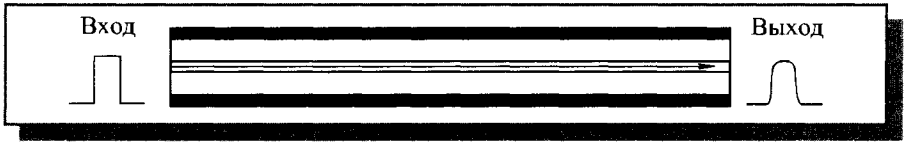



**Рис. 2.5.** Распространение света в одномодовом кабеле

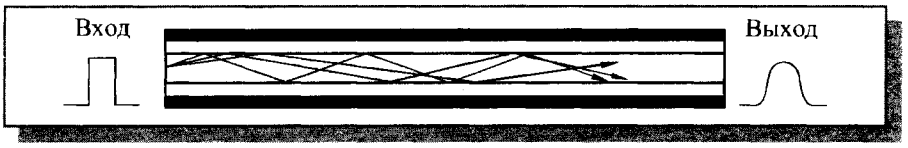



**Рис. 2.6.** Распространение света в многомодовом кабеле

расстояние, чем в случае применения многомодового кабеля. Для одномодового кабеля применяются лазерные приемопередатчики, использующие свет исключительно с требуемой длиной волны. Такие приемопередатчики пока еще сравнительно дороги и не долговечны. Однако в перспективе одномодовый кабель должен стать основным типом благодаря своим прекрасным характеристикам. К тому же лазеры имеют большее быстродействие, чем обычные светодиоды. Затухание сигнала в одномодовом кабеле составляет около 5 дБ/км и может быть даже снижено до 1 дБ/км.

В многомодовом кабеле траектории световых лучей имеют заметный разброс, в результате чего форма сигнала на приемном конце кабеля искажается (рис. 2.6). Центральное волокно имеет диаметр 62,5 мКм, а диаметр внешней оболочки — 125 мКм (это иногда обозначается как 62,5/125). Для передачи используется обычный (не лазерный) светодиод, что снижает стоимость и увеличивает срок службы приемопередатчиков по сравнению с одномодовым кабелем. Длина волны света в многомодовом кабеле равна 0,85 мКм, при этом наблюдается разброс длин волн около 30–50 нм. Допустимая длина кабеля составляет 2–5 км. Многомодовый кабель – это основной тип оптоволоконного кабеля в настоящее время, так как он дешевле и доступнее. Затухание в многомодовом кабеле больше, чем в одномодовом, и составляет 5–20 дБ/км.

Типичная величина задержки для наиболее распространенных кабелей составляет около 4–5 нс/м, что близко к величине задержки в электрических кабелях.

Оптоволоконные кабели, как и электрические, выпускаются в исполнении plenum и non-plenum.

## Бескабельные каналы связи

Кроме кабельных каналов, в компьютерных сетях иногда используются также бескабельные каналы. Их главное преимущество состоит в том, что не требуется никакой прокладки проводов (не надо делать отверстий в стенах, закреплять кабель в трубах и желобах, прокладывать его под фальшполами, над подвесными потолками или в вентиляционных шахтах, искать и устранять повреждения). К тому же компьютеры сети можно легко перемещать в пределах комнаты или здания, так как они ни к чему не привязаны.

Радиоканал использует передачу информации по радиоволнам, поэтому теоретически он может обеспечить связь на многие десятки, сотни и даже тысячи километров. Скорость передачи достигает десятков мегабит в секунду (здесь многое зависит от выбранной длины волны и способа кодирования).

Особенность радиоканала состоит в том, что сигнал свободно излучается в эфир, он не замкнут в кабель, поэтому возникают проблемы совместимости с другими источниками радиоволн (радио- и телевещательными станциями, радарами, радиолюбительскими и профессиональными передатчиками и т.д.). В радиоканале используется передача в узком диапазоне частот и модуляция информационным сигналом сигнала несущей частоты.

Главным недостатком радиоканала является его плохая защита от прослушивания, так как радиоволны распространяются неконтролируемо. Другой большой недостаток радиоканала – слабая помехозащищенность.

Для локальных беспроводных сетей (WLAN – Wireless LAN) в настоящее время применяются подключения по радиоканалу на небольших расстояниях (обычно до 100 метров) и в пределах прямой видимости. Чаще всего используются два частотных диапазона – 2,4 ГГц и 5 ГГц. Скорость передачи – до 54 Мбит/с. Распространен вариант со скоростью 11 Мбит/с.

Сети WLAN позволяют устанавливать беспроводные сетевые соединения на ограниченной территории (обычно внутри офисного или университетского здания или в таких общественных местах, как аэропорты). Они могут использоваться во временных офисах или в других местах, где прокладка кабелей неосуществима, а также в качестве дополнения к имеющейся проводной локальной сети, призванного обеспечить пользователям возможность работать, перемещаясь по зданию.

Популярная технология Wi-Fi (Wireless Fidelity) позволяет организовать связь между компьютерами числом от 2 до 15 с помощью концентратора (называемого *точка доступа*, Access Point, AP), или нескольких концентраторов, если компьютеров от 10 до 50. Кроме того, эта технология дает возможность связать две локальные сети на расстоянии до 25 километров с помощью мощных беспроводных мостов. Для примера на рис. 2.7 показано объединение компьютеров с помощью одной точки доступа. Важно, что многие

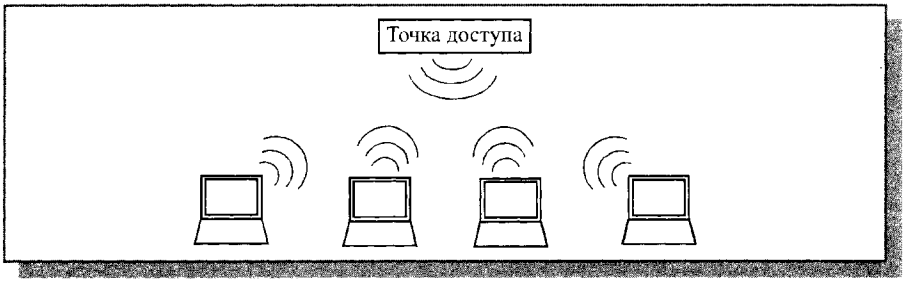



**Рис. 2.7.** Объединение компьютеров с помощью технологии Wi-Fi

мобильные компьютеры (ноутбуки) уже имеют встроенный контроллер Wi-Fi, что существенно упрощает их подключение к беспроводной сети.

Радиоканал широко применяется в глобальных сетях как для наземной, так и для спутниковой связи. В этом применении у радиоканала нет конкурентов, так как радиоволны могут дойти до любой точки земного шара.

**Инфракрасный канал** также не требует соединительных проводов, так как использует для связи инфракрасное излучение (подобно пульту дистанционного управления домашнего телевизора). Главное его преимущество по сравнению с радиоканалом – нечувствительность к электромагнитным помехам, что позволяет применять его, например, в производственных условиях, где всегда много помех от силового оборудования. Правда, в данном случае требуется довольно высокая мощность передачи, чтобы не влияли никакие другие источники теплового (инфракрасного) излучения. Плохо работает инфракрасная связь и в условиях сильной запыленности воздуха.

Скорость передачи информации по инфракрасному каналу обычно не превышает 5–10 Мбит/с, но при использовании инфракрасных лазеров может быть достигнута скорость более 100 Мбит/с. Секретность передаваемой информации, как и в случае радиоканала, не достигается. Также требуются сравнительно дорогие приемники и передатчики. Все это приводит к тому, что применяют инфракрасные каналы в локальных сетях довольно редко. В основном они используются для связи компьютеров с периферией (интерфейс IrDA).

Инфракрасные каналы делятся на две группы:

- Каналы прямой видимости, в которых связь осуществляется на лучах, идущих непосредственно от передатчика к приемнику. При этом связь возможна только при отсутствии препятствий между компьютерами сети. Зато протяженность канала прямой видимости может достигать нескольких километров.
- Каналы на рассеянном излучении, которые работают на сигналах, отраженных от стен, потолка, пола и других препятствий. Препятствия в данном случае — не помеха, но связь может осуществляться только в пределах одного помещения.

Если говорить о возможных топологиях, то наиболее естественно все беспроводные каналы связи подходят для топологии типа «шина», в которой информация передается одновременно всем абонентам. Но при использовании узконаправленной передачи и/или частотного разделения по каналам можно реализовать любые топологии (кольцо, звезда, комбинированные топологии) как на радиоканале, так и на инфракрасном канале.

# Лекция 3. Подключение линий связи и коды передачи информации

**В этой лекции рассказывается о принципах подключения электрических линий связи в локальных сетях, методах их согласования, экранирования и гальванической развязки, а также о кодах передачи информации.**

**Ключевые слова:** согласование, волновое сопротивление, экранирование, дифференциальная передача, гальваническая развязка, кодирование информации, самосинхронизирующиеся коды, модуляция.

## Согласование, экранирование и гальваническая развязка линий связи

Как уже отмечалось, электрические линии связи (витые пары, коаксиальные кабели) требуют проведения специальных мер, без которых невозможна не только безошибочная передача данных, но и вообще любое функционирование сети. Оптоволоконные кабели решают все подобные проблемы автоматически.

**Согласование** электрических линий связи применяется для обеспечения нормального прохождения сигнала по длинной линии без отражений и искажений. Следует отметить, что в локальных сетях кабель работает в режиме длинной линии даже при минимальных расстояниях между компьютерами, так как скорости передачи информации и частотный спектр сигнала очень велики.

Принцип согласования кабеля прост: на его концах необходимо установить согласующие резисторы (терминаторы) с сопротивлением, равным волновому сопротивлению используемого кабеля.

Как уже упоминалось, волновое сопротивление – это параметр данного типа кабеля, зависящий только от его устройства (сечения, количества и формы проводников, толщины и материала изоляции и т.д.). Величина волнового сопротивления обязательно указывается в сопроводительной документации на кабель и составляет обычно от 50–100 Ом для коаксиального кабеля до 100–150 Ом для витой пары или плоского многопроводного кабеля. Точное значение волнового сопротивления легко можно измерить с помощью генератора прямоугольных импульсов и осциллографа как раз по отсутствию искажения формы передаваемого по кабелю импульса. Обычно требуется, чтобы отклонение величины согласующего резистора не превышало 10% в ту или другую сторону.

Если согласующее, нагрузочное сопротивление $R_н$ меньше волнового сопротивления кабеля $R_в$, то фронт передаваемого прямоугольного

импульса на приемном конце будет затянут. Если же Rн больше Rв, то на фронте будет колебательный процесс (рис.3.1).

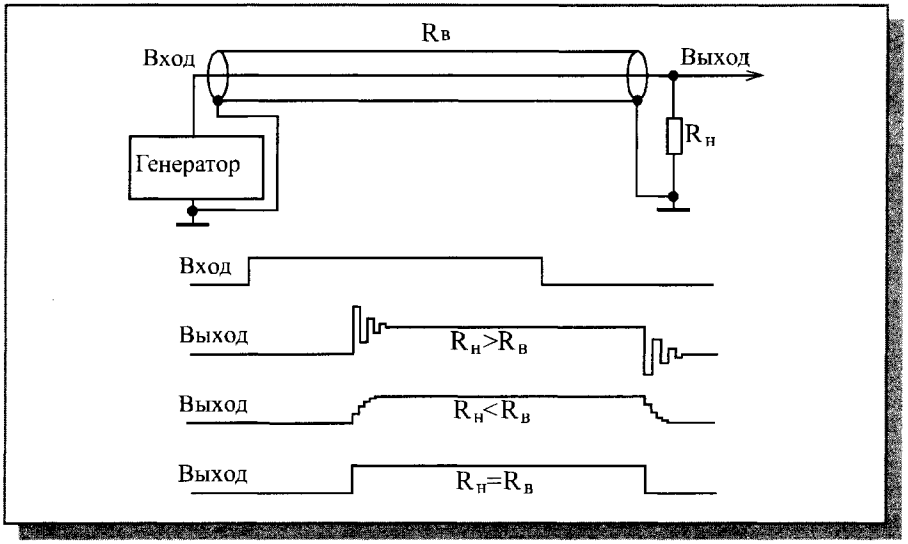



**Рис. 3.1.** Передача сигналов по электрическому кабелю

Сетевые адаптеры, их приемники и передатчики специально рассчитываются на работу с данным типом кабеля с известным волновым сопротивлением. Поэтому даже при идеально согласованном на концах кабеля, волновое сопротивление которого существенно отличается от стандартного, сеть, скорее всего, работать не будет или будет работать со сбоями.

Здесь же стоит упомянуть о том, что сигналы с пологими фронтами передаются по длинному электрическому кабелю лучше, чем сигналы с крутыми фронтами. Их форма значительно меньше искажается (рис. 3.2).

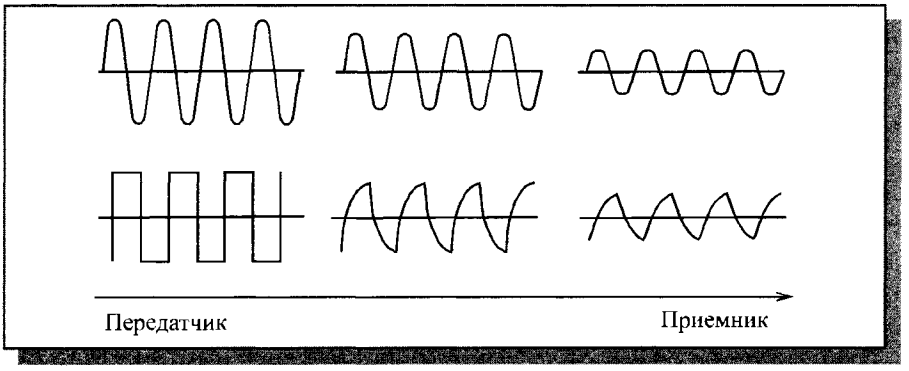



**Рис. 3.2.** Затухание сигналов в электрическом кабеле

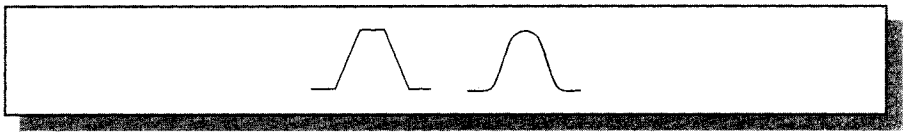


**Рис. 3.3.** Трапециевидный и колоколообразный импульсы

Это связано с разницей величин затухания для разных частот (высокие частоты затухают сильнее). Меньше всего искажается форма синусоидального сигнала — он просто уменьшается по амплитуде. Для улучшения качества передачи нередко используются трапецивидные или колоколообразные импульсы (рис. 3.3.), близкие по форме к полуволне синуса, для чего искусственно затягиваются или сглаживаются фронты изначальных прямоугольных сигналов.

**Экранирование** электрических линий связи применяется для снижения влияния на кабель внешних электромагнитных полей. Экран представляет собой медную или алюминиевую оболочку (плетеную или из фольги), в которую заключаются провода кабеля. Экранирование будет работать, если экран заземлен, поскольку необходимо, чтобы наведенные на него токи стекали на землю. Кроме того, экранирование заметно уменьшает и внешние излучения кабеля, что важно для обеспечения секретности передаваемой информации. Побочными полезными эффектами экранирования являются увеличение прочности кабеля и трудности с механическим подключением к кабелю для подслушивания. Экран заметно повышает стоимость кабеля, но также его механическую прочность.

Снизить влияние наведенных помех можно и без экрана, если использовать дифференциальную передачу сигнала (рис. 3.4). В этом случае передача идет по двум проводам, причем оба провода являются сигнальными. Передатчик формирует противофазные сигналы, а приемник реагирует на разность сигналов в обоих проводах. Условием согласования является равенство сопротивлений согласующих резисторов R половине волнового сопротивления кабеля Rв. Если оба провода имеют одинаковую длину и проложены рядом (в одном кабеле), то помехи действуют на

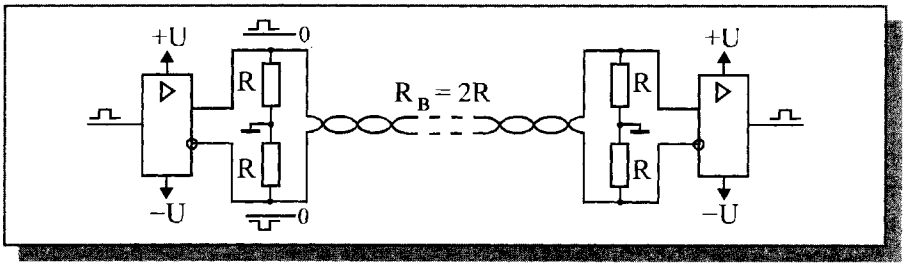



**Рис. 3.4.** Дифференциальная передача сигналов по витой паре

оба провода примерно одинаково, и в результате разностный сигнал между проводами практически не искажается. Именно такая дифференциальная передача применяется обычно в кабелях из витых пар. Но экранирование и в этом случае существенно улучшает помехоустойчивость.

**Гальваническая развязка** компьютеров от сети при использовании электрического кабеля совершенно необходима. Дело в том, что по электрическим кабелям (как по сигнальным проводам, так и по экрану) могут идти не только информационные сигналы, но и так называемый выравнивающий ток, возникающий вследствие неидеальности заземления компьютеров.

Когда компьютер не заземлен, на его корпусе образуется наведенный потенциал около 110 вольт переменного тока (половина питающего напряжения). Его можно ощутить на себе, если одной рукой взяться за корпус компьютера, а другой — за батарею центрального отопления или за какой-нибудь заземленный прибор.

При автономной работе компьютера отсутствие заземления, как правило, не оказывает серьезного влияния на его работу. Правда, иногда увеличивается количество сбоев в работе машины. Но при соединении нескольких территориально разнесенных компьютеров электрическим кабелем заземление становится серьезной проблемой. Если один из соединяемых компьютеров заземлен, а другой нет, то возможен выход из строя одного из них или обоих. Поэтому компьютеры крайне желательно заземлять.

В случае использования трехконтактной вилки и розетки, в которых есть нулевой провод, это получается автоматически. При двухконтактной вилке и розетке необходимо принимать специальные меры — организовывать заземление отдельным проводом большого сечения. Стоит также отметить, что в случае трехфазной сети желательно обеспечить питание всех компьютеров от одной фазы.

Но проблема заключается еще и в том, что «земля», к которой присоединяются компьютеры, обычно далека от идеала. Теоретически заземляющие провода компьютеров должны сходиться в одной точке, соединенной короткой массивной шиной с зарытым в землю массивным проводником. Такая ситуация возможна только если компьютеры не слишком разнесены, и заземление действительно сделано грамотно. Обычно же заземляющая шина имеет значительную длину, в результате чего стекающие по ней токи создают довольно большую разность потенциалов между ее отдельными точками. Особенно велика эта разность потенциалов в случае подключения к шине мощных и высокочастотных потребителей энергии.

Присоединенные к одной и той же шине, но в разных точках, компьютеры имеют на своих корпусах разные потенциалы (рис. 3.5). В результате по электрическому кабелю, соединяющему компьютеры, потечет выравнивающий ток (переменный с высокочастотными составляющими).

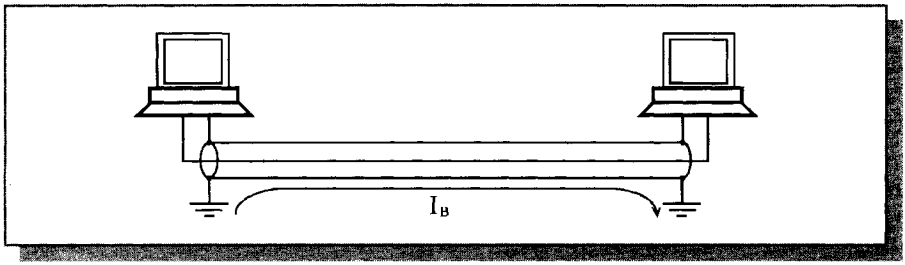



**Рис. 3.5**. Выравнивающий ток при отсутствии гальванической развязки

Хуже, когда компьютеры подключаются к разным шинам заземления. Выравнивающий ток может достигать в этом случае величины в несколько ампер. Подобные токи смертельно опасны для малосигнальных узлов компьютера. Кроме того выравнивающий ток существенно влияет на передаваемый сигнал, порой полностью забивая его. Даже тогда, когда сигналы передаются без участия экрана (например, по двум проводам, заключенным в экран), вследствие индуктивного действия выравнивающий ток мешает передаче информации. Именно поэтому экран всегда должен быть заземлен только в одной точке.

Однако если каждый из компьютеров самостоятельно заземлен, то заземление экрана в одной точке становится невозможным без *гальванической развязки* компьютеров от сети. Таким образом не должно быть связи по постоянному току между корпусом («землей») компьютера и экраном («землей») сетевого кабеля. В то же время, информационный сигнал должен передаваться из компьютера в сеть и из сети в компьютер. Для гальванической развязки обычно применяют импульсные трансформаторы, которые входят в состав сетевого оборудования (например, сетевых адаптеров). Трансформатор пропускает высокочастотные информационные сигналы, но обеспечивает полную изоляцию по постоянному току.

Грамотное соединение компьютеров локальной сети электрическим кабелем обязательно должно включать в себя следующее (рис. 3.6):

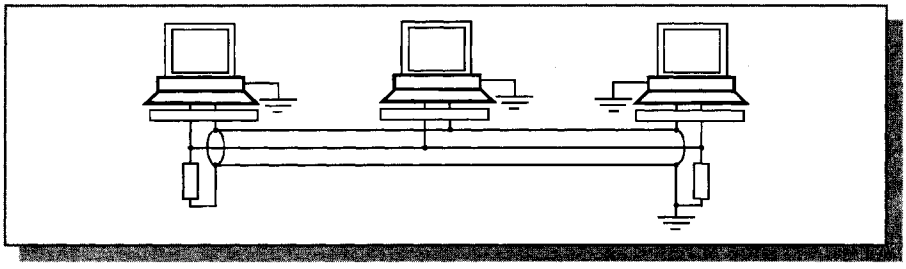


**Рис. 3.6.** Правильное соединение компьютеров сети (гальваническая развязка условно показана в виде прямоугольника)

- оконечное согласование кабеля с помощью терминаторов;
- гальваническую развязку компьютеров от сети;
- заземление каждого компьютера;
- заземление экрана (если, конечно, он есть) в одной точке.

Не стоит пренебрегать каким-либо из этих требований. Например, гальваническая развязка сетевых адаптеров часто рассчитывается на допустимое напряжение изоляции всего лишь 100 В, что при отсутствии заземления одного из компьютеров может легко привести к выходу из строя его адаптера.

Следует отметить, что для присоединения коаксиального кабеля обычно применяются разъемы в металлическом корпусе. Этот корпус не должен соединяться ни с корпусом компьютера, ни с «землей» (на плате адаптера он установлен с пластиковой изоляцией от крепежной планки). Заземление экрана кабеля сети лучше производить не через корпус компьютера, а отдельным специальным проводом, что обеспечивает лучшую надежность. Пластмассовые корпуса разъемов RJ-45 для кабелей с неэкранированными витыми парами снимают эту проблему.

Важно также учитывать, что экран кабеля, заземленный в одной точке, является радиоантенной с заземленным основанием. Он может улавливать и усиливать высокочастотные помехи с длиной волны, кратной его длине. Для снижения этого «антенного эффекта» применяется многоточечное заземление экрана по высокой частоте. В каждом сетевом адаптере «земля» сетевого кабеля соединяется с «землей» компьютера через высоковольтные

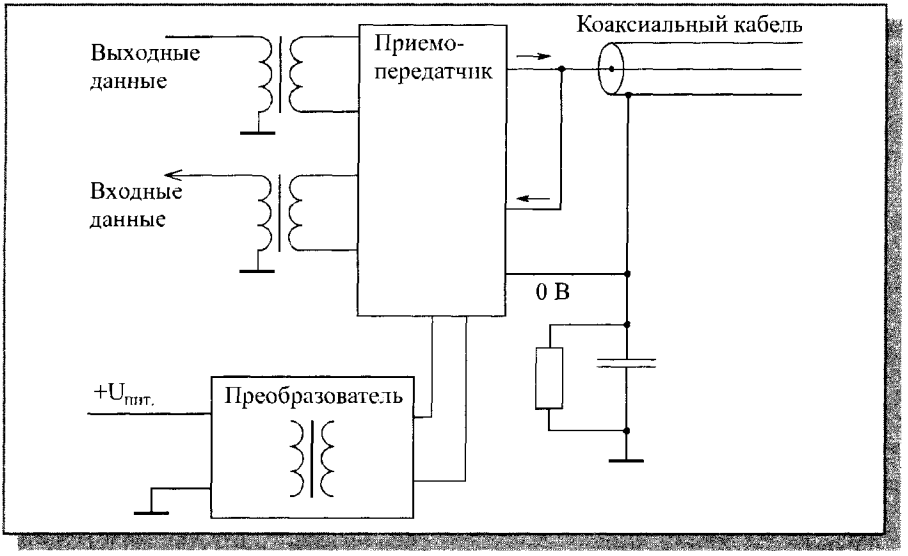



**Рис. 3.7**. Схема гальванической развязки в сети Ethernet

керамические конденсаторы. Для примера на рис. 3.7 показана упрощенная схема гальванической развязки, применяемая в сетевых адаптерах Ethernet.

Приемопередатчик напрямую связан с кабелем сети, но гальванически развязан с помощью трансформаторов от компьютера и остальной части сетевого адаптера. Это продиктовано особенностями протокола CSMA/CD и манчестерского кода, применяемых в Ethernet. Для обеспечения полной развязки питание приемопередатчика осуществляется посредством преобразователя питающего напряжения, имеющего внутри также трансформаторную гальваническую развязку. Оплетка коаксиального кабеля соединена с общим проводом компьютера через высоковольтный конденсатор. Параллельно конденсатору включен резистор с большим сопротивлением (1 МОм), который предотвращает электрический удар пользователя при одновременном касании им оплетки кабеля (корпуса разъема) и корпуса компьютера.

В случае применения витых пар все гораздо проще. Каждая витая пара имеет развязывающие импульсные трансформаторы на обоих своих концах. Ни один из проводов витой пары не заземляется (оба они сигнальные). К тому же разъемы для витых пар имеют пластмассовый корпус.

## Кодирование информации в локальных сетях

Информация в кабельных локальных сетях передается в закодированном виде, то есть каждому биту передаваемой информации соответствует свой набор уровней электрических сигналов в сетевом кабеле. Модуляция высокочастотных сигналов применяется в основном в бескабельных сетях, в радиоканалах. В кабельных сетях передача идет без модуляции или, как еще говорят, в основной полосе частот.

Правильный выбор кода позволяет повысить достоверность передачи информации, увеличить скорость передачи или снизить требования к выбору кабеля. Например, при разных кодах предельная скорость передачи по одному и тому же кабелю может отличаться в два раза. От выбранного кода напрямую зависит также сложность сетевой аппаратуры (узлы кодирования и декодирования кода). Код должен в идеале обеспечивать хорошую синхронизацию приема, низкий уровень ошибок, работу с любой длиной передаваемых информационных последовательностей.

Некоторые коды, используемые в локальных сетях, показаны на рис. 3.8. Далее будут рассмотрены их преимущества и недостатки.

### Код NRZ

Код NRZ (Non Return to Zero – без возврата к нулю) – это простейший код, представляющий собой обычный цифровой сигнал. Логическому

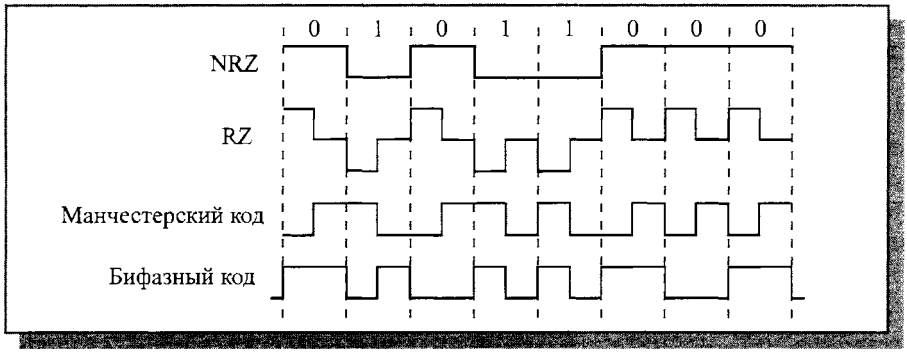



**Рис. 3.8.** Наиболее распространенные коды передачи информации

нулю соответствует высокий уровень напряжения в кабеле, логической единице – низкий уровень напряжения (или наоборот, что не принципиально). Уровни могут быть разной полярности (положительной и отрицательной) или же одной полярности (положительной или отрицательной). В течение *битового интервала* (bit time, BT), то есть времени передачи одного бита, никаких изменений уровня сигнала в кабеле не происходит.

К несомненным достоинствам кода NRZ относятся его довольно простая реализация (исходный сигнал не надо ни специально кодировать на передающем конце, ни декодировать на приемном конце), а также минимальная среди других кодов пропускная способность линии связи, требуемая при данной скорости передачи. Ведь наиболее частое изменение сигнала в сети будет при непрерывном чередовании единиц и нулей, то есть при последовательности 1010101010..., поэтому при скорости передачи, равной 10 Мбит/с (длительность одного бита равна 100 нс), частота изменения сигнала и соответственно требуемая пропускная способность линии составит 1 / 200нс = 5 МГц (рис. 3.9).

Самый большой недостаток кода NRZ – это возможность потери синхронизации приемником во время приема слишком длинных блоков (пакетов) информации. Приемник может привязывать момент начала

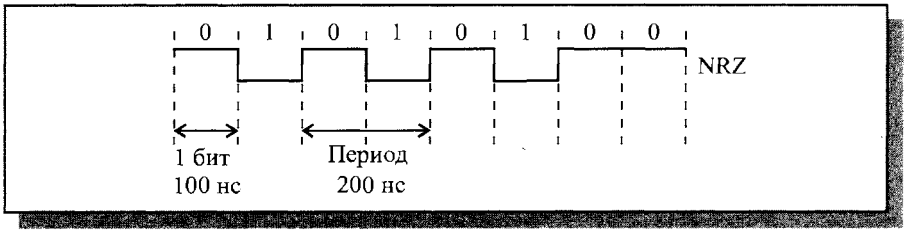



**Рис. 3.9.** Скорость передачи и требуемая пропускная способность при коде NRZ

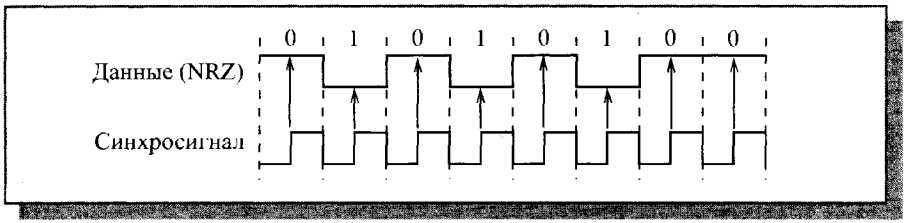



**Рис. 3.10.** Передача в коде NRZ с синхросигналом

приема только к первому (стартовому) биту пакета, а в течение приема пакета он вынужден пользоваться только внутренним тактовым генератором (внутренними часами). Например, если передается последовательность нулей или последовательность единиц, то приемник может определить, где проходят границы битовых интервалов, только по внутренним часам. И если часы приемника расходятся с часами передатчика, то временной сдвиг к концу приема пакета может превысить длительность одного или даже нескольких бит. В результате произойдет потеря переданных данных. Так, при длине пакета в 10000 бит допустимое расхождение часов составит не более 0,01% даже при идеальной передаче формы сигнала по кабелю.

Во избежание потери синхронизации можно было бы ввести вторую линию связи для синхросигнала (рис. 3.10). Но при этом требуемое количество кабеля, число приемников и передатчиков увеличивается в два раза. При большой длине сети и значительном количестве абонентов это невыгодно.

В связи с этим код NRZ используется только для передачи короткими пакетами (обычно до 1 Кбита).

Большой недостаток кода NRZ состоит еще и в том, что он может обеспечить обмен сообщениями (последовательностями, пакетами) только фиксированной, заранее обговоренной длины. Дело в том, что по принимаемой информации приемник не может определить, идет ли еще передача или уже закончилась. Для синхронизации начала приема пакета используется стартовый служебный бит, чей уровень отличается от пассивного состояния линии связи (например, пассивное состояние линии при отсутствии передачи – 0, стартовый бит – 1). Заканчивается прием после отсчета приемником заданного количества бит последовательности (рис. 3.11).

Наиболее известное применение кода NRZ – это стандарт RS232-C, последовательный порт персонального компьютера. Передача информации в нем ведется байтами (8 бит), сопровождаемыми стартовым и стоповым битами.

Три остальных кода (RZ, манчестерский код, бифазный код) принципиально отличаются от NRZ тем, что сигнал имеет дополнительные переходы (фронты) в пределах битового интервала. Это сделано для того, чтобы приемник мог подстраивать свои часы под принимаемый сигнал на


**Рис. 3.11.** Определение окончания последовательности при коде NRZ

каждом битовом интервале. Отслеживая фронты сигналов, приемник может точно синхронизовать прием каждого бита. В результате небольшие расхождения часов приемника и передатчика уже не имеют значения. Приемник может надежно принимать последовательности любой длины. Такие коды называются самосинхронизирующимися. Можно считать, что *самосинхронизирующиеся* коды несут в себе синхросигнал.

## Код RZ

Код RZ (Return to Zero – с возвратом к нулю) – этот трехуровневый код получил такое название потому, что после значащего уровня сигнала в первой половине битового интервала следует возврат к некоему «нулевому», среднему уровню (например, к нулевому потенциалу). Переход к нему происходит в середине каждого битового интервала. Логическому нулю, таким образом, соответствует положительный импульс, логической единице – отрицательный (или наоборот) в первой половине битового интервала.

В центре битового интервала всегда есть переход сигнала (положительный или отрицательный), следовательно, из этого кода приемник легко может выделить синхроимпульс (строб). Возможна временная привязка не только к началу пакета, как в случае кода NRZ, но и к каждому отдельному биту, поэтому потери синхронизации не произойдет при любой длине пакета.

Еще одно важное достоинство кода RZ – простая временная привязка приема, как к началу последовательности, так и к ее концу. Приемник просто должен анализировать, есть изменение уровня сигнала в течение битового интервала или нет. Первый битовый интервал без изменения уровня сигнала соответствует окончанию принимаемой последовательности бит (рис. 3.12). Поэтому в коде RZ можно использовать передачу последовательностями переменной длины.

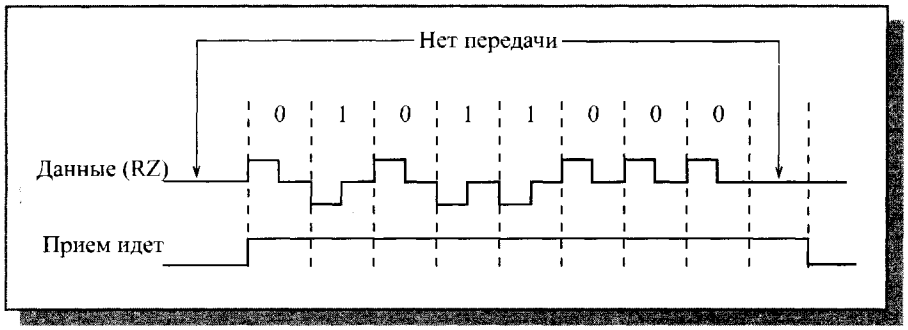



**Рис. 3.12.** Определение начала и конца приема при коде RZ

Недостаток кода RZ состоит в том, что для него требуется вдвое большая полоса пропускания канала при той же скорости передачи по сравнению с NRZ (так как здесь на один битовый интервал приходится два изменения уровня сигнала). Например, для скорости передачи информации 10 Мбит/с требуется пропускная способность линии связи 10 МГц, а не 5 МГц, как при коде NRZ (рис. 3.13).

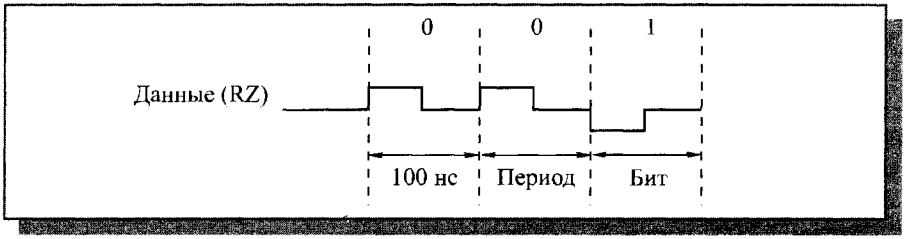



**Рис. 3.13.** Скорость передачи и пропускная способность при коде RZ

Другой важный недостаток – наличие трех уровней, что всегда усложняет аппаратуру как передатчика, так и приемника.

Код RZ применяется не только в сетях на основе электрического кабеля, но и в оптоволоконных сетях. Правда, в них не существует положительных и отрицательных уровней сигнала, поэтому используется три следующие уровня: отсутствие света, «средний» свет, «сильный» свет. Это очень удобно: даже когда нет передачи информации, свет все равно присутствует, что позволяет легко определить целостность оптоволоконной линии связи без дополнительных мер (рис. 3.14).

### Манчестерский код

Манчестерский код (или код Манчестер-II) получил наибольшее распространение в локальных сетях. Он также относится к самосинхро-

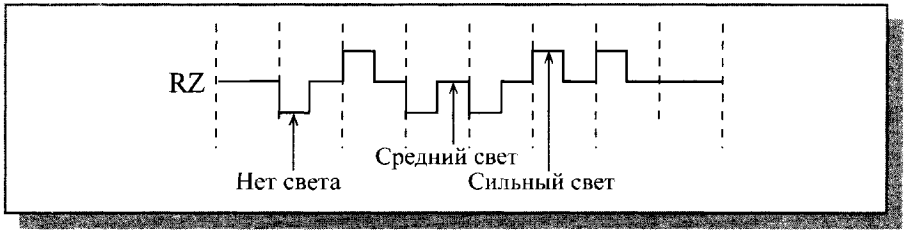



**Рис. 3.14.** Использование кода RZ в оптоволоконных сетях

низирующимся кодам, но в отличие от RZ имеет не три, а всего два уровня, что способствует его лучшей помехозащищенности и упрощению приемных и передающих узлов. Логическому нулю соответствует положительный переход в центре битового интервала (то есть первая половина битового интервала – низкий уровень, вторая половина – высокий), а логической единице соответствует отрицательный переход в центре битового интервала (или наоборот).

Как и в RZ, обязательное наличие перехода в центре бита позволяет приемнику манчестерского кода легко выделить из пришедшего сигнала синхросигнал и передать информацию сколь угодно большими последовательностями без потерь из-за рассинхронизации. Допустимое расхождение часов приемника и передатчика может достигать 25%.

Подобно коду RZ, при использовании манчестерского кода требуется пропускная способность линии в два раза выше, чем при применении простейшего кода NRZ. Например, для скорости передачи 10 Мбит/с требуется полоса пропускания 10 МГц (рис. 3.15).

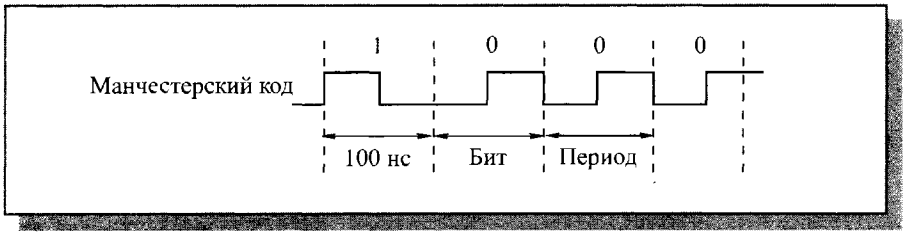



**Рис. 3.15.** Скорость передачи и пропускная способность при манчестерском коде

Как и при коде RZ, в данном случае приемник легко может определить не только начало передаваемой последовательности бит, но и ее конец. Если в течение битового интервала нет перехода сигнала, то прием заканчивается. В манчестерском коде можно передавать последовательности бит переменной длины (рис. 3.16). Процесс определения времени передачи называют еще контролем несущей, хотя в явном виде несущей частоты в данном случае не присутствует.

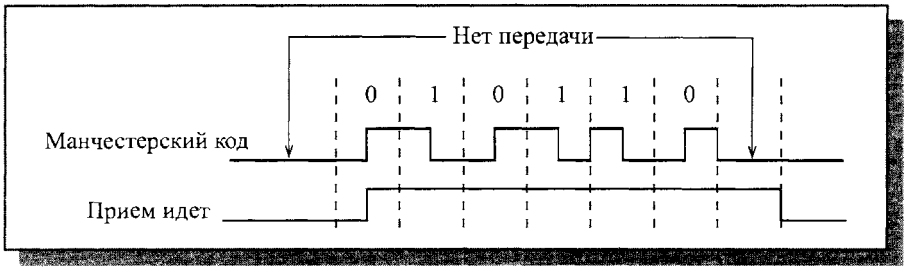



**Рис. 3.16.** Определение начала и конца приема при манчестерском коде

Манчестерский код используется как в электрических, так и в оптоволоконных кабелях (в последнем случае один уровень соответствует отсутствию света, а другой – его наличию).

Основное достоинство манчестерского кода – постоянная составляющая в сигнале (половину времени сигнал имеет высокий уровень, другую половину – низкий). Постоянная составляющая равна среднему значению между двумя уровнями сигнала.

Если высокий уровень имеет положительную величину, а низкий – такую же отрицательную, то постоянная составляющая равна нулю. Это дает возможность легко применять для гальванической развязки импульсные трансформаторы. При этом не требуется дополнительного источника питания для линии связи (как, например, в случае использования оптронной гальванической развязки), резко уменьшается влияние низкочастотных помех, которые не проходят через трансформатор, легко решается проблема согласования.

Если же один из уровней сигнала в манчестерском коде — нулевой (как, например, в сети Ethernet), то величина постоянной составляющей в течение передачи будет равна примерно половине амплитуды сигнала. Это позволяет легко фиксировать столкновения пакетов в сети (конфликт, коллизию) по отклонению величины постоянной составляющей за установленные пределы.

Частотный спектр сигнала при манчестерском кодировании включает в себя только две частоты: при скорости передачи 10 Мбит/с это 10 МГц (соответствует передаваемой цепочке из одних нулей или из одних единиц) и 5 МГц (соответствует последовательности из чередующихся нулей и единиц: 1010101010...). Поэтому с помощью простейших полосовых фильтров можно легко избавиться от всех других частот (помехи, наводки, шумы).

### Бифазный код

Бифазный код часто рассматривают как разновидность манчестерского, так как их характеристики практически полностью совпадают.

Данный код отличается от классического манчестерского кода тем, что он не зависит от перемены мест двух проводов кабеля. Особенно это удобно в случае, когда для связи применяется витая пара, провода которой легко перепутать. Именно этот код используется в одной из самых известных сетей Token-Ring компании IBM.

Принцип данного кода прост: в начале каждого битового интервала сигнал меняет уровень на противоположный предыдущему, а в середине единичных (и только единичных) битовых интервалов уровень изменяется еще раз. Таким образом, в начале битового интервала всегда есть переход, который используется для самосинхронизации. Как и в случае классического манчестерского кода, в частотном спектре при этом присутствует две частоты. При скорости 10 Мбит/с это частоты 10 МГц (при последовательности одних единиц: 11111111...) и 5 МГц (при последовательности одних нулей: 00000000...).

Имеется также еще один вариант бифазного кода (его еще называют дифференциальным манчестерским кодом). В этом коде единице соответствует наличие перехода в начале битового интервала, а нулю – отсутствие перехода в начале битового интервала (или наоборот). При этом в середине битового интервала переход имеется всегда, и именно он служит для побитовой самосинхронизации приемника. Характеристики этого варианта кода также полностью соответствуют характеристикам манчестерского кода.

Здесь же стоит упомянуть о том, что часто совершенно неправомерно считается, что единица измерения скорости передачи бод – это то же самое, что бит в секунду, а скорость передачи в бодах равняется скорости передачи в битах в секунду. Это верно только в случае кода NRZ. Скорость в бодах характеризует не количество передаваемых бит в секунду, а число изменений уровня сигнала в секунду. И при RZ или манчестерском кодах требуемая скорость в бодах оказывается вдвое выше, чем при NRZ. В бодах измеряется скорость передачи сигнала, а в битах в секунду – скорость передачи информации. Поэтому, чтобы избежать неоднозначного понимания, скорость передачи по сети лучше указывать в битах в секунду (бит/с, Кбит/с, Мбит/с, Гбит/с).

### Другие коды

Все разрабатываемые в последнее время коды призваны найти компромисс между требуемой при заданной скорости передачи полосой пропускания кабеля и возможностью самосинхронизации. Разработчики стремятся сохранить самосинхронизацию, но не ценой двукратного увеличения полосы пропускания, как в рассмотренных RZ, манчестерском и бифазном кодах.

Чаще всего для этого в поток передаваемых битов добавляют биты синхронизации. Например, один бит синхронизации на 4, 5 или 6 инфор-

мационных битов или два бита синхронизации на 8 информационных битов. В действительности все обстоит несколько сложнее: кодирование не сводится к простой вставке в передаваемые данные дополнительных битов. Группы информационных битов преобразуются в передаваемые по сети группы с количеством битов на один или два больше. Приемник осуществляет обратное преобразование, восстанавливает исходные информационные биты. Довольно просто осуществляется в этом случае и обнаружение несущей частоты (детектирование передачи).

Так, например, в сети FDDI (скорость передачи 100 Мбит/с) применяется код 4B/5B, который 4 информационных бита преобразует в 5 передаваемых битов. При этом синхронизация приемника осуществляется один раз на 4 бита, а не в каждом бите, как в случае манчестерского кода. Но зато требуемая полоса пропускания увеличивается по сравнению с кодом NRZ не в два раза, а только в 1,25 раза (то есть составляет не 100 МГц, а всего лишь 62,5 МГц). По тому же принципу строятся и другие коды, в частности, 5B/6B, используемый в стандартной сети 100VG-AnyLAN, или 8B/10B, применяемый в сети Gigabit Ethernet.

В сегменте 100BASE-T4 сети Fast Ethernet использован несколько иной подход. Там применяется код 8B/6T, предусматривающий параллельную передачу трех трехуровневых сигналов по трем витым парам. Это позволяет достичь скорости передачи 100 Мбит/с на дешевых кабелях с витыми парами категории 3, имеющих полосу пропускания всего лишь16 МГц (см. табл. 2.1). Правда, это требует большего расхода кабеля и увеличения количества приемников и передатчиков. К тому же принципиально, чтобы все провода были одной длины и задержки сигнала в них не слишком различались.

Иногда уже закодированная информация подвергается дополнительному кодированию, что позволяет упростить синхронизацию на приемном конце. Наибольшее распространение для этого получили 2-уровневый код NRZI, применяемый в оптоволоконных сетях (FDDI и 100BASE-FX), а также 3-уровневый код MLT-3, используемый в сетях на витых парах (TPDDI и 100BASE-TX). Оба эти кода (рис. 3.17) не являются самосинхронизирующимися.

Код NRZI (без возврата к нулю с инверсией единиц – Non-Return to Zero, Invert to one) предполагает, что уровень сигнала меняется на противоположный в начале единичного битового интервала и не меняется при передаче нулевого битового интервала. При последовательности единиц на границах битовых интервалов имеются переходы, при последовательности нулей – переходов нет. В этом смысле код NRZI лучше синхронизируется, чем NRZ (там нет переходов ни при последовательности нулей, ни при последовательности единиц).

Код MLT-3 (Multi-Level Transition-3) предполагает, что при передаче нулевого битового интервала уровень сигнала не меняется, а при переда-

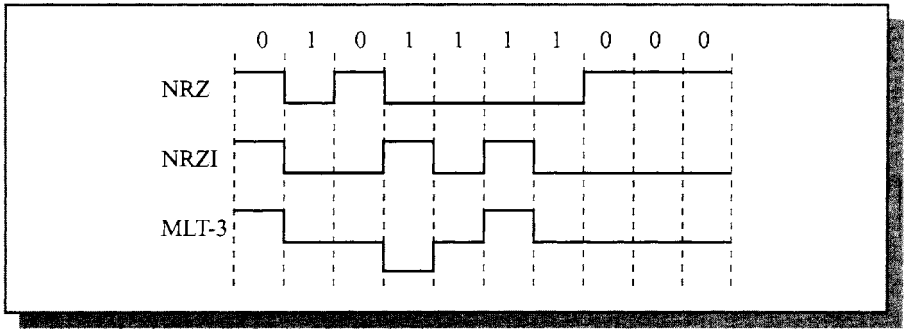



**Рис. 3.17.** Коды NRZI и MLT-3

че единицы – меняется на следующий уровень по такой цепочке: +U, 0, –U, 0 +U, 0, –U и т.д. Таким образом, максимальная частота смены уровней получается вчетверо меньше скорости передачи в битах (при последовательности сплошных единиц). Требуемая полоса пропускания оказывается меньше, чем при коде NRZ.

Все упомянутые в данном разделе коды предусматривают непосредственную передачу в сеть цифровых двух- или трехуровневых прямоугольных импульсов.

Однако иногда в сетях используется и другой путь – модуляция информационными импульсами высокочастотного аналогового сигнала (синусоидального). Такое аналоговое кодирование позволяет при переходе на широкополосную передачу существенно увеличить пропускную способность канала связи (в этом случае по сети можно передавать несколько бит одновременно). К тому же, как уже отмечалось, при прохождении по каналу связи аналогового сигнала (синусоидального) не искажается форма сигнала, а только уменьшается его амплитуда, а в случае цифрового сигнала форма сигнала искажается (см. рис. 3.2).

К самым простым видам аналогового кодирования относятся следующие (рис. 3.18):

- Амплитудная модуляция (AM, АМ – Amplitude Modulation), при которой логической единице соответствует наличие сигнала (или сигнал большей амплитуды), а логическому нулю – отсутствие сигнала (или сигнал меньшей амплитуды). Частота сигнала при этом остается постоянной. Недостаток амплитудной модуляции состоит в том, что AM-сигнал сильно подвержен действию помех и шумов, а также предъявляет повышенные требования к затуханию сигнала в канале связи. Достоинства – простота аппаратурной реализации и узкий частотный спектр.
- Частотная модуляция (ЧМ, FM – Frequency Modulation), при которой логической единице соответствует сигнал более высокой часто-

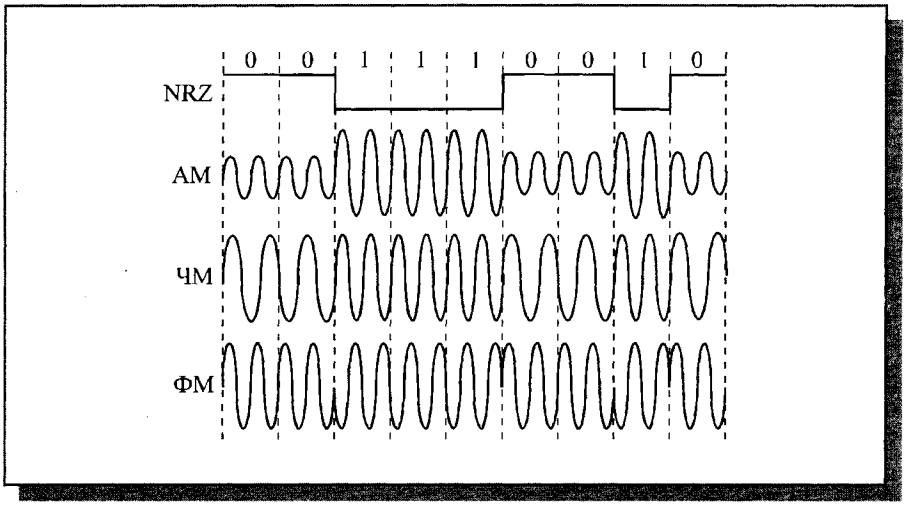



**Рис. 3.18.** Аналоговое кодирование цифровой информации

ты, а логическому нулю – сигнал более низкой частоты (или наоборот). Амплитуда сигнала при частотной модуляции остается постоянной, что является большим преимуществом по сравнению с амплитудной модуляцией.

- Фазовая модуляция (ФМ, PM – Phase Modulation), при которой смене логического нуля на логическую единицу и наоборот соответствует резкое изменение фазы синусоидального сигнала одной частоты и амплитуды. Важно, что амплитуда модулированного сигнала остается постоянной, как и в случае частотной модуляции.

Применяются и значительно более сложные методы модуляции, являющиеся комбинацией перечисленных простейших методов. О некоторых из них будет рассказано в главе 12.

Чаще всего аналоговое кодирование используется при передаче информации по каналу с узкой полосой пропускания, например, по телефонным линиям в глобальных сетях. Кроме того, аналоговое кодирование применяется в радиоканалах, что позволяет обеспечивать связь между многими пользователями одновременно. В локальных кабельных сетях аналоговое кодирование практически не используется из-за высокой сложности и стоимости как кодирующего, так и декодирующего оборудования.

# Глава 3. Пакеты, протоколы и методы управления обменом

## Лекция 4. Пакеты, протоколы и методы управления обменом

**В этой лекции говорится о принципах передачи информации по сети, назначении и типах информационных пакетов, структуре пакетов, методах управления обменом в сетях с разной топологией, их достоинствах и недостатках.**

**Ключевые слова:** пакет, кадр, поля пакета, инкапсуляция пакетов, время доступа, централизованный метод, маркерный метод, случайный метод.

### Назначение пакетов и их структура

Информация в локальных сетях, как правило, передается отдельными порциями, кусками, называемыми в различных источниках пакетами (packets), кадрами (frames) или блоками. Причем предельная длина этих пакетов строго ограничена (обычно величиной в несколько килобайт). Ограничена длина пакета и снизу (как правило, несколькими десятками байт). Выбор пакетной передачи связан с несколькими важными соображениями.

Локальная сеть, как уже отмечалось, должна обеспечивать качественную, прозрачную связь всем абонентам (компьютерам) сети. Важнейшим параметром является так называемое время доступа к сети (access time), которое определяется как временной интервал между моментом готовности абонента к передаче (когда ему есть, что передавать) и моментом начала этой передачи. Это время ожидания абонентом начала своей передачи. Естественно, оно не должно быть слишком большим, иначе величина реальной, интегральной скорости передачи информации между приложениями сильно уменьшится даже при высокоскоростной связи.

Ожидание начала передачи связано с тем, что в сети не может происходить несколько передач одновременно (во всяком случае, при топологиях «шина» и «кольцо»). Всегда есть только один передатчик и один приемник (реже – несколько приемников). В противном случае информация от разных передатчиков смешивается и искажается. В связи с этим абоненты передают свою информацию по очереди. И каждому абоненту,

прежде чем начать передачу, надо дождаться своей очереди. Вот это время ожидания своей очереди и есть время доступа.

Если бы вся требуемая информация передавалась каким-то абонентом сразу, непрерывно, без разделения на пакеты, то это привело бы к монопольному захвату сети этим абонентом на довольно продолжительное время. Все остальные абоненты вынуждены были бы ждать окончания передачи всей информации, что в ряде случаев могло бы потребовать десятков секунд и даже минут (например, при копировании содержимого целого жесткого диска). С тем чтобы уравнять в правах всех абонентов, а также сделать примерно одинаковыми для всех них величину времени доступа к сети и интегральную скорость передачи информации, как раз и применяются пакеты (кадры) ограниченной длины. Важно также и то, что при передаче больших массивов информации вероятность ошибки из-за помех и сбоев довольно высока. Например, при характерной для локальных сетей величине вероятности одиночной ошибки в $10^{-8}$ пакет длиной 10 Кбит будет искажен с вероятностью $10^{-4}$, а массив длиной 10 Мбит – уже с вероятностью $10^{-1}$. К тому же выявить ошибку в массиве из нескольких мегабайт намного сложнее, чем в пакете из нескольких килобайт. А при обнаружении ошибки придется повторить передачу всего большого массива. Но и при повторной передаче большого массива снова высока вероятность ошибки, и процесс этот при слишком большом массиве может повторяться до бесконечности.

С другой стороны, сравнительно большие пакеты имеют преимущества перед очень маленькими пакетами, например, перед побайтовой (8 бит) или пословной (16 бит или 32 бита) передачей информации.

Дело в том, что каждый пакет помимо собственно данных, которые требуется передать, должен содержать некоторое количество служебной информации. Прежде всего, это адресная информация, которая определяет, от кого и кому передается данный пакет (как на почтовом конверте – адреса получателя и отправителя). Если порция передаваемых данных будет очень маленькой (например, несколько байт), то доля служебной информации станет непозволительно высокой, что резко снизит интегральную скорость обмена информацией по сети.

Существует некоторая оптимальная длина пакета (или оптимальный диапазон длин пакетов), при которой средняя скорость обмена информацией по сети будет максимальна. Эта длина не является неизменной величиной — она зависит от уровня помех, метода управления обменом, количества абонентов сети, характера передаваемой информации, и от многих других факторов. Имеется диапазон длин, который близок к оптимуму.

Таким образом, процесс информационного обмена в сети представляет собой чередование пакетов, каждый из которых содержит информацию, передаваемую от абонента к абоненту.

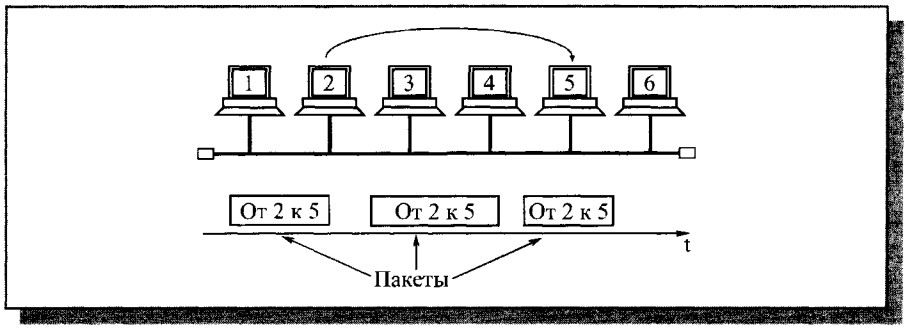



**Рис. 4.1.** Передача пакетов в сети между двумя абонентами

В частном случае (рис. 4.1) все эти пакеты могут передаваться одним абонентом (когда другие абоненты не хотят передавать). Но обычно в сети чередуются пакеты, посланные разными абонентами (рис. 4.2).

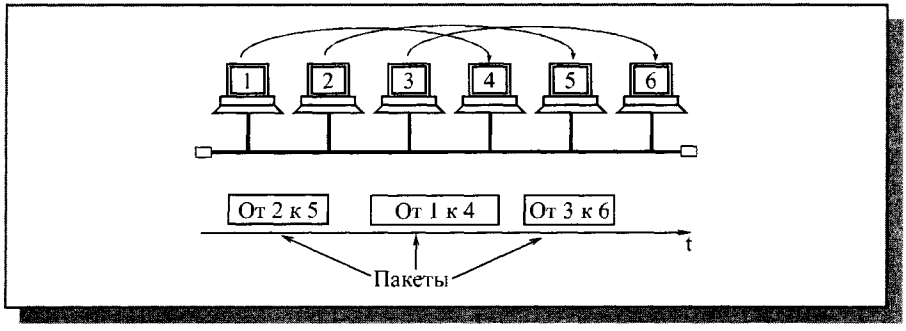



**Рис. 4.2.** Передача пакетов в сети между несколькими абонентами

Структура и размеры пакета в каждой сети жестко определены стандартом на данную сеть и связаны, прежде всего, с аппаратурными особенностями данной сети, выбранной топологией и типом среды передачи информации. Кроме того, эти параметры зависят от используемого протокола (порядка обмена информацией).

Но существуют некоторые общие принципы формирования структуры пакета, которые учитывают характерные особенности обмена информацией по любым локальным сетям.

Чаще всего пакет содержит в себе следующие основные поля или части (рис. 4.3):

- Стартовая комбинация битов или преамбула, которая обеспечивает предварительную настройку аппаратуры адаптера или другого сетевого устройства на прием и обработку пакета. Это поле может полностью отсутствовать или же сводиться к единственному стартовому биту.

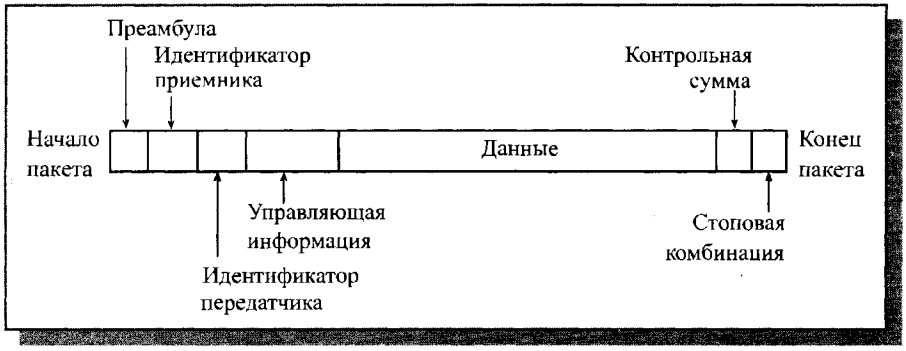



**Рис. 4.3.** Типичная структура пакета

- Сетевой адрес (идентификатор) принимающего абонента, то есть индивидуальный или групповой номер, присвоенный каждому принимающему абоненту в сети. Этот адрес позволяет приемнику распознать пакет, адресованный ему лично, группе, в которую он входит, или всем абонентам сети одновременно (при широком вещании).
- Сетевой адрес (идентификатор) передающего абонента, то есть индивидуальный номер, присвоенный каждому передающему абоненту. Этот адрес информирует принимающего абонента, откуда пришел данный пакет. Включение в пакет адреса передатчика необходимо в том случае, когда одному приемнику могут попеременно приходить пакеты от разных передатчиков.
- Служебная информация, которая может указывать на тип пакета, его номер, размер, формат, маршрут его доставки, на то, что с ним надо делать приемнику и т.д.
- Данные (*поле данных*) – это та информация, ради передачи которой используется пакет. В отличие от всех остальных полей пакета поле данных имеет переменную длину, которая, собственно, и определяет полную длину пакета. Существуют специальные *управляющие пакеты*, которые не имеют поля данных. Их можно рассматривать как сетевые команды. Пакеты, включающие поле данных, называются *информационными пакетами*. Управляющие пакеты могут выполнять функцию начала и конца сеанса связи, подтверждения приема информационного пакета, запроса информационного пакета и т.д.
- Контрольная сумма пакета – это числовой код, формируемый передатчиком по определенным правилам и содержащий в свернутом виде информацию обо всем пакете. Приемник, повторяя вычисления, сделанные передатчиком, с принятым пакетом, сравнивает их результат с контрольной суммой и делает вывод о правильности или ошибочности передачи пакета. Если пакет ошибочен, то приемник запра-

шивает его повторную передачу. Обычно используется циклическая контрольная сумма (CRC). Подробнее об этом рассказано в главе 7.

- Стоповая комбинация служит для информирования аппаратуры принимающего абонента об окончании пакета, обеспечивает выход аппаратуры приемника из состояния приема. Это поле может отсутствовать, если используется самосинхронизирующийся код, позволяющий определять момент окончания передачи пакета.

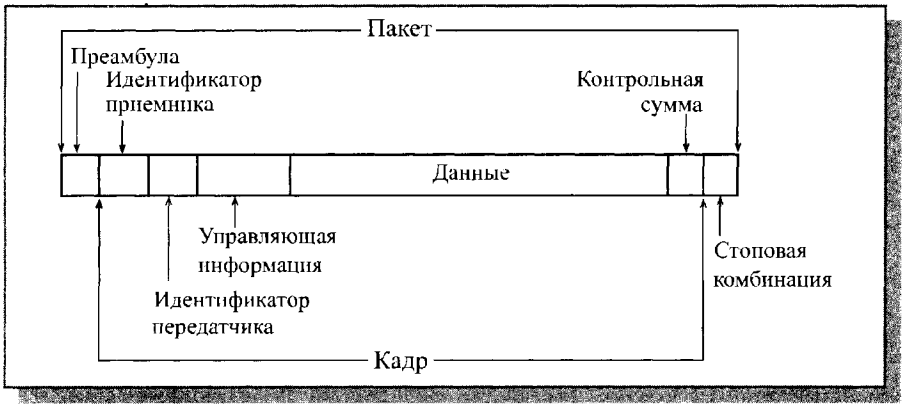



**Рис. 4.4.** Вложение кадра в пакет

Нередко в структуре пакета выделяют всего три поля:

- Начальное управляющее поле пакета (или *заголовок* пакета), то есть поле, включающее в себя стартовую комбинацию, сетевые адреса приемника и передатчика, а также служебную информацию.
- Поле данных пакета.
- Конечное управляющее поле пакета (*заключение*, *трейлер*), куда входят контрольная сумма и стоповая комбинация, а также, возможно, служебная информация.

Как уже упоминалось, помимо термина «пакет» (packet) в литературе также нередко встречается термин «кадр» (frame). Иногда под этими терминами имеется в виду одно и то же. Но иногда подразумевается, что кадр и пакет различаются. Причем единства в объяснении этих различий не наблюдается.

В некоторых источниках утверждается, что кадр вложен в пакет. В этом случае все перечисленные поля пакета кроме преамбулы и стоповой комбинации относятся к кадру (рис. 4.4). Например, в описаниях сети Ethernet говорится, что в конце преамбулы передается признак начала кадра.

В других, напротив, поддерживается мнение о том, что пакет вложен в кадр. И тогда под пакетом подразумевается только информация, содержащаяся в кадре, который передается по сети и снабжен служебными полями.

Во избежание путаницы, в данной книге термин «пакет» будет использоваться как более понятный и универсальный.

В процессе сеанса обмена информацией по сети между передающим и принимающим абонентами происходит обмен информационными и управляющими пакетами по установленным правилам, называемым протоколом обмена. Это позволяет обеспечить надежную передачу информации при любой интенсивности обмена по сети.

Пример простейшего протокола показан на рис. 4.5.

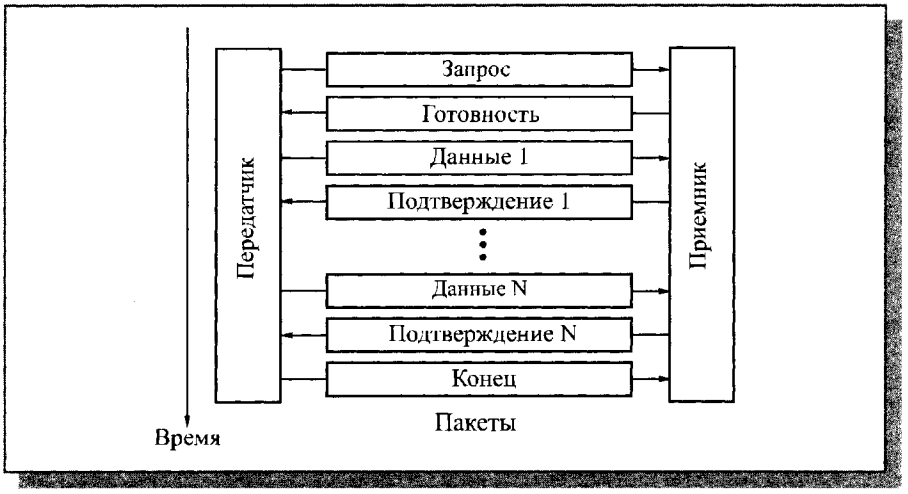



**Рис. 4.5.** Пример обмена пакетами при сеансе связи

Сеанс обмена начинается с запроса передатчиком готовности приемника принять данные. Для этого используется управляющий пакет «Запрос». Если приемник не готов, он отказывается от сеанса специальным управляющим пакетом. В случае, когда приемник готов, он посылает в ответ управляющий пакет «Готовность». Затем начинается собственно передача данных. При этом на каждый полученный информационный пакет приемник отвечает управляющим пакетом «Подтверждение». В случае, когда пакет данных передан с ошибками, в ответ на него приемник запрашивает повторную передачу. Заканчивается сеанс управляющим пакетом «Конец», которым передатчик сообщает о разрыве связи. Существует множество стандартных протоколов, которые используют как передачу с подтверждением (с гарантированной доставкой пакета), так и передачу без подтверждения (без гарантии доставки пакета). Подробнее о протоколах обмена будет рассказано в следующей главе.

При реальном обмене по сети применяются многоуровневые протоколы, каждый из уровней которых предполагает свою структуру пакета

(адресацию, управляющую информацию, формат данных и т.д.). Ведь протоколы высоких уровней имеют дело с такими понятиями, как файл-сервер или приложение, запрашивающее данные у другого приложения, и вполне могут не иметь представления ни о типе аппаратуры сети, ни о методе управления обменом. Все пакеты более высоких уровней последовательно вкладываются в передаваемый пакет, точнее, в поле данных передаваемого пакета (рис. 4.6). Этот процесс последозательной упаковки данных для передачи называется также инкапсуляцией пакетов.

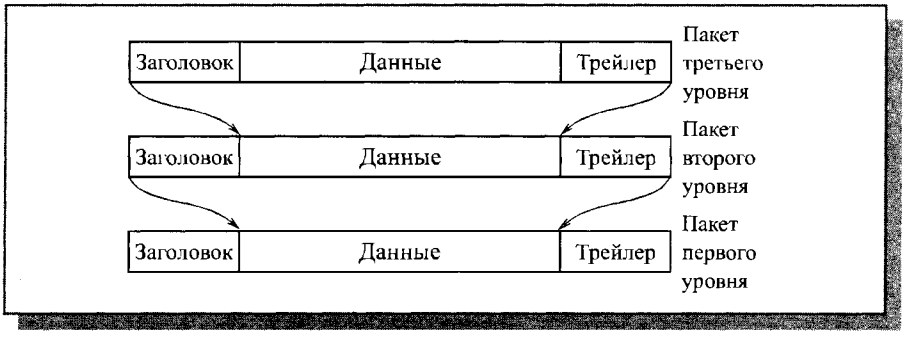



**Рис. 4.6.** Многоуровневая система вложения пакетов

Каждый следующий вкладываемый пакет может содержать собственную служебную информацию, располагающуюся как до данных (заголовок), так и после них (трейлер), причем ее назначение может быть различным. Безусловно, доля вспомогательной информации в пакетах при этом возрастает с каждым следующим уровнем, что снижает эффективную скорость передачи данных. Для увеличения этой скорости предпочтительнее, чтобы протоколы обмена были проще, и уровней этих протоколов было меньше. Иначе никакая скорость передачи битов не поможет, и быстрая сеть может передавать файл дольше, чем медленная сеть, которая пользуется более простым протоколом.

Обратный процесс последовательной распаковки данных приемником называется *декапсуляцией пакетов*.

## Адресация пакетов

Каждый абонент (узел) локальной сети должен иметь свой уникальный адрес (идентификатор или MAC-адрес), для того чтобы ему можно было адресовать пакеты. Существуют две основные системы присвоения адресов абонентам сети (точнее, сетевым адаптерам этих абонентов).

Первая система сводится к тому, что при установке сети каждому абоненту пользователь присваивает индивидуальный адрес по порядку, к

примеру, от 0 до 30 или от 0 до 254. Присваивание адресов производится программно или с помощью переключателей на плате адаптера. При этом требуемое количество разрядов адреса определяется из неравенства:

$$2^n > N_{max}$$

где $n$ – количество разрядов адреса, а $N_{max}$ – максимально возможное количество абонентов в сети. Например, восемь разрядов адреса достаточно для сети из 255 абонентов. Один адрес (обычно 1111....11) отводится для широковещательной передачи, то есть он используется для пакетов, адресованных всем абонентам одновременно.

Именно такой подход применен в известной сети Arcnet. Достоинства данного подхода – малый объем служебной информации в пакете, а также простота аппаратуры адаптера, распознающей адрес пакета. Недостаток – трудоемкость задания адресов и возможность ошибки (например, двум абонентам сети может быть присвоен один и тот же адрес). Контроль уникальности сетевых адресов всех абонентов возлагается на администратора сети.

Второй подход к адресации был разработан международной организацией IEEE, занимающейся стандартизацией сетей. Именно он используется в большинстве сетей и рекомендован для новых разработок. Идея этого подхода состоит в том, чтобы присваивать уникальный сетевой адрес каждому адаптеру сети еще на этапе его изготовления. Если количество возможных адресов будет достаточно большим, то можно быть уверенным, что в любой сети по всему миру никогда не будет абонентов с одинаковыми адресами. Поэтому был выбран 48-битный формат адреса, что соответствует примерно 280 триллионам различных адресов. Понятно, что столько сетевых адаптеров никогда не будет выпущено.

С тем чтобы распределить возможные диапазоны адресов между многочисленными изготовителями сетевых адаптеров, была предложена следующая структура адреса (рис. 4.7):

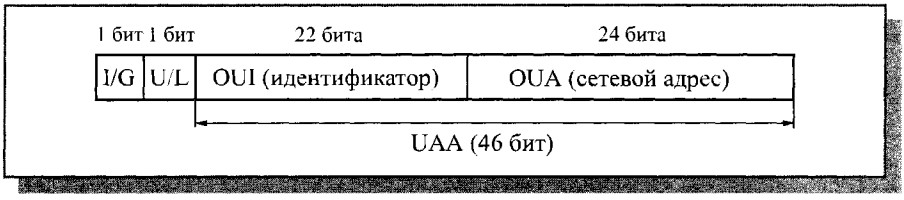



**Рис. 4.7**. Структура 48-битного стандартного MAC-адреса

- Младшие 24 разряда кода адреса называются OUA (Organizationally Unique Address) – организационно уникальный адрес. Именно их при-

сваивает каждый из зарегистрированных производителей сетевых адаптеров. Всего возможно свыше 16 миллионов комбинаций, то есть каждый изготовитель может выпустить 16 миллионов сетевых адаптеров.

- Следующие 22 разряда кода называются OUI (Organizationally Unique Identifier) – организационно уникальный идентификатор. IEEE присваивает один или несколько OUI каждому производителю сетевых адаптеров. Это позволяет исключить совпадения адресов адаптеров от разных производителей. Всего возможно свыше 4 миллионов разных OUI — это означает, что теоретически может быть зарегистрировано 4 миллиона производителей. Вместе OUA и OUI называются UAA (Universally Administered Address) – универсально управляемый адрес или IEEE-адрес.
- Два старших разряда адреса — управляющие, они определяют тип адреса, способ интерпретации остальных 46 разрядов. Старший бит I/G (Individual/Group) указывает на тип адреса. Если он установлен в 0, то он — индивидуальный, если в 1, то групповой (многопунктовый или функциональный). Пакеты с групповым адресом получат все имеющие этот групповой адрес сетевые адаптеры. Причем групповой адрес определяется 46 младшими разрядами. Второй управляющий бит U/L (Universal/Local) называется флажком универсального/местного управления и определяет, как был присвоен адрес данному сетевому адаптеру. Обычно он установлен в 0. Установка бита U/L в 1 означает, что адрес задан не производителем сетевого адаптера, а организацией, использующей данную сеть. Это случается довольно редко.

Для широковещательной передачи (то есть передачи всем абонентам сети одновременно) применяется специально выделенный сетевой адрес, все 48 битов которого установлены в единицу. Его принимают все абоненты сети независимо от их индивидуальных и групповых адресов.

Данной системы адресов придерживаются такие популярные сети, как Ethernet, Fast Ethernet, Token-Ring, FDDI, 100VG-AnyLAN. Ее недостатки – высокая сложность аппаратуры сетевых адаптеров, а также большая доля служебной информации в передаваемом пакете (адреса источника и приемника вместе требуют уже 96 битов пакета или 12 байт).

Во многих сетевых адаптерах предусмотрен так называемый циркулярный режим. В этом режиме адаптер принимает все пакеты, приходящие к нему, независимо от значения поля адреса приемника. Такой режим используется, например, для проведения диагностики сети, измерения ее производительности, контроля ошибок передачи. При этом один компьютер принимает и контролирует все пакеты, проходящие по сети, но сам ничего не передает. В данном режиме работают сетевые адаптеры мостов и коммутаторы, которые должны обрабатывать перед ретрансляцией все пакеты, приходящие к ним.

## Методы управления обменом

Сеть всегда объединяет несколько абонентов, каждый из которых имеет право передавать свои пакеты. Но, как уже отмечалось, по одному кабелю одновременно передавать два (или более) пакета нельзя, иначе может возникнуть конфликт (коллизия), который приведет к искажению либо потере обоих пакетов (или всех пакетов, участвующих в конфликте). Значит, надо каким-то образом установить очередность доступа к сети (захвата сети) всеми абонентами, желающими передавать. Это относится, прежде всего, к сетям с топологиями «шина» и «кольцо». Точно так же при топологии «звезда» необходимо установить очередность передачи пакетов периферийными абонентами, иначе центральный абонент просто не сможет справиться с их обработкой.

В сети обязательно применяется тот или иной *метод управления обменом* (*метод доступа, метод арбитража*), разрешающий или предотвращающий конфликты между абонентами. От эффективности работы выбранного метода управления обменом зависит очень многое: скорость обмена информацией между компьютерами, нагрузочная способность сети (способность работать с различными интенсивностями обмена), время реакции сети на внешние события и т.д. Метод управления – это один из важнейших параметров сети.

Тип метода управления обменом во многом определяется особенностями топологии сети. Но в то же время он не привязан жестко к топологии, как нередко принято считать.

Методы управления обменом в локальных сетях делятся на две группы:

- *Централизованные методы*, в которых все управление обменом сосредоточенно в одном месте. Недостатки таких методов: неустойчивость к отказам центра, малая гибкость управления (центр обычно не может оперативно реагировать на все события в сети). Достоинство централизованных методов – отсутствие конфликтов, так как центр всегда предоставляет право на передачу только одному абоненту, и ему не с кем конфликтовать.
- *Децентрализованные методы*, в которых отсутствует центр управления. Всеми вопросами управления, в том числе предотвращением, обнаружением и разрешением конфликтов, занимаются все абоненты сети. Главные достоинства децентрализованных методов: высокая устойчивость к отказам и большая гибкость. Однако в данном случае возможны конфликты, которые надо разрешать.

Существует и другое деление методов управления обменом, относящееся, главным образом, к децентрализованным методам:

- Детерминированные методы определяют четкие правила, по которым чередуются захватывающие сеть абоненты. Абоненты имеют

определенную систему приоритетов, причем приоритеты эти различны для всех абонентов. При этом, как правило, конфликты полностью исключены (или маловероятны), но некоторые абоненты могут дожидаться своей очереди на передачу слишком долго. К детерминированным методам относится, например, маркерный доступ (сети Token-Ring, FDDI), при котором право передачи передается по эстафете от абонента к абоненту.

- Случайные методы подразумевают случайное чередование передающих абонентов. При этом возможность конфликтов подразумевается, но предлагаются способы их разрешения. Случайные методы значительно хуже, чем детерминированные, работают при больших информационных потоках в сети (при большом трафике сети) и не гарантируют абоненту величину времени доступа. В то же время они обычно более устойчивы к отказам сетевого оборудования и более эффективно используют сеть при малой интенсивности обмена. Пример случайного метода – CSMA/CD (сеть Ethernet).

Для трех основных топологий характерны три наиболее типичных метода управления обменом.

### Управление обменом в сети с топологией «звезда»

Для топологии «звезда» лучше всего подходит централизованный метод управления. Это связано с тем, что все информационные потоки проходят через центр, и именно этому центру логично доверить управление обменом в сети. Причем не так важно, что находится в центре звезды: компьютер (центральный абонент), как на рис. 1.6, или же специальный концентратор, управляющий обменом, но сам не участвующий в нем. В данном случае речь идет уже не о пассивной звезде (рис. 1.11), а о некой промежуточной ситуации, когда центр не является полноценным абонентом, но управляет обменом. Это, к примеру, реализовано в сети 100VG AnyLAN.

Самый простейший централизованный метод состоит в следующем.

Периферийные абоненты, желающие передать свой пакет (или, как еще говорят, имеющие заявки на передачу), посылают центру свои запросы (управляющие пакеты или специальные сигналы). Центр же предоставляет им право передачи пакета в порядке очередности, например, по их физическому расположению в звезде по часовой стрелке. После окончания передачи пакета каким-то абонентом право передавать получит следующий по порядку (по часовой стрелке) абонент, имеющий заявку на передачу (рис. 4.8). Например, если передает второй абонент, то после него имеет право на передачу третий. Если же третьему абоненту не надо передавать, то право на передачу переходит к четвертому и т.д.

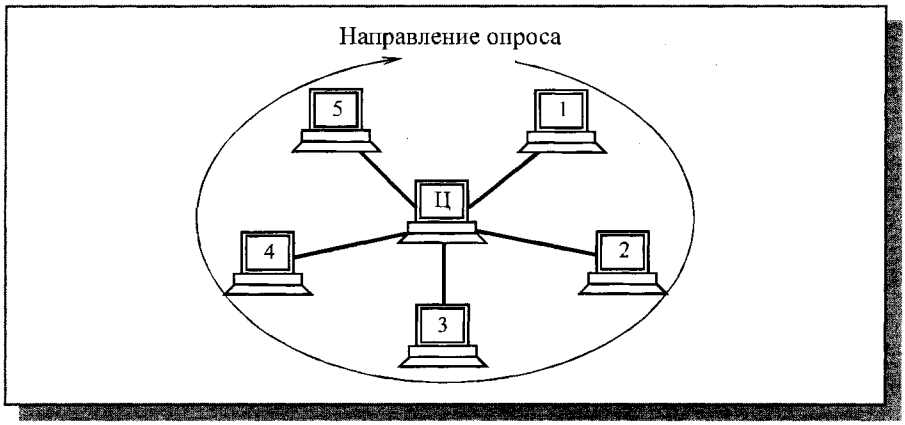



**Рис. 4.8.** Централизованный метод управления обменом в сети с топологией «звезда»

В этом случае говорят, что абоненты имеют географические приоритеты (по их физическому расположению). В каждый конкретный момент наивысшим приоритетом обладает следующий по порядку абонент, но в пределах полного цикла опроса ни один из абонентов не имеет никаких преимуществ перед другими. Никому не придется ждать своей очереди слишком долго. Максимальная величина времени доступа для любого абонента в этом случае будет равна суммарному времени передачи пакетов всех абонентов сети кроме данного. Для топологии, показанной на рис. 4.8, она составит четыре длительности пакета. Никаких столкновений пакетов при этом методе в принципе быть не может, так как все решения о доступе принимаются в одном месте.

Рассмотренный метод управления можно назвать методом с пассивным центром, так как центр пассивно прослушивает всех абонентов. Возможен и другой принцип реализации централизованного управления (его можно назвать методом с активным центром).

В этом случае центр посылает запросы о готовности передавать (управляющие пакеты или специальные сигналы) по очереди всем периферийным абонентам. Тот периферийный абонент, который хочет передавать (первый из опрошенных) посылает ответ (или же сразу начинает свою передачу). В дальнейшем центр проводит сеанс обмена именно с ним. После окончания этого сеанса центральный абонент продолжает опрос периферийных абонентов по кругу (как на рис. 4.8). Если желает передавать центральный абонент, он передает вне очереди.

Как в первом, так и во втором случае никаких конфликтов быть не может (решение принимает единый центр, которому не с кем конфликтовать). Если все абоненты активны, и заявки на передачу поступа-

ют интенсивно, то все они будут передавать строго по очереди. Но центр должен быть исключительно надежен, иначе будет парализован весь обмен. Механизм управления не слишком гибок, так как центр работает по жестко заданному алгоритму. К тому же скорость управления невысока. Ведь даже в случае, когда передает только один абонент, ему все равно приходится ждать после каждого переданного пакета, пока центр опросит всех остальных абонентов.

Как правило, централизованные методы управления применяются в небольших сетях (с числом абонентов не более чем несколько десятков). В случае больших сетей нагрузка по управлению обменом на центр существенно возрастает.

### Управление обменом в сети с топологией «шина»

При топологии «шина» также возможно централизованное управление. При этом один из абонентов («центральный») посылает по шине всем остальным («периферийным») запросы (управляющие пакеты), выясняя, кто из них хочет передать, затем разрешает передачу одному из абонентов. Абонент, получивший право на передачу, по той же шине передает свой информационный пакет тому абоненту, которому хочет. А после окончания передачи передававший абонент все по той же шине сообщает «центру», что он закончил передачу (управляющим пакетом), и «центр» снова начинает опрос (рис. 4.9).

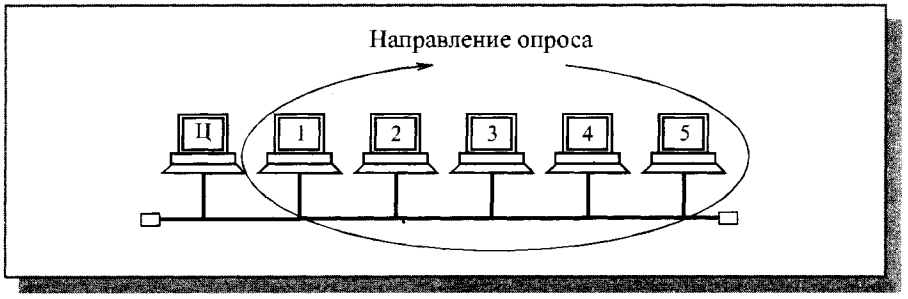



**Рис. 4.9.** Централизованное управление в сети с топологией «шина»

Преимущества и недостатки такого управления – те же самые, что и в случае централизованно управляемой звезды. Единственное отличие состоит в том, что центр здесь не пересылает информацию от одного абонента к другому, как в топологии активная «звезда», а только управляет обменом.

Гораздо чаще в шине используется децентрализованное случайное управление, так как сетевые адаптеры всех абонентов в данном случае одинаковы, и именно этот метод наиболее органично подходит шине.

При выборе децентрализованного управления все абоненты имеют равные права доступа к сети, то есть особенности топологии совпадают с особенностями метода управления. Решение о том, когда можно передавать свой пакет, принимается каждым абонентом на месте, исходя только из анализа состояния сети. В данном случае возникает конкуренция между абонентами за захват сети, и, следовательно, возможны конфликты между ними и искажения передаваемой информации из-за наложения пакетов.

Существует множество алгоритмов доступа или, как еще говорят, сценариев доступа, порой очень сложных. Их выбор зависит от скорости передачи в сети, длины шины, загруженности сети (интенсивности обмена или трафика сети), используемого кода передачи.

Иногда для управления доступом к шине применяется дополнительная линия связи, что позволяет упростить аппаратуру контроллеров и методы доступа, но заметно увеличивает стоимость сети за счет удвоения длины кабеля и количества приемопередатчиков. Поэтому данное решение не получило широкого распространения.

Суть всех случайных методов управления обменом довольно проста.

Если сеть свободна (то есть никто не передает своих пакетов), то абонент, желающий передавать, сразу начинает свою передачу. Время доступа в этом случае равно нулю.

Если же в момент возникновения у абонента заявки на передачу сеть занята, то абонент, желающий передавать, ждет освобождения сети. В противном случае исказятся и пропадут оба пакета. После освобождения сети абонент, желающий передавать, начинает свою передачу.

Возникновение конфликтных ситуаций (столкновений пакетов, коллизий), в результате которых передаваемая информация искажается, возможно в двух случаях.

- При одновременном начале передачи двумя или более абонентами, когда сеть свободна (рис. 4.10). Это ситуация довольно редкая, но все-таки вполне возможная.
- При одновременном начале передачи двумя или более абонентами сразу после освобождения сети (рис. 4.11). Это ситуация наиболее типична, так как за время передачи пакета одним абонентом вполне может возникнуть несколько новых заявок на передачу у других абонентов.

Существующие случайные методы управления обменом (арбитража) различаются тем, как они предотвращают возможные конфликты или же разрешают уже возникшие. Ни один конфликт не должен нарушать обмен, все абоненты должны, в конце концов, передать свои пакеты.

В процессе развития локальных сетей было разработано несколько разновидностей случайных методов управления обменом.

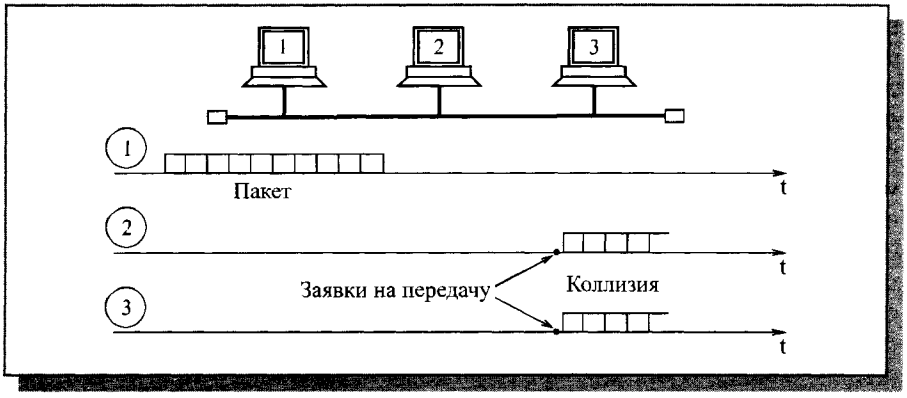



**Рис. 4.10.** Коллизии в случае начала передачи при свободной сети

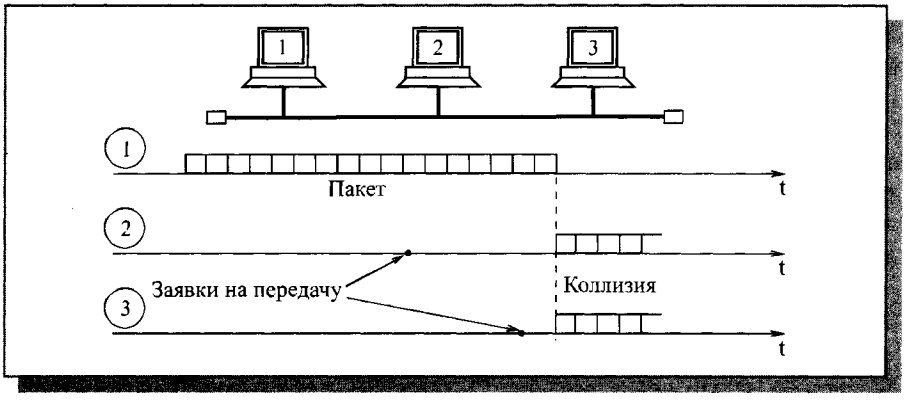



**Рис. 4.11.** Коллизии в случае начала передачи после освобождения сети

Например, был предложен метод, при котором не все передающие абоненты распознают коллизию, а только те, которые имеют меньшие приоритеты. Абонент с максимальным приоритетом из всех, начавших передачу, закончит передачу своего пакета без ошибок. Остальные, обнаружив коллизию, прекратят свою передачу и будут ждать освобождения сети для новой попытки. Для контроля коллизии каждый передающий абонент производит побитное сравнение передаваемой им в сеть информации и данных, присутствующих в сети. Побеждает тот абонент, заголовок пакета которого дольше других не искажается от коллизии. Этот метод, называемый децентрализованным кодовым приоритетным методом, отличается низким быстродействием и сложностью реализации.

При другом методе управления обменом каждый абонент начинает свою передачу после освобождения сети не сразу, а, выдержав свою,

строго индивидуальную задержку, что предотвращает коллизии после освобождения сети и тем самым сводит к минимуму общее количество коллизий. Максимальным приоритетом в этом случае будет обладать абонент с минимальной задержкой. Столкновения пакетов возможны только тогда, когда два и более абонентов захотели передавать одновременно при свободной сети. Этот метод, называемый децентрализованным временным приоритетным методом, хорошо работает только в небольших сетях, так как каждому абоненту нужно обеспечить свою индивидуальную задержку.

В обоих случаях имеется система приоритетов, все же данные методы относятся к случайным, так как исход конкуренции невозможно предсказать. Случайные приоритетные методы ставят абонентов в неравные условия при большой интенсивности обмена по сети, так как высокоприоритетные абоненты могут надолго заблокировать сеть для низкоприоритетных абонентов.

Чаще всего система приоритетов в методе управления обменом в шине отсутствует полностью. Именно так работает наиболее распространенный стандартный метод управления обменом **CSMA/CD** (Carrier Sense Multiple Access with Collision Detection – множественный доступ с контролем несущей и обнаружением коллизий), используемый в сети Ethernet. Его главное достоинство в том, что все абоненты полностью равноправны, и ни один из них не может надолго заблокировать обмен другому (как в случае наличия приоритетов). В этом методе коллизии не предотвращаются, а разрешаются.

Суть метода состоит в том, что абонент начинает передавать сразу, как только он выяснит, что сеть свободна. Если возникают коллизии, то они обнаруживаются всеми передающими абонентами. После чего все абоненты прекращают свою передачу и возобновляют попытку начать новую передачу пакета через временной интервал, длительность которого выбирается случайным образом. Поэтому повторные коллизии мало вероятны. Подробнее метод CSMA/CD будет рассмотрен в главе 7.

Еще один распространенный метод случайного доступа – **CSMA/CA** (Carrier Sense Multiple Access with Collision Avoidance – множественный доступ с контролем несущей и избежанием коллизий) применяющийся, например, в сети Apple LocalTalk. Абонент, желающий передавать и обнаруживший освобождение сети, передает сначала короткий управляющий пакет запроса на передачу. Затем он заданное время ждет ответного короткого управляющего пакета подтверждения запроса от абонента-приемника. Если ответа нет, передача откладывается. Если ответ получен, передается пакет. Коллизии полностью не устраняются, но в основном сталкиваются управляющие пакеты. Столкновения информационных пакетов выявляются на более высоких уровнях протокола.

Подобные методы будут хорошо работать только при не слишком большой интенсивности обмена по сети. Считается, что приемлемое качество связи обеспечивается при нагрузке не выше 30–40% (то есть когда сеть занята передачей информации примерно на 30–40% всего времени). При большей нагрузке повторные столкновения учащаются настолько, что наступает так называемый коллапс или крах сети, представляющий собой резкое падение ее производительности.

Недостаток всех случайных методов состоит еще и в том, что они не гарантируют величину времени доступа к сети, которая зависит не только от выбора задержки между попытками передачи, но и от общей загруженности сети. Поэтому, например, в сетях, выполняющих задачи управления оборудованием (на производстве, в научных лабораториях), где требуется быстрая реакция на внешние события, сети со случайными методами управления используются довольно редко.

При любом случайном методе управления обменом, использующем детектирование коллизии (в частности, при CSMA/CD), возникает вопрос о том, какой должна быть минимальная длительность пакета, чтобы коллизию обнаружили все начавшие передавать абоненты. Ведь сигнал по любой физической среде распространяется не мгновенно, и при больших размерах сети (диаметре сети) задержка распространения может составлять десятки и сотни микросекунд. Кроме того, информацию об одновременно происходящих событиях разные абоненты получают не в одно время. С тем чтобы рассчитать минимальную длительность пакета, следует обратиться к рис. 4.12.

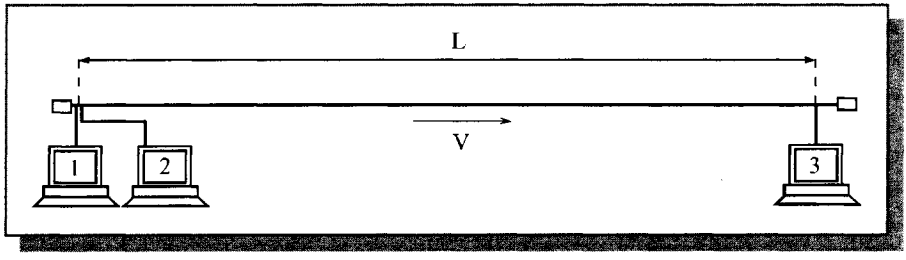



**Рис. 4.12.** Расчет минимальной длительности пакета

Пусть L – полная длина сети, V – скорость распространения сигнала в используемом кабеле. Допустим, абонент 1 закончил свою передачу, а абоненты 2 и 3 захотели передавать во время передачи абонента 1 и ждали освобождения сети.

После освобождения сети абонент 2 начнет передавать сразу же, так как он расположен рядом с абонентом 1. Абонент 3 после освобождения сети узнает об этом событии и начнет свою передачу через временной ин-

тервал прохождения сигнала по всей длине сети, то есть через время L/V. При этом пакет от абонента 3 дойдет до абонента 2 еще через временной интервал L/V после начала передачи абонентом 3 (обратный путь сигнала). К этому моменту передача пакета абонентом 2 не должна закончиться, иначе абонент 2 так и не узнает о столкновении пакетов (о коллизии), в результате чего будет передан неправильный пакет.

Получается, что минимально допустимая длительность пакета в сети должна составлять 2L/V, то есть равняться удвоенному времени распространения сигнала по полной длине сети (или по пути наибольшей длины в сети). Это время называется двойным или *круговым временем задержки* сигнала в сети или PDV (Path Delay Value). Этот же временной интервал можно рассматривать как универсальную меру одновременности любых событий в сети.

Стандартом на сеть задается как раз величина PDV, определяющая минимальную длину пакета, и из нее уже рассчитывается допустимая длина сети. Дело в том, что скорость распространения сигнала в сети для разных кабелей отличается. Кроме того, надо еще учитывать задержки сигнала в различных сетевых устройствах. Расчетам допустимых конфигураций сети Ethernet посвящена глава 10.

Отдельно следует остановиться на том, как сетевые адаптеры распознают коллизию в кабеле шины, то есть столкновение пакетов. Ведь простое побитное сравнение передаваемой абонентом информации с той, которая реально присутствует в сети, возможно только в случае самого простого кода NRZ, используемого довольно редко. При применении манчестерского кода, который обычно подразумевается в случае метода управления обменом CSMA/CD, требуется принципиально другой подход.

Как уже отмечалось, сигнал в манчестерском коде всегда имеет постоянную составляющую, равную половине размаха сигнала (если один из двух уровней сигнала — нулевой). Однако в случае столкновения двух и более пакетов (при коллизии) это правило выполняться не будет. Постоянная составляющая суммарного сигнала в сети будет обязательно больше или меньше половины размаха (рис. 4.13). Ведь пакеты всегда отличаются друг от друга и к тому же сдвинуты друг относительно друга во времени. Именно по выходу уровня постоянной составляющей за установленные пределы и определяет каждый сетевой адаптер наличие коллизии в сети.

Задача обнаружения коллизии существенно упрощается, если используется не истинная шина, а равноценная ей пассивная звезда (рис. 4.14).

При этом каждый абонент соединяется с центральным концентратором, как правило, двумя кабелями, каждый из которых передает информацию в своем направлении. Во время передачи своего пакета абоненту

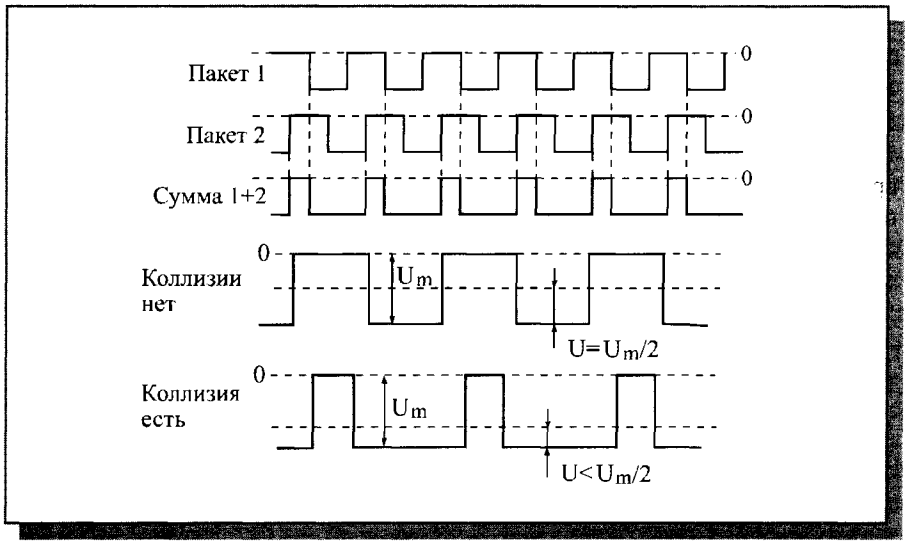



**Рис. 4.13.** Определение факта коллизии в шине при использовании манчестерского кода

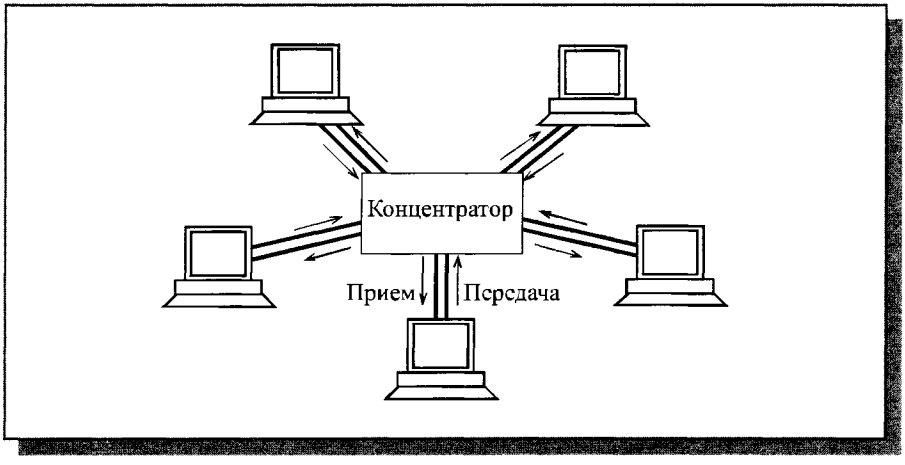



**Рис. 4.14.** Обнаружение коллизии в сети пассивная *звезда*

достаточно всего лишь контролировать, не приходит ли ему в данный момент по встречному кабелю (приемному) другой пакет. Если встречный пакет приходит, то детектируется коллизия. Точно так же обнаруживает коллизии и концентратор.

## Управление обменом в сети с топологией «кольцо»

Кольцевая топология имеет свои особенности при выборе метода управления обменом. В этом случае важно то, что любой пакет, посланный по кольцу, последовательно пройдя всех абонентов, через некоторое время возвратится в ту же точку, к тому же абоненту, который его передавал (так как топология замкнутая). Здесь нет одновременного распространения сигнала в две стороны, как в топологии шина. Как уже отмечалось, сети с топологией кольцо бывают однонаправленными и двунаправленными. Наиболее распространены однонаправленные.

В сети с топологией кольцо можно использовать различные централизованные методы управления (как в звезде), а также методы случайного доступа (как в шине), но чаще выбирают все-таки специфические методы управления, в наибольшей степени соответствующие особенностям кольца.

Самые популярные методы управления в кольцевых сетях — *маркерные* (эстафетные), те, которые используют маркер (эстафету) – небольшой управляющий пакет специального вида. Именно эстафетная передача маркера по кольцу позволяет передавать право на захват сети от одного абонента к другому. Маркерные методы относятся к децентрализованным и детерминированным методам управления обменом в сети. В них нет явно выраженного центра, но существует четкая система приоритетов, и потому не бывает конфликтов.

Работа маркерного метода управления в сети с топологией «кольцо» представлена на рис. 4.15.

По кольцу непрерывно ходит специальный управляющий пакет минимальной длины, маркер, предоставляющий абонентам право передавать свой пакет. Алгоритм действий абонентов:

1. Абонент 1, желающий передать свой пакет, должен дождаться прихода к нему свободного маркера. Затем он присоединяет к маркеру свой пакет, помечает маркер как занятый и отправляет эту посылку следующему по кольцу абоненту.
2. Все остальные абоненты (2, 3, 4), получив маркер с присоединенным пакетом, проверяют, им ли адресован пакет. Если пакет адресован не им, то они передают полученную посылку (маркер + пакет) дальше по кольцу.
3. Если какой-то абонент (в данном случае это абонент 3) распознает пакет как адресованный ему, то он его принимает, устанавливает в маркере бит подтверждения приема и передает посылку (маркер + пакет) дальше по кольцу.
4. Передававший абонент 1 получает свою посылку, прошедшую по всему кольцу, обратно, помечает маркер как свободный, удаляет из сети свой пакет и посылает свободный маркер дальше по кольцу.

Абонент, желающий передавать, ждет этого маркера, и все повторяется снова.

Приоритет при данном методе управления получается географический, то есть право передачи после освобождения сети переходит к следующему по направлению кольца абоненту от последнего передававшего абонента. Но эта система приоритетов работает только при большой интенсивности обмена. При малой интенсивности обмена все абоненты равноправны, и время доступа к сети каждого из них определяется только положением маркера в момент возникновения заявки на передачу.

В чем-то рассматриваемый метод похож на метод опроса (централизованный), хотя явно выделенного центра здесь не существует. Однако некий центр обычно все-таки присутствует. Один из абонентов (или специальное устройство) должен следить, чтобы маркер не потерялся в процессе прохождения по кольцу (например, из-за действия помех или сбоя в работе какого-то абонента, а также из-за подключения и отключения абонентов). В противном случае механизм доступа работать не будет.

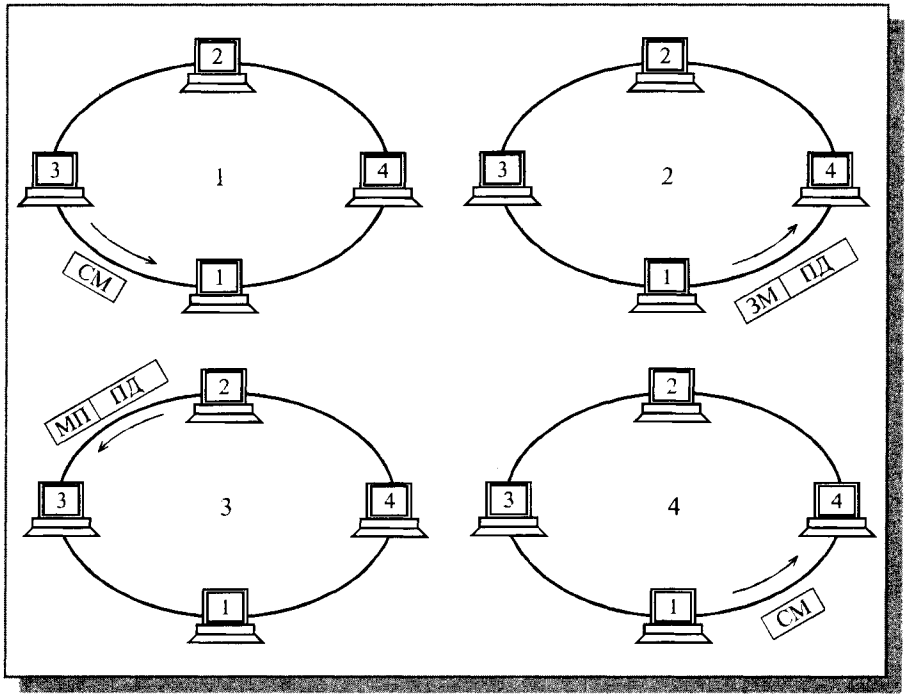



**Рис. 4.15.** Маркерный метод управления обменом
(СМ — свободный маркер, ЗМ — занятый маркер,
МП — занятый маркер с подтверждением, ПД — пакет данных)

Следовательно, надежность управления в данном случае снижается (выход центра из строя приводит к полной дезорганизации обмена). Существуют специальные средства для повышения надежности и восстановления центра контроля маркера.

Основное преимущество маркерного метода перед CSMA/CD состоит в гарантированной величине времени доступа. Его максимальная величина, как и при централизованном методе, составит $(N-1) \cdot t_{пк}$, где N – полное число абонентов в сети, $t_{пк}$ – время прохождения пакета по кольцу. Вообще, маркерный метод управления обменом при большой интенсивности обмена в сети (загруженность более 30–40%) гораздо эффективнее случайных методов. Он позволяет сети работать с большей нагрузкой, которая теоретически может даже приближаться к 100%.

Метод маркерного доступа используется не только в кольце (например, в сети IBM Token Ring или FDDI), но и в шине (в частности, сеть Arcnet-BUS), а также в пассивной звезде (к примеру, сеть Arcnet-STAR). В этих случаях реализуется не физическое, а логическое кольцо, то есть все абоненты последовательно передают друг другу маркер, и эта цепочка передачи маркеров замкнута в кольцо (рис. 4.16). При этом совмещаются достоинства физической топологии «шина» и маркерного метода управления.

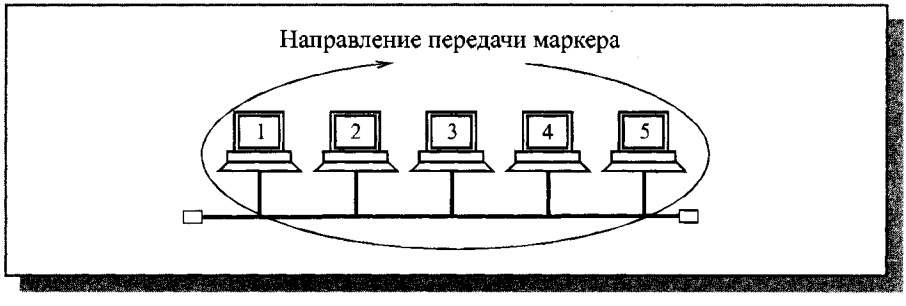



**Рис. 4.16.** Применение маркерного метода управления в «шине»

# Глава 4. Уровни сетевой архитектуры

## Лекция 5. Модель OSI. Нижние уровни

**В этой лекции дается представление о стандартной модели взаимодействия открытых систем OSI, уровнях функций, выполняемых при взаимодействии по сети, возможностях сетевых адаптеров и промежуточных сетевых устройств.**

**Ключевые слова:** модель OSI, уровни модели, подуровни LLC и MAC, сетевые адаптеры (NIC), репитеры, трансиверы, концентраторы, коммутаторы, мосты, маршрутизаторы.

В сети производится множество операций, обеспечивающих передачу данных от компьютера к компьютеру. Пользователя не интересует, как именно это происходит, ему необходим доступ к приложению или компьютерному ресурсу, расположенному в другом компьютере сети. В действительности же вся передаваемая информация проходит много этапов обработки.

Прежде всего, она разбивается на блоки, каждый из которых снабжается управляющей информацией. Полученные блоки оформляются в виде сетевых пакетов, потом эти пакеты кодируются, передаются с помощью электрических или световых сигналов по сети в соответствии с выбранным методом доступа, затем из принятых пакетов вновь восстанавливаются заключенные в них блоки данных, блоки соединяются в данные, которые и становятся доступны другому приложению. Это, конечно, упрощенное описание происходящих процессов.

Часть из указанных процедур реализуются только программно, другая часть – аппаратно, а какие-то операции могут выполняться как программами, так и аппаратурой.

Упорядочить все выполняемые процедуры, разделить их на уровни и подуровни, взаимодействующие между собой, как раз и призваны модели сетей. Эти модели позволяют правильно организовать взаимодействие как абонентам внутри одной сети, так и самым разным сетям на различных уровнях. В настоящее время наибольшее распространение получила так называемая эталонная модель обмена информацией открытой системы OSI (Open System Interchange). Под термином «открытая система» понимается не замкнутая в себе система, имеющая возможность взаимодействия с какими-то другими системами (в отличие от закрытой системы).

## Эталонная модель OSI

Модель OSI была предложена Международной организацией стандартов ISO (International Standards Organization) в 1984 году. С тех пор ее используют (более или менее строго) все производители сетевых продуктов. Как и любая универсальная модель, OSI довольно громоздка, избыточна, и не слишком гибка. Поэтому реальные сетевые средства, предлагаемые различными фирмами, не обязательно придерживаются принятого разделения функций. Однако знакомство с моделью OSI позволяет лучше понять, что же происходит в сети.

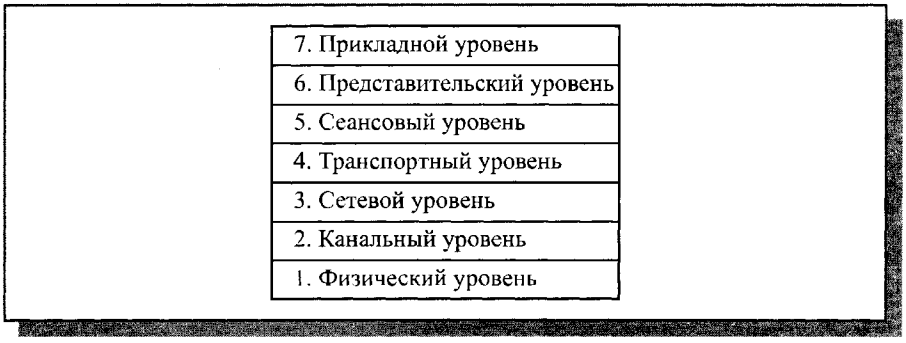



**Рис. 5.1.** Семь уровней модели OSI

Все сетевые функции в модели разделены на 7 уровней (рис. 5.1). При этом вышестоящие уровни выполняют более сложные, глобальные задачи, для чего используют в своих целях нижестоящие уровни, а также управляют ими. Цель нижестоящего уровня – предоставление услуг вышестоящему уровню, причем вышестоящему уровню не важны детали выполнения этих услуг. Нижестоящие уровни выполняют более простые и конкретные функции. В идеале каждый уровень взаимодействует только с теми, которые находятся рядом с ним (выше и ниже него). Верхний уровень соответствует прикладной задаче, работающему в данный момент приложению, нижний – непосредственной передаче сигналов по каналу связи.

Модель OSI относится не только к локальным сетям, но и к любым сетям связи между компьютерами или другими абонентами. В частности, функции сети Интернет также можно поделить на уровни в соответствии с моделью OSI. Принципиальные отличия локальных сетей от глобальных, с точки зрения модели OSI, наблюдаются только на нижних уровнях модели.

Функции, входящие в показанные на рис 5.1 уровни, реализуются каждым абонентом сети. При этом каждый уровень на одном абоненте работает так, как будто он имеет прямую связь с соответствующим уровнем другого абонента. Между одноименными уровнями абонентов сети

существует виртуальная (логическая) связь, например, между прикладными уровнями взаимодействующих по сети абонентов. Реальную же, физическую связь (кабель, радиоканал) абоненты одной сети имеют только на самом нижнем, первом, физическом уровне. В передающем абоненте информация проходит все уровни, начиная с верхнего и заканчивая нижним. В принимающем абоненте полученная информация совершает обратный путь: от нижнего уровня к верхнему (рис. 5.2).

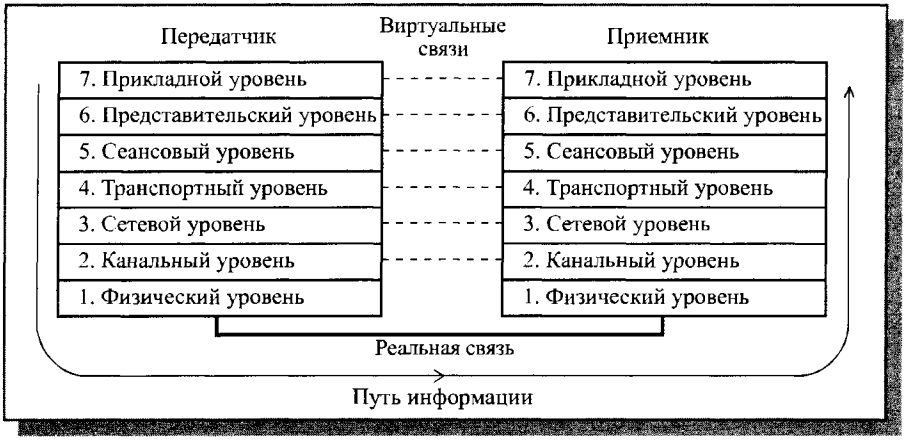



**Рис. 5.2.** Путь информации от абонента к абоненту

Данные, которые необходимо передать по сети, на пути от верхнего (седьмого) уровня до нижнего (первого) проходят процесс инкапсуляции (см. рис. 4.6). Каждый нижеследующий уровень не только производит обработку данных, приходящих с более высокого уровня, но и снабжает их своим заголовком, а также служебной информацией. Такой процесс обрастания служебной информацией продолжается до последнего (физического) уровня. На физическом уровне вся эта многооболочечная конструкция передается по кабелю приемнику. Там она проделывает обратную процедуру декапсуляции, то есть при передаче на вышестоящий уровень убирается одна из оболочек. Верхнего седьмого уровня достигают уже данные, освобожденные от всех оболочек, то есть от всей служебной информации нижестоящих уровней. При этом каждый уровень принимающего абонента производит обработку данных, полученных с нижеследующего уровня в соответствии с убираемой им служебной информацией.

Если на пути между абонентами в сети включаются некие промежуточные устройства (например, трансиверы, репитеры, концентраторы, коммутаторы, маршрутизаторы), то и они тоже могут выполнять функции, входящие в нижние уровни модели OSI. Чем больше сложность промежуточного устройства, тем больше уровней оно захватывает. Но любое

промежуточное устройство должно принимать и возвращать информацию на нижнем, физическом уровне. Все внутренние преобразования данных должны производиться дважды и в противоположных направлениях (рис. 5.3). Промежуточные сетевые устройства в отличие от полноценных абонентов (например, компьютеров) работают только на нижних уровнях и к тому же выполняют двустороннее преобразование.

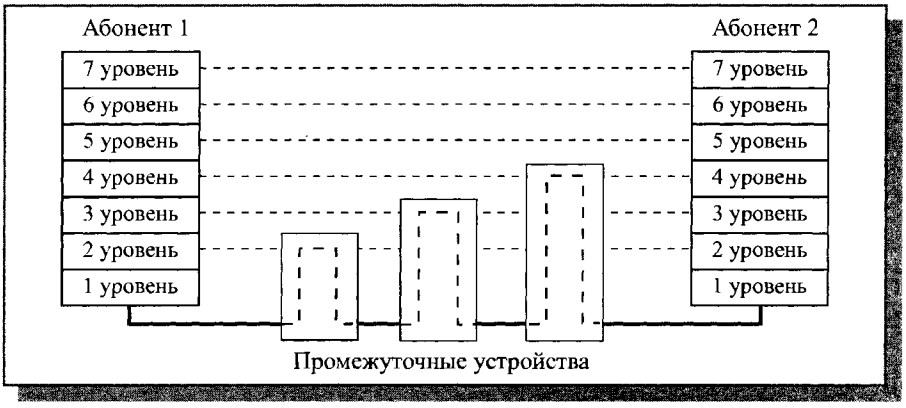



**Рис. 5.3.** Включение промежуточных устройств между абонентами сети

Рассмотрим подробнее функции разных уровней.

- **Прикладной (7) уровень** (Application Layer) или уровень приложений обеспечивает услуги, непосредственно поддерживающие приложения пользователя, например, программные средства передачи файлов, доступа к базам данных, средства электронной почты, службу регистрации на сервере. Этот уровень управляет всеми остальными шестью уровнями. Например, если пользователь работает с электронными таблицами Excel и решает сохранить рабочий файл в своей директории на сетевом файл-сервере, то прикладной уровень обеспечивает перемещение файла с рабочего компьютера на сетевой диск прозрачно для пользователя.
- **Представительский (6) уровень** (Presentation Layer) или уровень представления данных определяет и преобразует форматы данных и их синтаксис в форму, удобную для сети, то есть выполняет функцию переводчика. Здесь же производится шифрование и дешифрирование данных, а при необходимости – и их сжатие. Стандартные форматы существуют для текстовых файлов (ASCII, EBCDIC, HTML), звуковых файлов (MIDI, MPEG, WAV), рисунков (JPEG. GIF, TIFF), видео (AVI). Все преобразования форматов делаются на представительском уровне. Если данные передаются в виде двоичного кода, то преобразования формата не требуется.

- **Сеансовый (5) уровень** (Session Layer) управляет проведением сеансов связи (то есть устанавливает, поддерживает и прекращает связь). Этот уровень предусматривает три режима установки сеансов: симплексный (передача данных в одном направлении), полудуплексный (передача данных поочередно в двух направлениях) и полнодуплексный (передача данных одновременно в двух направлениях). Сеансовый уровень может также вставлять в поток данных специальные контрольные точки, которые позволяют контролировать процесс передачи при разрыве связи. Этот же уровень распознает логические имена абонентов, контролирует предоставленные им права доступа.
- **Транспортный (4) уровень** (Transport Layer) обеспечивает доставку пакетов без ошибок и потерь, а также в нужной последовательности. Здесь же производится разбивка на блоки передаваемых данных, помещаемые в пакеты, и восстановление принимаемых данных из пакетов. Доставка пакетов возможна как с установлением соединения (виртуального канала), так и без. Транспортный уровень является пограничным и связующим между верхними тремя, сильно зависящими от приложений, и тремя нижними уровнями, сильно привязанными к конкретной сети.
- **Сетевой (3) уровень** (Network Layer) отвечает за адресацию пакетов и перевод логических имен (логических адресов, например, IP-адресов или IPX-адресов) в физические сетевые MAC-адреса (и обратно). На этом же уровне решается задача выбора маршрута (пути), по которому пакет доставляется по назначению (если в сети имеется несколько маршрутов). На сетевом уровне действуют такие сложные промежуточные сетевые устройства, как маршрутизаторы.
- **Канальный (2) уровень** или уровень управления линией передачи (Data link Layer) отвечает за формирование пакетов (кадров) стандартного для данной сети (Ethernet, Token-Ring, FDDI) вида, включающих начальное и конечное управляющие поля. Здесь же производится управление доступом к сети, обнаруживаются ошибки передачи путем подсчета контрольных сумм, и производится повторная пересылка приемнику ошибочных пакетов. Канальный уровень делится на два подуровня: верхний LLC и нижний MAC. На канальном уровне работают такие промежуточные сетевые устройства, как, например, коммутаторы.
- **Физический (1) уровень** (Physical Layer) – это самый нижний уровень модели, который отвечает за кодирование передаваемой информации в уровни сигналов, принятые в используемой среде передачи, и обратное декодирование. Здесь же определяются требования к соединителям, разъемам, электрическому согласованию, заземлению, защите от помех и т.д. На физическом уровне работают такие сетевые устройства, как трансиверы, репитеры и репитерные концентраторы.

Большинство функций двух нижних уровней модели (1 и 2) обычно реализуются аппаратно (часть функций уровня 2 – программным драйвером сетевого адаптера). Именно на этих уровнях определяется скорость передачи и топология сети, метод управления обменом и формат пакета, то есть то, что имеет непосредственное отношение к типу сети, например, Ethernet, Token-Ring, FDDI, 100VG-AnyLAN. Более высокие уровни, как правило, не работают напрямую с конкретной аппаратурой, хотя уровни 3, 4 и 5 еще могут учитывать ее особенности. Уровни 6 и 7 никак не связаны с аппаратурой, замены одного типа аппаратуры на другой они не замечают.

Как уже отмечалось, в уровне 2 (канальном) нередко выделяют два подуровня (sublayers) LLC и MAC (рис. 5.4):

- Верхний подуровень (LLC – Logical Link Control) осуществляет управление логической связью, то есть устанавливает виртуальный канал связи. Строго говоря, эти функции не связаны с конкретным типом сети, но часть из них все же возлагается на аппаратуру сети (сетевой адаптер). Другая часть функций подуровня LLC выполняется программой драйвера сетевого адаптера. Подуровень LLC отвечает за взаимодействие с уровнем 3 (сетевым).
- Нижний подуровень (MAC – Media Access Control) обеспечивает непосредственный доступ к среде передачи информации (каналу связи). Он напрямую связан с аппаратурой сети. Именно на подуровне MAC осуществляется взаимодействие с физическим уровнем. Здесь производится контроль состояния сети, повторная передача пакетов заданное число раз при коллизиях, прием пакетов и проверка правильности передачи.

Помимо модели OSI существует также модель IEEE Project 802, принятая в феврале 1980 года (отсюда и число 802 в названии), которую можно рассматривать как модификацию, развитие, уточнение модели OSI.

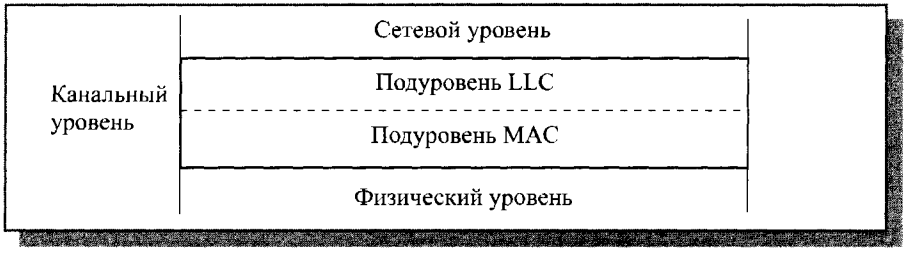



**Рис. 5.4.** Подуровни LLC и MAC канального уровня

Стандарты, определяемые этой моделью (так называемые 802-спецификации) относятся к нижним двум уровням модели OSI и делятся на двенадцать категорий, каждой из которых присвоен свой номер:

802.1 – объединение сетей с помощью мостов и коммутаторов.
802.2 – управление логической связью на подуровне LLC.
802.3 – локальная сеть с методом доступа CSMA/CD и топологией шина (Ethernet).
802.4 – локальная сеть с топологией «шина» и маркерным доступом (Token-Bus).
802.5 – локальная сеть с топологией «кольцо» и маркерным доступом (Token-Ring).
802.6 – городская сеть (Metropolitan Area Network, MAN) с расстояниями между абонентами более 5 км.
802.7 – широкополосная технология передачи данных.
802.8 – оптоволоконная технология.
802.9 – интегрированные сети с возможностью передачи речи и данных.
802.10 – безопасность сетей, шифрование данных.
802.11 – беспроводная сеть по радиоканалу (WLAN – Wireless LAN).
802.12 – локальная сеть с централизованным управлением доступом по приоритетам запросов и топологией «звезда» (100VG-AnyLAN).

## Аппаратура локальных сетей

Аппаратура локальных сетей обеспечивает реальную связь между абонентами. Выбор аппаратуры имеет важнейшее значение на этапе проектирования сети, так как стоимость аппаратуры составляет наиболее существенную часть от стоимости сети в целом, а замена аппаратуры связана не только с дополнительными расходами, но зачастую и с трудоемкими работами. К аппаратуре локальных сетей относятся:

- кабели для передачи информации;
- разъемы для присоединения кабелей;
- согласующие терминаторы;
- сетевые адаптеры;
- репитеры;
- трансиверы;
- концентраторы;
- мосты;
- маршрутизаторы;
- шлюзы.

О первых трех компонентах сетевой аппаратуры уже говорилось в предыдущих главах. А сейчас следует остановиться на функциях остальных компонентов.

**Сетевые адаптеры (они же контроллеры, карты, платы, интерфейсы, NIC – Network Interface Card)** – это основная часть аппаратуры локальной сети.

Назначение сетевого адаптера – сопряжение компьютера (или другого абонента) с сетью, то есть обеспечение обмена информацией между компьютером и каналом связи в соответствии с принятыми правилами обмена. Именно они реализуют функции двух нижних уровней модели OSI. Как правило, сетевые адаптеры выполняются в виде платы (рис. 5.5), вставляемой в слоты расширения системной магистрали (шины) компьютера (чаще всего PCI, ISA или PC-Card). Плата сетевого адаптера обычно имеет также один или несколько внешних разъемов для подключения к ней кабеля сети.

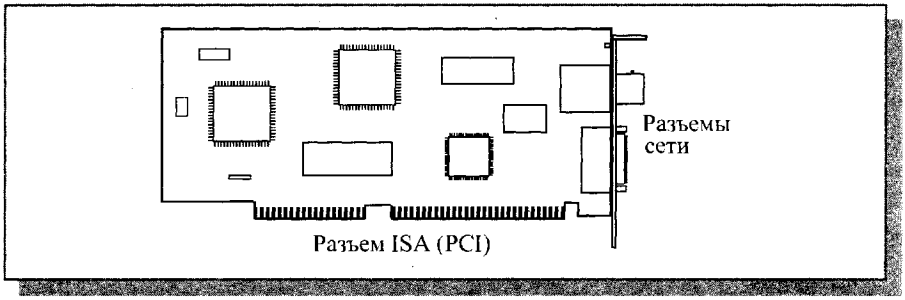



**Рис. 5.5.** Плата сетевого адаптера

Например, сетевые адаптеры Ethernet могут выпускаться со следующими наборами разъемов:

- TPO – разъем RJ-45 (для кабеля на витых парах по стандарту 10BASE-T).
- TPC – разъемы RJ-45 (для кабеля на витых парах 10BASE-T) и BNC (для коаксиального кабеля 10BASE2).
- TP – разъем RJ-45 (10BASE-T) и трансиверный разъем AUI.
- Combo – разъемы RJ-45 (10BASE-T), BNC (10BASE2), AUI.
- Coax – разъемы BNC, AUI.
- FL – разъем ST (для оптоволоконного кабеля 10BASE-FL).

Функции сетевого адаптера делятся на магистральные и сетевые. К магистральным относятся те функции, которые осуществляют взаимодействие адаптера с магистралью (системной шиной) компьютера (то есть опознание своего магистрального адреса, пересылка данных в компьютер и из компьютера, выработка сигнала прерывания работы компьютера и т.д.). Сетевые функции обеспечивают общение адаптера с сетью.

К основным сетевым функциям адаптеров относятся:

- гальваническая развязка компьютера и кабеля локальной сети (для этого обычно используется передача сигналов через импульсные трансформаторы);
- преобразование логических сигналов в сетевые (электрические или световые) и обратно;

- кодирование и декодирование сетевых сигналов, то есть прямое и обратное преобразование сетевых кодов передачи информации (например, манчестерский код);
- опознание принимаемых пакетов (выбор из всех приходящих пакетов тех, которые адресованы данному абоненту или всем абонентам сети одновременно);
- преобразование параллельного кода в последовательный при передаче и обратное преобразование при приеме;
- буферирование передаваемой и принимаемой информации в буферной памяти адаптера;
- организация доступа к сети в соответствии с принятым методом управления обменом;
- подсчет контрольной суммы пакетов при передаче и приеме.

Типичный алгоритм взаимодействия компьютера с сетевым адаптером выглядит следующим образом.

Если компьютер хочет передать пакет, то он сначала формирует этот пакет в своей памяти, затем пересылает его в буферную память сетевого адаптера и дает команду адаптеру на передачу. Адаптер анализирует текущее состояние сети и при первой же возможности выдает пакет в сеть (выполняет управление доступом к сети). При этом он производит преобразование информации из буферной памяти в последовательный вид для побитной передачи по сети, подсчитывает контрольную сумму, кодирует биты пакета в сетевой код и через узел гальванической развязки выдает пакет в кабель сети. Буферная память в данном случае позволяет освободить компьютер от контроля состояния сети, а также обеспечить требуемый для сети темп выдачи информации.

Если по сети приходит пакет, то сетевой адаптер через узел гальванической развязки принимает биты пакета, производит их декодирование из сетевого кода и сравнивает сетевой адрес приемника из пакета со своим собственным адресом. Адрес сетевого адаптера, как правило, устанавливается производителем адаптера. Если адрес совпадает, то сетевой адаптер записывает пришедший пакет в свою буферную память и сообщает компьютеру (обычно – сигналом аппаратного прерывания) о том, что пришел пакет и его надо читать. Одновременно с записью пакета производится подсчет контрольной суммы, что позволяет к концу приема сделать вывод, имеются ли ошибки в этом пакете. Буферная память в данном случае опять же позволяет освободить компьютер от контроля сети, а также обеспечить высокую степень готовности сетевого адаптера к приему пакетов.

Чаще всего сетевые функции выполняются специальными микросхемами высокой степени интеграции, что дает возможность снизить стоимость адаптера и уменьшить площадь его платы.

Некоторые адаптеры позволяют реализовать функцию удаленной загрузки, то есть поддерживать работу в сети бездисковых компьютеров, загружающих свою операционную систему прямо из сети. Для этого в состав таких адаптеров включается постоянная память с соответствующей программой загрузки. Правда, не все сетевые программные средства поддерживают данный режим работы.

Сетевой адаптер выполняет функции первого и второго уровней модели OSI (рис. 5.6).

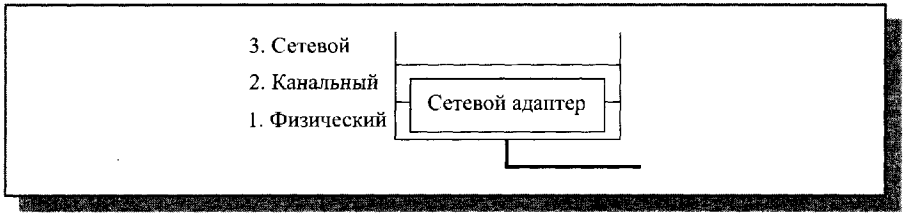



**Рис. 5.6.** Функции сетевого адаптера в модели OSI

Все остальные аппаратные средства локальных сетей (кроме адаптеров) имеют вспомогательный характер, и без них часто можно обойтись. Это сетевые промежуточные устройства.

**Трансиверы** или приемопередатчики (от английского TRANsmitter + reCEIVER) служат для передачи информации между адаптером и кабелем сети или между двумя сегментами (частями) сети. Трансиверы усиливают сигналы, преобразуют их уровни или преобразуют сигналы в другую форму (например, из электрической в световую и обратно). Трансиверами также часто называют встроенные в адаптер приемопередатчики.

**Репитеры** или повторители (repeater) выполняют более простую функцию, чем трансиверы. Они не преобразуют ни уровни сигналов, ни их физическую природу, а только восстанавливают ослабленные сигналы (их амплитуду и форму), приводя их к исходному виду. Цель такой ретрансляции сигналов состоит исключительно в увеличении длины сети (рис. 5.7). Однако часто репитеры выполняют и некоторые другие, вспомогательные функции, например, гальваническую развязку соединяемых сегментов и

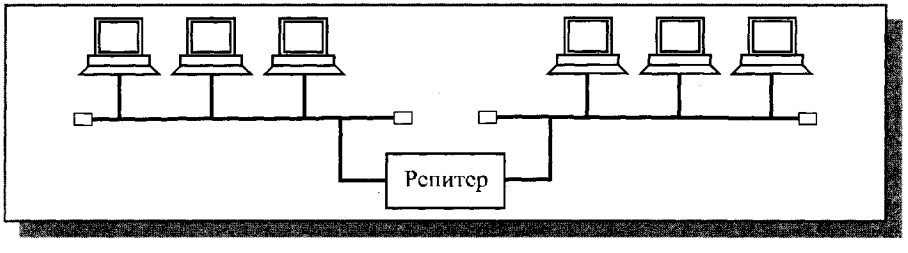



**Рис. 5.7.** Соединение репитером двух сегментов сети

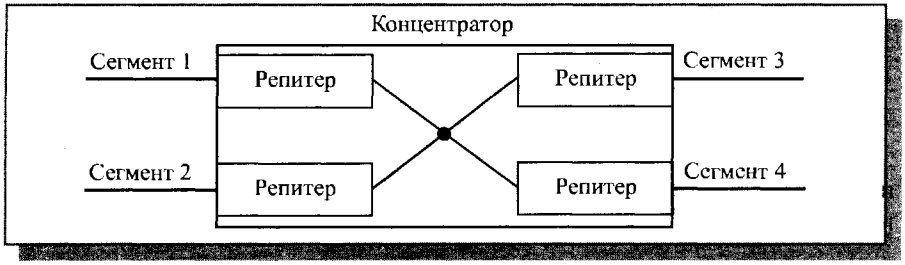



**Рис. 5.8.** Структура репитерного концентратора

оконечное согласование. Репитеры так же как трансиверы не производят никакой информационной обработки проходящих через них сигналов.

**Концентраторы** (хабы, hub), как следует из их названия, служат для объединения в сеть нескольких сегментов. Концентраторы (или репитерные концентраторы) представляют собой несколько собранных в едином конструктиве репитеров, они выполняют те же функции, что и репитеры (рис. 5.8).

Преимущество подобных концентраторов по сравнению с отдельными репитерами в том, что все точки подключения собраны в одном месте, это упрощает реконфигурацию сети, контроль и поиск неисправностей. К тому же все репитеры в данном случае питаются от единого качественного источника питания.

Концентраторы иногда вмешиваются в обмен, помогая устранять некоторые явные ошибки обмена. В любом случае они работают на первом уровне модели OSI, так как имеют дело только с физическими сигналами, с битами пакета и не анализируют содержимое пакета, рассматривая пакет как единое целое (рис. 5.9). На первом же уровне работают и трансиверы, и репитеры.

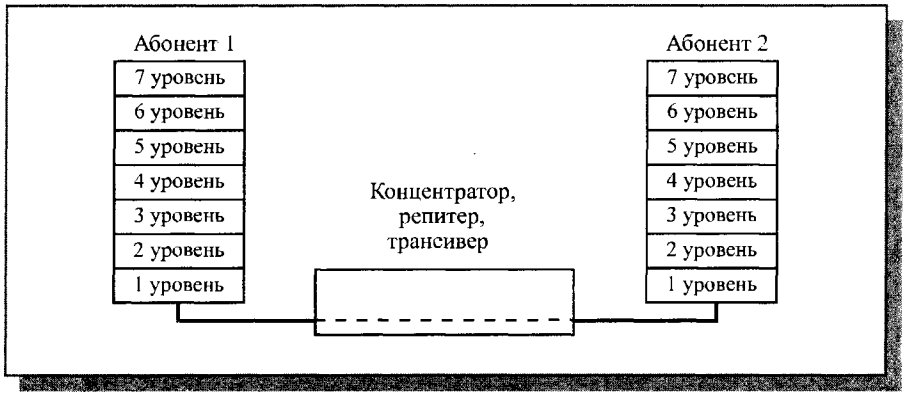



**Рис. 5.9.** Функции концентраторов, репитеров и трансиверов в модели OSI

Выпускаются также совсем простые концентраторы, которые соединяют сегменты сети без восстановления формы сигналов. Они не увеличивают длину сети.

**Коммутаторы** (свичи, коммутирующие концентраторы, switch), как и концентраторы, служат для соединения сегментов в сеть. Они также выполняют более сложные функции, производя сортировку поступающих на них пакетов.

Коммутаторы передают из одного сегмента сети в другой не все поступающие на них пакеты, а только те, которые адресованы компьютерам из другого сегмента. Пакеты, передаваемые между абонентами одного сегмента, через коммутатор не проходят. При этом сам пакет коммутатором не принимается, а только пересылается. Интенсивность обмена в сети снижается вследствие разделения нагрузки, поскольку каждый сегмент работает не только со своими пакетами, но и с пакетами, пришедшими из других сегментов.

Коммутатор работает на втором уровне модели OSI (подуровень MAC), так как анализирует MAC-адреса внутри пакета (рис.5.10). Естественно, он выполняет и функции первого уровня.

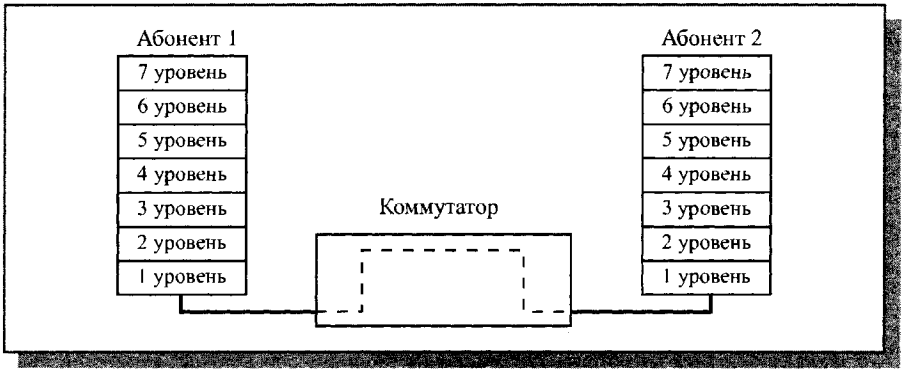



**Рис. 5.10.** Функции коммутаторов в модели OSI

В последнее время объем выпуска коммутаторов сильно вырос, цена на них упала, поэтому коммутаторы постепенно вытесняют концентраторы.

**Мосты** (bridge), **маршрутизаторы** (router) и **шлюзы** (gateway) служат для объединения в одну сеть несколько разнородных сетей с разными протоколами обмена нижнего уровня, в частности, с разными форматами пакетов, методами кодирования, скоростью передачи и т.д. В результате их применения сложная и неоднородная сеть, содержащая в себе различные сегменты, с точки зрения пользователя выглядит самой обычной сетью. Обеспечивается прозрачность сети для протоколов высокого уровня. Все они гораздо дороже, чем концентраторы, так как от

них требуется довольно сложная обработка информации. Реализуются они обычно на базе компьютеров, подключенных к сети с помощью сетевых адаптеров. По сути, они представляют собой специализированные абоненты (узлы) сети.

**Мосты** – наиболее простые устройства, служащие для объединения сетей с разными стандартами обмена, например, Ethernet и Arcnet, или нескольких сегментов (частей) одной и той же сети, например, Ethernet (рис. 5.11). В последнем случае мост, как и коммутатор, только разделяет нагрузку сегментов, повышая тем самым производительность сети в целом. В отличие от коммутаторов мосты принимают поступающие пакеты целиком и в случае необходимости производят их простейшую обработку. Мосты, как и коммутаторы, работают на втором уровне модели OSI (рис. 5.10), но в отличие от них могут захватывать также и верхний подуровень LLC второго уровня (для связи разнородных сетей). В последнее время мосты быстро вытесняются коммутаторами, которые становятся более функциональными.

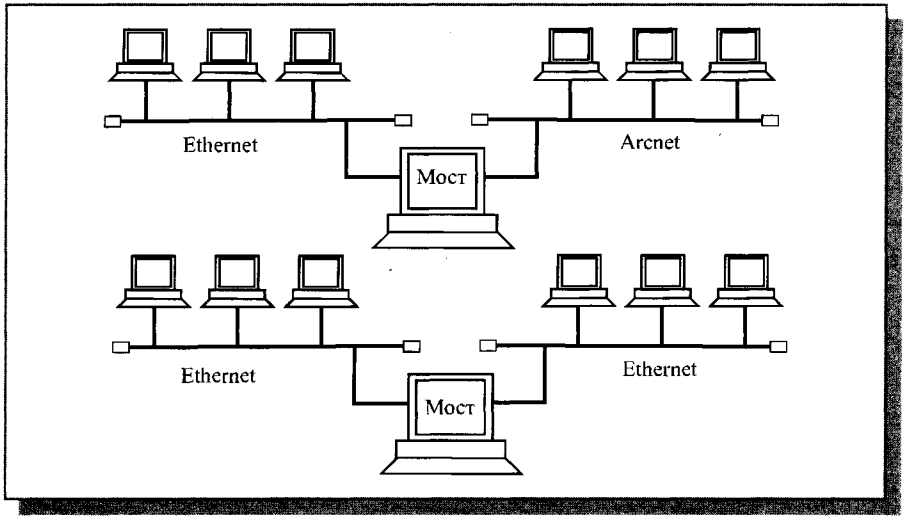



**Рис. 5.11.** Включение моста

**Маршрутизаторы** осуществляют выбор оптимального маршрута для каждого пакета с целью избежания чрезмерной нагрузки отдельных участков сети и обхода поврежденных участков. Они применяются, как правило, в сложных разветвленных сетях, имеющих несколько маршрутов между отдельными абонентами. Маршрутизаторы не преобразуют протоколы нижних уровней, поэтому они соединяют только сегменты одноименных сетей.

Маршрутизаторы работают на третьем уровне модели OSI, так как они анализируют не только MAC-адреса пакета, но и IP-адреса, то есть более глубоко проникают в инкапсулированный пакет (рис. 5.12).

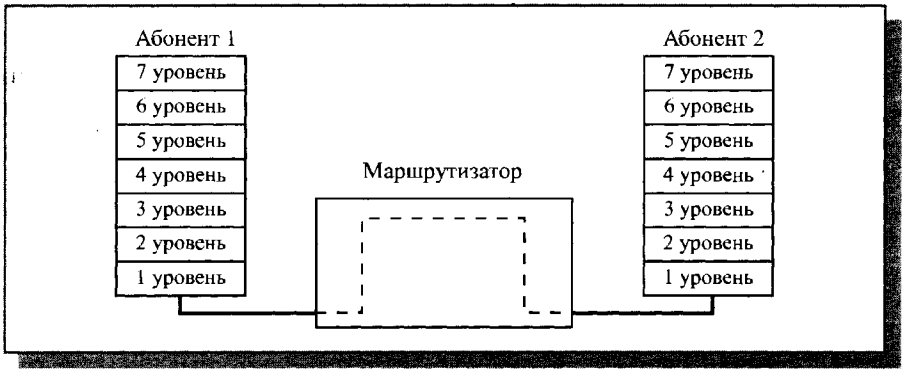



**Рис. 5.12.** Функции маршрутизатора в модели OSI

Существуют также гибридные маршрутизаторы (brouter), представляющие собой гибрид моста и маршрутизатора. Они выделяют пакеты, которым нужна маршрутизация, и обрабатывают их как маршрутизатор, а для остальных пакетов служат обычным мостом.

**Шлюзы** – это устройства для соединения сетей с сильно отличающимися протоколами, например, для соединения локальных сетей с большими компьютерами или с глобальными сетями. Это самые дорогие и редко применяемые сетевые устройства. Шлюзы реализуют связь между абонентами на верхних уровнях модели OSI (с четвертого по седьмой). Соответственно, они должны выполнять и все функции нижестоящих уровней.

Подробнее промежуточные сетевые устройства будут рассмотрены в разделах, посвященных конкретным стандартным локальным сетям.

# Лекция 6. Модель OSI. Верхние уровни

**В этой лекции говорится о функциях модели OSI, реализуемых программно, стандартных протоколах обмена, их достоинствах и недостатках, типах сетевых программных средств и особенностях сетевых программ крупнейших производителей.**

**Ключевые слова:** драйвер, стек протоколов, дейтаграмма, IP и IPX-адреса, одноранговая сеть, сеть на основе сервера, домен, права доступа.

## Стандартные сетевые протоколы

Протоколы – это набор правил и процедур, регулирующих порядок осуществления связи. Компьютеры, участвующие в обмене, должны работать по одним и тем же протоколам, чтобы в результате передачи вся информация восстанавливалась в первоначальном виде.

О протоколах нижних уровней (физического и канального), относящихся к аппаратуре, уже упоминалось в предыдущих разделах. В частности, к ним относятся методы кодирования и декодирования, а также управления обменом в сети. Подробнее некоторые из них будут изложены в главах книги, посвященных стандартным сетям. А сейчас следует остановиться на особенностях протоколов более высоких уровней, реализуемых программно.

Связь сетевого адаптера с сетевым программным обеспечением осуществляют **драйверы** сетевых адаптеров. Именно благодаря драйверу компьютер может не знать никаких аппаратных особенностей адаптера (его адресов, правил обмена с ним, его характеристик). Драйвер унифицирует, делает единообразным взаимодействие программных средств высокого уровня с любым адаптером данного класса. Сетевые драйверы, поставляемые вместе с сетевыми адаптерами, позволяют сетевым программам одинаково работать с платами разных поставщиков и даже с платами разных локальных сетей (Ethernet, Arcnet, Token-Ring и т.д.). Если говорить о стандартной модели OSI, то драйверы, как правило, выполняют функции канального уровня, хотя иногда они реализуют и часть функций сетевого уровня (рис. 6.1). Например, драйверы формируют передаваемый пакет в буферной памяти адаптера, читают из этой памяти пришедший по сети пакет, дают команду на передачу, информируют компьютер о приеме пакета.

Качество написания программы драйвера во многом определяет эффективность работы сети в целом. Даже при самых лучших характеристиках сетевого адаптера некачественный драйвер может резко ухудшить обмен по сети.

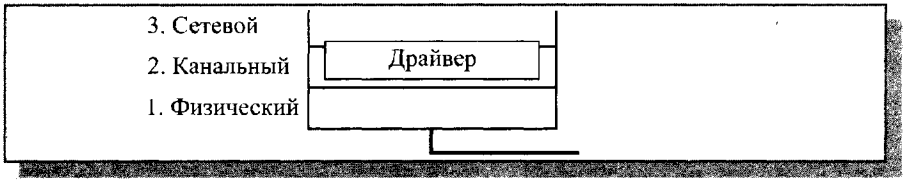



**Рис. 6.1.** Функции драйвера сетевого адаптера в модели OSI

Прежде чем приобрести плату адаптера, необходимо ознакомиться со списком совместимого оборудования (Hardware Compatibility List, HCL), который публикуют все производители сетевых операционных систем. Выбор там довольно велик (например, для Microsoft Windows Server список включает более сотни драйверов сетевых адаптеров). Если в перечень HCL не входит адаптер какого-то типа, лучше его не покупать.

### Протоколы высоких уровней

Существует несколько стандартных наборов (или, как их еще называют, стеков) протоколов, получивших сейчас широкое распространение:

- набор протоколов ISO/OSI;
- IBM System Network Architecture (SNA);
- Digital DECnet;
- Novell NetWare;
- Apple AppleTalk;
- набор протоколов глобальной сети Интернет, TCP/IP.

Включение в этот список протоколов глобальной сети вполне объяснимо, ведь, как уже отмечалось, модель OSI используется для любой открытой системы: на базе как локальной, так и глобальной сети или комбинации локальной и глобальной сетей.

Протоколы перечисленных наборов делятся на три основные типа:

- Прикладные протоколы (выполняющие функции трех верхних уровней модели OSI – прикладного, представительского и сеансового);
- Транспортные протоколы (реализующие функции средних уровней модели OSI – транспортного и сеансового);
- Сетевые протоколы (осуществляющие функции трех нижних уровней модели OSI).

**Прикладные протоколы** обеспечивают взаимодействие приложений и обмен данными между ними. Наиболее популярны:

- FTAM (File Transfer Access and Management) – протокол OSI–доступа к файлам;
- X.400 – протокол CCITT для международного обмена электронной почтой;
- X.500 – протокол CCITT служб файлов и каталогов на нескольких системах;

- SMTP (Simple Mail Transfer Protocol) – протокол глобальной сети Интернет для обмена электронной почтой;
- FTP (File Transfer Protocol) – протокол глобальной сети Интернет для передачи файлов;
- SNMP (Simple Network Management Protocol) – протокол для мониторинга сети, контроля за работой сетевых компонентов и управления ими;
- Telnet – протокол глобальной сети Интернет для регистрации на удаленных серверах и обработки данных на них;
- Microsoft SMBs (Server Message Blocks, блоки сообщений сервера) и клиентские оболочки или редиректоры фирмы Microsoft;
- NCP (Novell NetWare Core Protocol) и клиентские оболочки или редиректоры фирмы Novell.

**Транспортные протоколы** поддерживают сеансы связи между компьютерами и гарантируют надежный обмен данными между ними. Наиболее популярные из них следующие:

- TCP (Transmission Control Protocol) – часть набора протоколов TCP/IP для гарантированной доставки данных, разбитых на последовательность фрагментов;
- SPX – часть набора протоколов IPX/SPX (Internetwork Packet Exchange/Sequential Packet Exchange) для гарантированной доставки данных, разбитых на последовательность фрагментов, предложенных компанией Novell;
- NWLink – реализация протокола IPX/SPX компании Microsoft;
- NetBEUI – (NetBIOS Extended User Interface, расширенный интерфейс NetBIOS) – устанавливает сеансы связи между компьютерами (NetBIOS) и предоставляет верхним уровням транспортные услуги (NetBEUI).

**Сетевые протоколы** управляют адресацией, маршрутизацией, проверкой ошибок и запросами на повторную передачу. Широко распространены следующие из них:

- IP (Internet Protocol) – TCP/IP-протокол для негарантированной передачи пакетов без установления соединений;
- IPX (Internetwork Packet Exchange) – протокол компании NetWare для негарантированной передачи пакетов и маршрутизации пакетов;
- NWLink – реализация протокола IPX/SPX компании Microsoft;
- NetBEUI – транспортный протокол, обеспечивающий услуги транспортировки данных для сеансов и приложений NetBIOS.

Все перечисленные протоколы могут быть поставлены в соответствие тем или иным уровням эталонной модели OSI. Но при этом надо учитывать, что разработчики протоколов не слишком строго придерживаются этих уровней. Например, некоторые протоколы выполняют функции, относящиеся сразу к нескольким уровням модели OSI, а другие – только часть функций одного из уровней. Это приводит к тому, что протоколы разных компаний часто оказы-

ваются несовместимы между собой.Кроме того, протоколы могут быть успешно использованы исключительно в составе своего набора протоколов (стека протоколов), который выполняет более или менее законченную группу функций. Как раз это и делает сетевую операционную систему «фирменной», то есть, по сути, несовместимой со стандартной моделью открытой системы OSI.

В качестве примера на рис. 6.2, 6.3 и 6.4 схематически показано соотношение протоколов, используемых популярными фирменными сетевыми операционными системами, и уровней стандартной модели OSI. Как видно из рисунков, практически ни на одном уровне нет четкого соответствия реального протокола какому-нибудь уровню идеальной модели. Выстраивание подобных соотношений довольно условно, так как трудно четко разграничить функции всех частей программного обеспечения. К тому же компании-производители программных средств далеко не всегда подробно описывают внутреннюю структуру продуктов.

Теперь следует подробнее рассмотреть некоторые наиболее распространенные протоколы.

Модель OSI допускает два основных метода взаимодействия абонентов в сети:

- Метод взаимодействия без логического соединения (или метод дейтаграмм).
- Метод взаимодействия с логическим соединением.

**Метод дейтаграмм** – это простейший метод, в котором каждый пакет рассматривается как самостоятельный объект (рис. 6.5).

Пакет при этом методе передается без установления логического канала, то есть без предварительного обмена служебными пакетами для выяснения готовности приемника, а также без ликвидации логического канала, то есть без пакета подтверждения окончания передачи. Дойдет пакет до приемника или нет – неизвестно (проверка факта получения переносится на более высокие уровни).

Метод дейтаграмм предъявляет повышенные требования к аппаратуре (так как приемник всегда должен быть готов к приему пакета). Достоинства метода в том, что передатчик и приемник работают независимо друг от друга, к тому же пакеты могут накапливаться в буфере и затем передаваться вместе. Можно также использовать широковещательную передачу, то есть адресовать пакет всем абонентам одновременно. Недостатки метода – это возможность потери пакетов, а также бесполезной загрузки сети пакетами в случае отсутствия или неготовности приемника.

**Метод с логическим соединением** (рис. 6.6, рис. 4.5) разработан позднее, чем метод дейтаграмм, и отличается усложненным порядком взаимодействия.

При этом методе пакет передается только после того, как будет установлено логическое соединение (канал) между приемником и передатчиком. Каждому информационному пакету сопутствует один или несколько

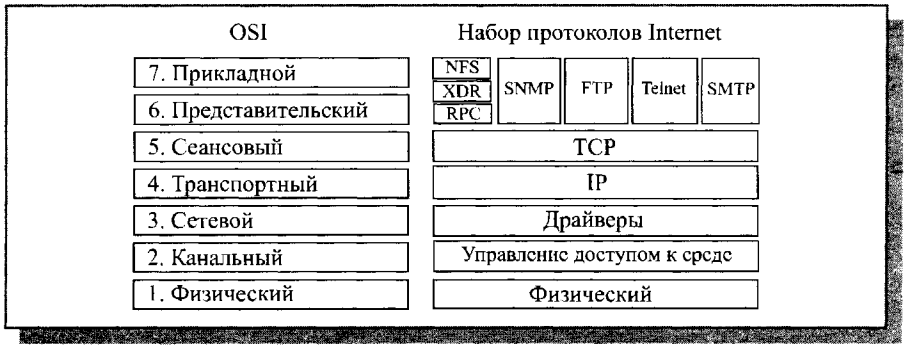



**Рис. 6.2.** Соотношение уровней модели OSI и протоколов сети Интернет

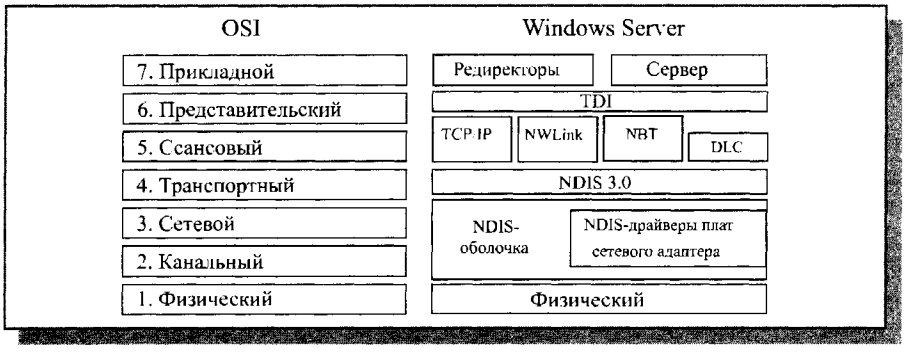



**Рис. 6.3.** Соотношение уровней модели OSI и протоколов операционной системы Windows Server

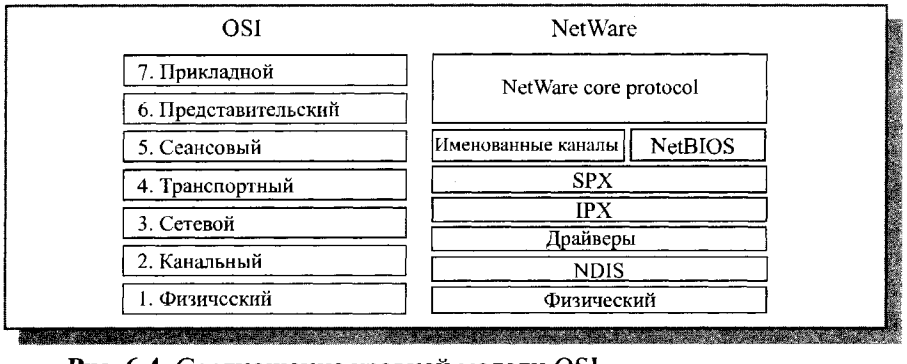



**Рис. 6.4.** Соотношение уровней модели OSI и протоколов операционной системы NetWare

служебных пакетов (установка соединения, подтверждение получения, запрос повторной передачи, разрыв соединения). Логический канал мо-

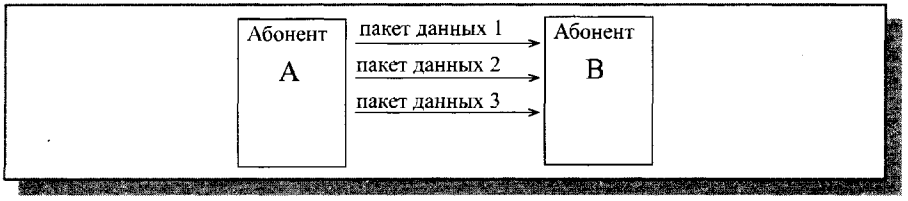



**Рис. 6.5.** Метод дейтаграмм

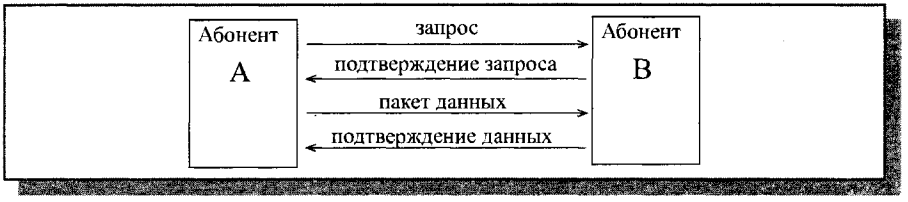



**Рис. 6.6.** Метод с логическим соединением

жет устанавливаться на время передачи одного или нескольких пакетов.

Метод с логическим соединением, как уже говорилось, более сложен, чем метод дейтаграмм, но гораздо надежнее, поскольку к моменту ликвидации логического канала передатчик уверен, что все его пакеты дошли до места назначения, причем дошли успешно. Не бывает при данном методе и перегрузки сети из-за бесполезных пакетов. Недостаток метода с логическим соединением состоит в том, что довольно сложно разрешить ситуацию, когда принимающий абонент по тем или иным причинам не готов к обмену, например, из-за обрыва кабеля, отключения питания, неисправности сетевого оборудования, сбоя в компьютере. При этом требуются алгоритм обмена с повторением неподтвержденного пакета заданное количество раз, причем важен и тип неподтвержденного пакета. Этот метод не может передавать широковещательные пакеты (то есть адресованные всем абонентам), так как нельзя организовать логические каналы сразу со всеми абонентами.

Примеры протоколов, работающих по методу дейтаграмм — это протоколы IP и IPX.

Примеры протоколов, работающих по методу с логическим соединением – это TCP и SPX.

Именно для того, чтобы объединить достоинства обоих методов, эти протоколы используются в виде связанных наборов: TCP/IP и IPX/SPX, в которых протокол более высокого уровня (TCP, SPX), работающий на базе протокола более низкого уровня (IP, IPX), гарантирует правильную доставку пакетов в требуемом порядке.

Протоколы **IPX/SPX**, разработанные компанией Novell, образуют набор (стек), используемый в сетевых программных средствах довольно широко распространенных локальных сетей Novell (NetWare). Это сравнительно небольшой и быстрый протокол, поддерживающий маршрутизацию.

Прикладные программы могут обращаться непосредственно к уровню IPX, например, для посылки широковещательных сообщений, но значительно чаще работают с уровнем SPX, гарантирующим быструю и надежную доставку пакетов. Если скорость не слишком важна, то прикладные программы применяют еще более высокий уровень, например, протокол NetBIOS, предоставляющий удобный сервис. Компанией Microsoft предложена своя реализация протокола IPX/SPX, называемая **NWLink**. Протоколы IPX/SPX и NWLink поддерживаются операционными системами NetWare и Windows. Выбор этих протоколов обеспечивает совместимость по сети любых абонентов с данными операционными системами.

Набор (стек) протоколов **TCP/IP** был специально разработан для глобальных сетей и для межсетевого взаимодействия. Он изначально ориентирован на низкое качество каналов связи, на большую вероятность ошибок и разрывов связей. Этот протокол принят во всемирной компьютерной сети Интернет, значительная часть абонентов которой подключается по коммутируемым линиям (то есть обычным телефонным линиям). Как и протокол IPX/SPX, протокол TCP/IP также поддерживает маршрутизацию. На его основе работают протоколы высоких уровней, такие как SMTP, FTP, SNMP. Недостаток протокола TCP/IP — более низкая скорость работы, чем у IPX/SPX. Однако сейчас протокол TCP/IP используется и в локальных сетях, чтобы упростить согласование протоколов локальных и глобальных сетей. В настоящее время он считается основным в самых распространенных операционных системах.

В стек протоколов TCP/IP часто включают и протоколы всех верхних уровней (рис. 6.7). И тогда уже можно говорить о функциональной полноте стека TCP/IP.

Как протокол IPX, так и протокол IP являются самыми низкоуровневыми протоколами, поэтому они непосредственно инкапсулируют свою информацию, называемую дейтаграммой, в поле данных передаваемого по сети пакета (см. рис. 4.6). При этом в заголовок дейтаграммы входят адреса

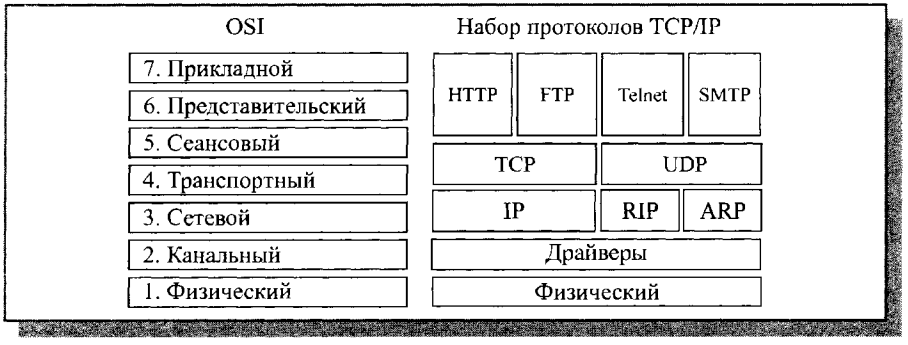



**Рис. 6.7.** Соотношение уровней модели OSI и стека протоколов TCP/IP

абонентов (отправителя и получателя) более высокого уровня, чем MAC-адреса, – это IPX-адреса для протокола IPX или IP-адреса для протокола IP. Эти адреса включают номера сети и узла, хоста (индивидуальный идентификатор абонента). При этом IPX-адреса (рис. 6.8) более простые, и они имеют всего один формат, а в IP-адрес (рис. 6.9) могут входить три формата (класса A, B и C), различающиеся значениями трех начальных битов.

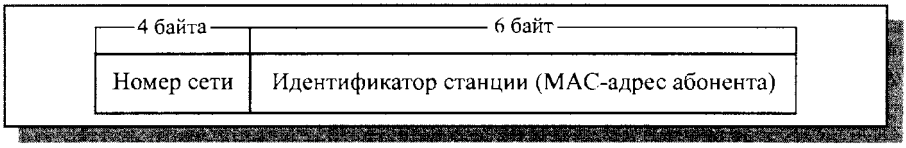



**Рис. 6.8.** Формат IPX- адреса

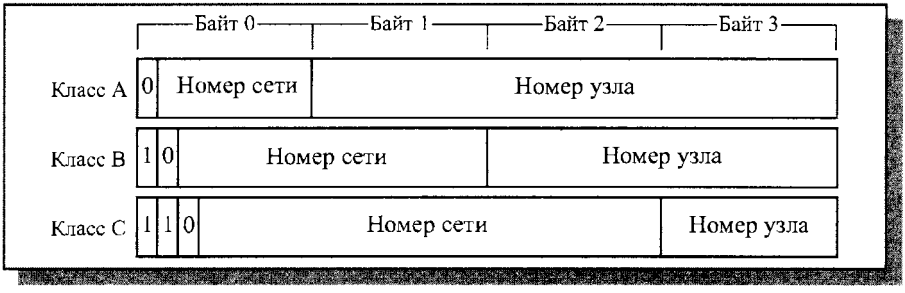



**Рис. 6.9.** Форматы IP-адреса

Интересно, что IP-адрес не имеет никакой связи с MAC-адресами абонентов. Номер узла в нем присваивается абоненту независимо от его MAC-адреса. В качестве идентификатора станции IPX-адрес включает в себя полный MAC-адрес абонента.

Номер сети – это код, присвоенный каждой конкретной сети, то есть каждой *широковещательной области* общей, единой сети. Под широковещательной областью понимается часть сети, которая прозрачна для широковещательных пакетов, и пропускает их беспрепятственно.

Протокол **NetBIOS** (сетевая базовая система ввода/вывода) был разработан компанией IBM для сетей IBM PC Network и IBM Token-Ring по образцу системы BIOS персонального компьютера. С тех пор этот протокол стал фактическим стандартом (официально он не стандартизован), и многие сетевые операционные системы содержат в себе эмулятор NetBIOS для обеспечения совместимости. Первоначально NetBIOS реализовывал сеансовый, транспортный и сетевой уровни, однако в последующих сетях на более низких уровнях используются стандартные протоколы (например, IPX/SPX), а на долю эмулятора NetBIOS остается только сеансовый уровень. NetBIOS обеспечивает более высокий уровень сервиса, чем IPX/SPX, но работает медленнее.

На основе протокола NetBIOS был разработан протокол NetBEUI, кото-

рый представляет собой развитие протокола NetBIOS до транспортного уровня. Однако недостаток NetBEUI состоит в том, что он не поддерживает межсетевое взаимодействие и не обеспечивает маршрутизацию. Поэтому данный протокол используется только в простых сетях, не рассчитанных на подключение к Интернет. Сложные сети ориентируются на более универсальные протоколы TCP/IP и IPX/SPX. Протокол NetBEUI в настоящее время считается устаревшим, хотя даже в операционной системе Windows XP предусмотрена его поддержка, правда, только как дополнительная опция.

Наконец, упоминавшийся уже набор протоколов OSI – это полный набор (стек) протоколов, где каждый протокол точно соответствует определенному уровню стандартной модели OSI. Набор содержит маршрутизируемые и транспортные протоколы, серии протоколов IEEE 802, протокол сеансового уровня, представительского уровня и несколько протоколов прикладного уровня. Пока широкого распространения этот набор протоколов не получил, хотя он и полностью соответствует эталонной модели OSI.

## Стандартные сетевые программные средства

Функции верхних уровней эталонной модели OSI выполняют сетевые программные средства. Для установки сети достаточно иметь набор сетевого оборудования, его драйверы, а также сетевое программное обеспечение. От выбора программного обеспечения зависит очень многое: допустимый размер сети, удобство использования и контроля сети, режимы доступа к ресурсам, производительность сети в разных режимах и т.д. Правда, заменить одну программную систему на другую значительно проще, чем сменить оборудование.

С точки зрения распределения функций между компьютерами сети, все сети можно разделить на две группы:

- *Одноранговые сети*, состоящие из равноправных (с точки зрения доступа к сети) компьютеров.
- *Сети на основе серверов*, в которых существуют только выделенные (dedicated) серверы, занимающиеся исключительно сетевыми функциями. Выделенный сервер может быть единственным или же их может быть несколько.

Согласно с этим, выделяют и типы программных средств, реализующих данные виды сетей.

### Одноранговые сети

Одноранговые сети (Peer-to-Peer Network) и соответствующие программные средства, как правило, используются для объединения небольшого количества компьютеров (рис. 6.10). Каждый компьютер такой сети может одновременно являться и сервером и клиентом сети, хотя вполне

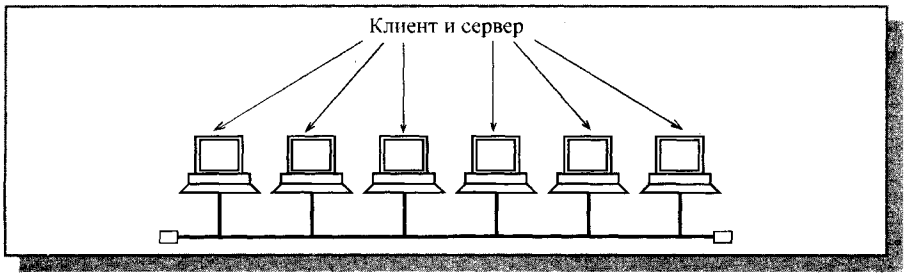



**Рис. 6.10.** Одноранговая сеть

допустимо назначение одного компьютера только сервером, а другого — только клиентом. Принципиальна возможность совмещения функций клиента и сервера. Важно также и то, что в одноранговой сети любой сервер может быть невыделенным (non-dedicated), он может не только обслуживать сеть, но и работать как автономный компьютер (правда, запросы к нему по сети сильно снижают скорость его работы). В одноранговой сети могут быть и выделенные серверы, только обслуживающие сеть.

Именно в данном случае наиболее правильно говорить о распределенных дисковых ресурсах, о виртуальном компьютере, а также о суммировании объемов дисков всех компьютеров сети. Если все компьютеры являются серверами, то любой файл, созданный на одном из них, сразу же становится доступным всем остальным компьютерам, его не надо передавать на централизованный сервер.

Достоинством одноранговых сетей является их высокая гибкость: в зависимости от конкретной задачи сеть может использоваться очень активно либо совсем не использоваться. Из-за большой самостоятельности компьютеров в таких сетях редко бывает ситуация перегрузки (к тому же количество компьютеров обычно невелико). Установка одноранговых сетей довольно проста, к тому же не требуются дополнительные дорогостоящие серверы. Кроме того, нет необходимости в системном администрировании, пользователи могут сами управлять своими ресурсами.

В одноранговых сетях допускается определение различных прав пользователей по доступу к сетевым ресурсам, но система разграничения прав не слишком развита. Если каждый ресурс защищен своим паролем, то пользователю приходится запоминать большое число паролей.

К недостаткам одноранговых сетей относятся также слабая система контроля и протоколирования работы сети, трудности с резервным копированием распределенной информации. К тому же выход из строя любого компьютера-сервера приводит к потере части общей информации, то есть все такие компьютеры должны быть по возможности высоконадежными. Эффективная скорость передачи информации по одноранговой сети часто оказывается недостаточной, поскольку трудно обеспечить быстродей-

ствие процессоров, большой объем оперативной памяти и высокие скорости обмена с жестким диском для всех компьютеров сети. К тому же компьютеры сети работают не только на сеть, но решают и другие задачи.

Несколько примеров одноранговых сетевых программных средств:

- NetWare Lite компании Novell (сейчас уже не производится);
- LANtastic компании Artisoft (выпуск практически прекращен);
- Windows for Workgroups компании Microsoft (первая версия ОС Windows со встроенной поддержкой сети, выпущенная в 1992 году);
- Windows NT Workstation компании Microsoft;
- Windows 95... Windows XP компании Microsoft.

Первые одноранговые сетевые программные средства представляли собой сетевые оболочки, работающие под управлением DOS (например, NetWare Lite). Они перехватывали все запросы DOS — те запросы, которые вызваны обращениями к сетевым устройствам, обрабатывались и выполнялись сетевой оболочкой, а те, которые вызваны обращениями к «местным», несетевым ресурсам, возвращались обратно в DOS и обрабатывались стандартным образом.

Более поздние одноранговые сетевые программные средства уже были встроены в операционную систему Windows. Это гораздо удобнее, так как исключается этап установки сетевых программ. Поэтому сетевые оболочки сейчас уже практически не используются, хотя многие их характеристики были заметно лучше, чем у сетевых средств Windows.

Сейчас считается, что одноранговая сеть наиболее эффективна в небольших сетях (около 10 компьютеров). При значительном количестве компьютеров сетевые операции сильно замедлят работу компьютеров и создадут множество других проблем. Тем не менее, для небольшого офиса одноранговая сеть – оптимальное решение.

Самая распространенная в настоящий момент одноранговая сеть – это сеть на основе **Windows XP** (или более ранних версий ОС Windows).

При этом пользователь, приобретая компьютер с установленной операционной системой, автоматически получает и возможность выхода в сеть. Естественно, это во многих случаях гораздо удобнее, чем приобретать и устанавливать пусть даже и более совершенные продукты других фирм. К тому же пользователю не надо изучать интерфейс пользователя сетевой программы, так как он строится так же, как и интерфейс пользователя всех остальных частей операционной системы.

Если приобретаемый компьютер еще и имеет установленный сетевой адаптер, то построить сеть пользователю совсем просто. Надо только соединить компьютеры кабелем и настроить сетевые программы.

В Windows предусмотрена поддержка совместного использования дисков (в том числе гибких дисков и CD), а также принтеров. Имеется возможность объединения всех пользователей в рабочие группы для бо-

лее удобного поиска требуемых ресурсов и организации доступа к ним. Пользователи имеют доступ ко встроенной системе электронной почты. Это означает, что все пользователи сети получают возможность совместно применять многие ресурсы ОС своего компьютера.

При настройке сети пользователь должен выбрать тип сетевого протокола. По умолчанию используется протокол TCP/IP, но возможно применение IPX/SPX (NWLink), а также NetBEUI. При выборе TCP/IP можно задавать адреса IP вручную или с помощью автоматической настройки адресации (в этом случае компьютер сам присвоит себе адрес из диапазона, не используемого в Интернете).

Кроме того, надо задать индивидуальное имя компьютера и определить рабочую группу, к которой он относится.

После этого можно разрешить доступ по сети к ресурсам каждого компьютера сети, к его файлам, папкам, принтерам, сканерам, доступу в Интернет.

### Сети на основе сервера

Сети на основе сервера (Server-based Network) применяются в тех случаях, когда в сеть должно быть объединено много пользователей. В этом случае возможностей одноранговой сети может не хватить. Поэтому в сеть включается специализированный компьютер – сервер, который обслуживает только сеть и не решает никаких других задач (рис. 6.11). Такой сервер называется выделенным. Сервер может быть и специализирован на решении одной задачи, например, сервер печати, но чаще всего серверами выступают именно компьютеры. В сети может быть и несколько серверов, каждый из которых решает свою задачу.

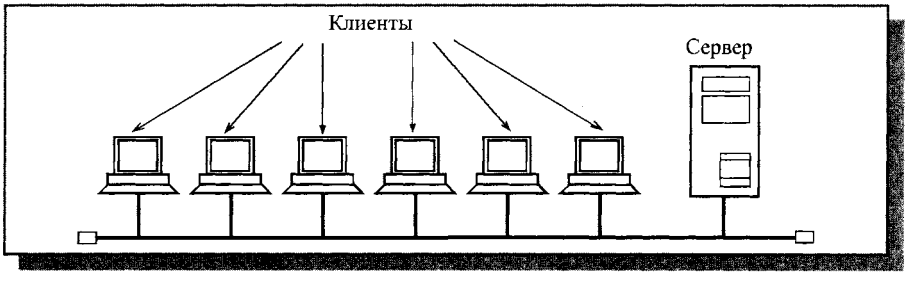



**Рис. 6.11.** Сеть на основе сервера

Серверы специально оптимизированы для быстрой обработки сетевых запросов на разделяемые ресурсы и для управления защитой файлов и каталогов. При больших размерах сети мощности одного сервера может оказаться недостаточно, и тогда в сеть включают несколько серверов. Серверы могут выполнять и некоторые другие задачи: сетевая печать, вы-

ход в глобальную сеть, связь с другой локальной сетью, обслуживание электронной почты и т.д. Количество пользователей сети на основе сервера может достигать нескольких тысяч. Одноранговой сетью такого размера просто невозможно было бы управлять. Кроме того, в сети на основе серверов можно легко менять количество подключаемых компьютеров. Такие сети называются *масштабируемыми*.

В любом случае в сети на основе сервера существует четкое разделение компьютеров на клиентов (или рабочие станции) и серверы. Клиенты не могут работать как серверы, а серверы – как клиенты и как автономные компьютеры. Очевидно, что все сетевые дисковые ресурсы могут располагаться только на сервере, а клиенты могут обращаться только к серверу, но не друг к другу. Однако это не значит, что они не могут общаться между собой, просто пересылка информации от одного клиента к другому возможна только через сервер, например, через файл, доступный всем клиентам. В данном случае реализуется некоторая «логическая звезда» с сервером в центре, хотя физическая топология сети может быть любой.

Достоинством сети на основе сервера часто называют надежность. Это верно, но только с одной оговоркой: если сам сервер действительно очень надежен. В противном случае любой отказ сервера приводит к полному параличу сети в отличие от ситуации с одноранговой сетью, где отказ одного из компьютеров не приводит к отказу всей сети. Бесспорное достоинство сети на основе сервера – высокая скорость обмена, так как сервер всегда оснащается быстрым процессором (или даже несколькими процессорами), оперативной памятью большого объема и быстрыми жесткими дисками. Так как все ресурсы сети собраны в одном месте, возможно применение гораздо более мощных средств управления доступом, защиты данных, протоколирования обмена, чем в одноранговых сетях.

К недостаткам сети на основе сервера относятся ее громоздкость в случае небольшого количества компьютеров, зависимость всех компьютеров-клиентов от сервера, более высокая стоимость сети вследствие использования дорогого сервера. Но, говоря о стоимости, надо также учитывать, что при одном и том же объеме сетевых дисков большой диск сервера получается дешевле, чем много дисков меньшего объема, входящих в состав всех компьютеров одноранговой сети.

Примеры некоторых сетевых программных средств на основе сервера:

- NetWare компании Novell (самая распространенная сетевая ОС);
- LAN Server компании IBM (почти не используется);
- LAN Manager компании Microsoft;
- Windows NT Server компании Microsoft;
- Windows Server 2003 компании Microsoft.

На файл-сервере в данном случае устанавливается специальная сетевая операционная система, рассчитанная на работу сервера. Эта сетевая ОС опти-

мизирована для эффективного выполнения специфических операций по организации сетевого обмена. На рабочих станциях (клиентах) может устанавливаться любая совместимая операционная система, поддерживающая сеть.

Для обеспечения надежной работы сети при авариях электропитания применяется бесперебойное электропитание сервера. В данном случае это гораздо проще, чем при одноранговой сети, где желательно оснащать источниками бесперебойного питания все компьютеры сети.

Для администрирования сети (то есть управления распределением ресурсов, контроля прав доступа, защиты данных, файловой системы, резервирования файлов и т.д.) в случае сети на основе сервера необходимо выделять специального человека, имеющего соответствующую квалификацию. Централизованное администрирование облегчает обслуживание сети и позволяет оперативно решать все вопросы. Особенно это важно для надежной защиты данных от несанкционированного доступа. В случае же одноранговой сети можно обойтись и без специалиста-администратора, правда, при этом все пользователи сети должны иметь хоть какое-то представление об администрировании.

Процесс установки серверной сетевой операционной системы гораздо сложнее, чем в случае одноранговой сети. Так, он включает в себя следующие обязательные процедуры:

- форматирование и разбиение на разделы жесткого диска компьютера-сервера;
- присвоение индивидуального имени серверу;
- присвоение имени сети;
- установка и настройка сетевого протокола;
- выбор сетевых служб;
- ввод пароля администратора.

Сетевая операционная система на базе сервера **Windows Server 2003** предоставляет пользователям гораздо больше возможностей, чем в случае одноранговой сети.

Она позволяет строить сложные иерархические структуры сети на основе логических групп компьютеров (*доменов*, domain), наборов доменов (*деревьев*, tree) и наборов деревьев (*леса*, forest).

Домен представляет собой группу компьютеров, управляемых специальным сервером — *контроллером домена*. Домен использует собственную базу данных, содержащую учетные записи пользователей, и управляет собственными ресурсами, такими как принтеры и общие файлы. Каждому домену присваивается свое имя (обычно домен рассматривается как отдельная сеть со своим номером). В каждый домен может входить несколько рабочих групп, которые формируются из пользователей, решающих общую или сходные задачи. В принципе домен может включать тысячи пользователей, однако обычно домены не слишком велики, и несколь-

ко доменов объединяются в дерево доменов. Это упрощает управление сетью. Точно так же несколько деревьев может объединяться в лес, самую крупную административную структуру, поддерживаемую данной ОС.

В процессе установки Windows Server 2003 необходимо задать тип протокола сети. По умолчанию используется TCP/IP, но возможно применение NWLink (IPX/SPX).

Каждому серверу необходимо назначить роль, которую он будет выполнять в сети:

- контроллер домена (управляет работой домена);
- файловый сервер (хранит совместно используемые файлы);
- сервер печати (управляет сетевым принтером);
- Web-сервер (содержит сайт, доступный по сети Интернет или по локальной сети);
- коммуникационный сервер (обеспечивает работу электронной почты и конференций);
- сервер удаленного доступа (обеспечивает удаленный доступ).

Каждому пользователю сети необходимо присвоить свое учетное имя и пароль, а также права доступа к ресурсам (полномочия). Права доступа могут задаваться как индивидуально, так и целой рабочей группе пользователей. Windows Server 2003 обеспечивает следующие виды полномочий для папок:

- полный контроль (просмотр, чтение, запись, удаление папки, подпапок, файлов, запуск на исполнение, установка прав доступа к папке);
- изменение (просмотр, чтение, запись, удаление подпапок и файлов, запуск на исполнение);
- чтение и исполнение (просмотр, чтение, запуск на исполнение);
- просмотр содержимого папки;
- запись нового содержимого в папку;
- чтение информации из папки.

Те же самые уровни полномочий (кроме просмотра содержимого) предусмотрены и для файлов, доступных по сети.

Сетевые операционные системы **NetWare** компании Novell сегодня очень популярны, что объясняется их высокой производительностью, совместимостью с разными аппаратными средствами и развитой системой средств защиты данных. Компания Novell выпускает сетевые программные средства с 1979 года: несколько версий сетевых ОС на базе файловых серверов (одна из последних версий – NetWare 6 и 6.5), клиентское программное обеспечение, а также средства диагностики работы сетей. Популярные до недавнего времени сетевые оболочки одноранговых сетей, такие как NetWare Lite и Personal NetWare сейчас уже не производятся.

Отличительной особенностью сетевых программных средств Novell всегда была их открытость, то есть совместимость с операционными системами различных фирм: Windows, UNIX, Macintosh, OS/2. Кроме того, они

всегда обеспечивали возможность работы с аппаратными средствами практически всех известных производителей. Это позволяет строить на их основе сети из разнообразных абонентов – от самых простых до самых сложных.

Все сетевые продукты NetWare допускают подключение бездисковых рабочих станций (клиентов), что позволяет при необходимости значительно снизить стоимость сети. Во всех продуктах предусмотрена поддержка сетевых мостов.

Продуктам Novell NetWare присущи и недостатки, например, их стоимость для небольших сетей оказывается достаточно высокой по сравнению с ценой продуктов других производителей. Кроме того, их установка сравнительно сложна, но они уже стали фактическим стандартом, поэтому их позиции на рынке довольно прочны.

Рассмотрим кратко особенности сетевой ОС **Novell NetWare 6.5**.

Как и в случае Microsoft Windows Server 2003, Novell NetWare 6.5 требует создания древовидной иерархической структуры, включающей в себя сетевые деревья, серверы, пользователей, группы и прочие объекты.

Novell NetWare 6.5 предусматривает обязательное разбиение жестких дисков с использованием собственной системы хранения файлов NSS (Novell Storage Services), которое требует создания логических разделов (Volumes) на диске. Это позволяет серверу более эффективно решать сетевые задачи.

Для каждого сервера сети надо выбрать один из трех типов:

- Настраиваемый сервер (в частности, Web-сервер, FTP-сервер).
- Основной файловый сервер.
- Специальный сервер (например, DNS/DHCP-сервер, контролирующий сетевые адреса и имена, или сервер резервного копирования).

Кроме того, надо задать тип используемого протокола – TCP/IP или IPX/SPX.

На компьютеры-клиенты следует установить клиентское программное обеспечение. Это сравнительно простая процедура.

Каждому клиенту присваивается учетная запись, предоставляются свои права доступа к ресурсам. Клиенты могут быть объединены в рабочие группы, каждой из которых присваиваются имена и права доступа.

Предусмотрены следующие виды доступа к файлам и каталогам (папкам):

- Изменение прав доступа к каталогу или файлу;
- Просмотр каталога;
- Создание каталогов и файлов в данном каталоге;
- Удаление каталогов и файлов в данном каталоге;
- Изменение содержимого файлов;
- Любые операции над файлами каталога;
- Запись в файл.

# Глава 5. Стандартные локальные сети

## Лекция 7. Старейшие стандартные сети

**В этой лекции говорится о стандартных локальных сетях, получивших большое распространение в конце XX века: Ethernet, Token Ring, Arcnet, их особенностях, достоинствах и недостатках, месте на рынке и перспективах.**

**Ключевые слова:** Ethernet, Fast Ethernet, Token-Ring, Arcnet, форматы пакетов, методы управления, среды передачи.

За время, прошедшее с момента появления первых локальных сетей, было разработано несколько сот самых разных сетевых технологий, однако заметное распространение получили немногие. Это связано, прежде всего, с высоким уровнем стандартизации принципов организации сетей и с поддержкой их известными компаниями. Тем не менее, не всегда стандартные сети обладают рекордными характеристиками, обеспечивают наиболее оптимальные режимы обмена. Но большие объемы выпуска их аппаратуры и, следовательно, ее невысокая стоимость дают им огромные преимущества. Немаловажно и то, что производители программных средств также в первую очередь ориентируются на самые распространенные сети. Поэтому пользователь, выбирающий стандартные сети, имеет полную гарантию совместимости аппаратуры и программ.

В настоящее время уменьшение количества типов используемых сетей стало тенденцией. Дело в том, что увеличение скорости передачи в локальных сетях до 100 и даже до 1000 Мбит/с требует применения самых передовых технологий, проведения дорогих научных исследований. Естественно, это могут позволить себе только крупнейшие фирмы, которые поддерживают свои стандартные сети и их более совершенные разновидности. К тому же большинство потребителей уже установило у себя какие-то сети и не желает сразу и полностью заменять сетевое оборудование. В ближайшем будущем вряд ли стоит ожидать того, что будут приняты принципиально новые стандарты.

На рынке предлагаются стандартные локальные сети всех возможных топологий, так что выбор у пользователей имеется. Стандартные сети обеспечивают широкий диапазон допустимых размеров сети, количества абонентов и, что не менее важно, цен на аппаратуру. Но сделать выбор все равно непросто. Ведь в отличие от программных средств, заменить которые нетрудно, аппаратура обычно служит многие годы, ее замена ведет не только к значительным затратам, к необходимости перекладки кабелей,

но и к пересмотру системы компьютерных средств организации. В связи с этим ошибки в выборе аппаратуры обычно обходятся гораздо дороже ошибок при выборе программных средств.

В данной главе будут рассмотрены основные особенности аппаратуры наиболее популярных локальных сетей, что несомненно поможет читателю при необходимости сделать правильный выбор.

В табл. 7.1 приведены характеристики классических вариантов стандартных локальных сетей. Все стандартные сети имеют несколько вариантов, отличающихся типом используемого кабеля, скоростями передачи, допустимыми размерами сети. О них подробнее рассказано в разделах, посвященных конкретным типам сетей.

**Таблица 7.1.** Параметры базовых вариантов стандартных сетей

| Параметр сети | Ethernet | Token-Ring | Arcnet | FDDI | 100VG-AnyLAN |
|---|---|---|---|---|---|
| Стандарт | IEEE 802.3 | IEEE 802.5 | Datapoint | ISO 9314 | IEEE 802.12 |
| Топология | Шина | Кольцо | Шина | Кольцо | Звезда |
| Скорость передачи | 10 (100) Мбит/с4 | (16) Мбит/с | 2,5 Мбит/с | 100 Мбит/с | 100 Мбит/с |
| Длина | 5 км | 120 м | 6 км | 20 км | 1 км |
| Среда | КК | ВП | КК | ОВ | ВП |
| Метод управления | CSMA/CD | Маркер | Маркер | Маркер | Центр |
| Код | Манчестер | Бифазный | Arcnet | 4B/5B | 5B/6B |
| Количество абонентов | До 1024 | До 260 | До 255 | До 1000 | До 1024 |

КК— коаксиальный кабель, ВП – кабель на витых парах,
ОВ – оптоволоконный кабель

## Сети Ethernet и Fast Ethernet

Наибольшее распространение среди стандартных сетей получила сеть Ethernet. Впервые она появилась в 1972 году (разработчиком выступила известная фирма Xerox). Сеть оказалась довольно удачной, и вследствие этого ее в 1980 году поддержали такие крупнейшие компании, как DEC и Intel (объединение этих компаний назвали DIX по первым буквам их названий). Их стараниями в 1985 году сеть Ethernet стала международным стандартом, ее приняли крупнейшие международные организации

по стандартам: комитет 802 IEEE (Institute of Electrical and Electronic Engineers) и ECMA (European Computer Manufacturers Association).

Стандарт получил название IEEE 802.3 (по-английски читается как «eight or two dot three»). Он определяет множественный доступ к моноканалу типа «шина» с обнаружением конфликтов и контролем передачи, то есть с уже упоминавшимся методом доступа CSMA/CD. Этому стандарту удовлетворяли и некоторые другие сети, так как уровень его детализации невысок. В результате сети стандарта IEEE 802.3 нередко были несовместимы между собой как по конструктивным, так и по электрическим характеристикам. Однако в последнее время стандарт IEEE 802.3 считается стандартом именно сети Ethernet.

Основные характеристики первоначального стандарта IEEE 802.3:

- топология – шина;
- среда передачи – коаксиальный кабель;
- скорость передачи – 10 Мбит/с;
- максимальная длина сети – 5 км;
- максимальное количество абонентов – до 1024;
- длина сегмента сети – до 500 м;
- количество абонентов на одном сегменте – до 100;
- метод доступа – CSMA/CD;
- передача узкополосная, то есть без модуляции (моноканал).

Строго говоря, между стандартами IEEE 802.3 и Ethernet существуют незначительные отличия, но о них обычно предпочитают не вспоминать.

Сеть Ethernet сейчас наиболее популярна в мире (более 90% рынка), предположительно таковой она и останется в ближайшие годы. Этому в немалой степени способствовало то, что с самого начала характеристики, параметры и протоколы сети были открыты, в результате чего огромное число производителей во всем мире стали выпускать аппаратуру Ethernet, полностью совместимую между собой.

В классической сети Ethernet применялся 50-омный коаксиальный кабель двух видов (толстый и тонкий). Однако в последнее время (с начала 1990-х годов) наибольшее распространение получила версия Ethernet, использующая в качестве среды передачи витые пары. Определен также стандарт для применения в сети оптоволоконного кабеля. Для учета этих изменений в изначальный стандарт IEEE 802.3 были сделаны соответствующие добавления. В 1995 году появился дополнительный стандарт на более быструю версию Ethernet, работающую на скорости 100 Мбит/с (так называемый Fast Ethernet, стандарт IEEE 802.3u) и использующую в качестве среды передачи витую пару или оптоволоконный кабель. В 1997 году появилась и версия на скорость 1000 Мбит/с (Gigabit Ethernet, стандарт IEEE 802.3z).

Помимо стандартной топологии «шина» все шире применяются топологии типа пассивная «звезда» и пассивное «дерево». При этом предполага-

ется использование репитеров и репитерных концентраторов, соединяющих между собой различные части (сегменты) сети. В результате может сформироваться древовидная структура на сегментах разных типов (рис. 7.1).

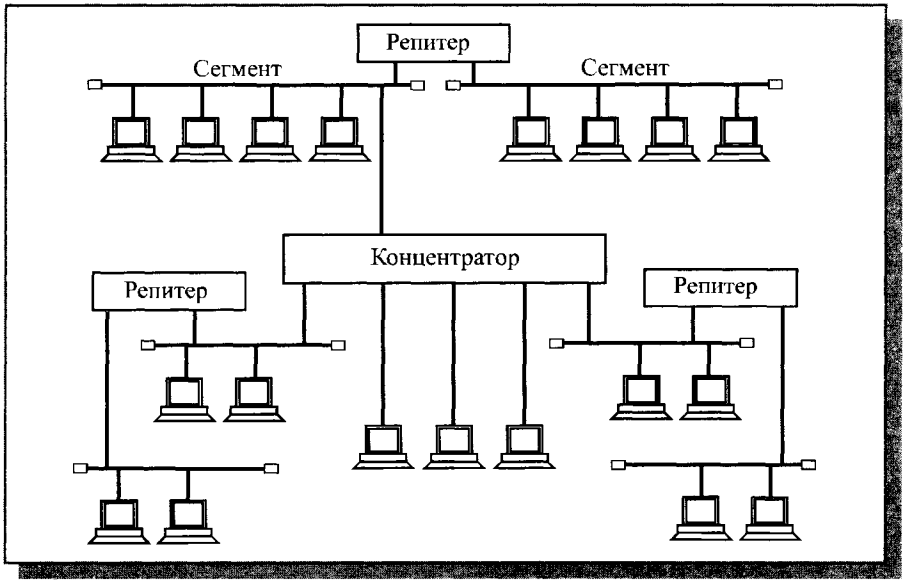



**Рис. 7.1.** Классическая топология сети Ethernet

В качестве сегмента (части сети) может выступать классическая шина или единичный абонент. Для шинных сегментов используется коаксиальный кабель, а для лучей пассивной звезды (для присоединения к концентратору одиночных компьютеров) – витая пара и оптоволоконный кабель. Главное требование к полученной в результате топологии – чтобы в ней не было замкнутых путей (петель). Фактически получается, что все абоненты соединены в физическую шину, так как сигнал от каждого из них распространяется сразу во все стороны и не возвращается назад (как в кольце).

Максимальная длина кабеля сети в целом (максимальный путь сигнала) теоретически может достигать 6,5 километров, но практически не превышает 3,5 километров.

В сети Fast Ethernet не предусмотрена физическая топология «шина», используется только пассивная звезда или пассивное дерево. К тому же в Fast Ethernet гораздо более жесткие требования к предельной длине сети. Ведь при увеличении в 10 раз скорости передачи и сохранении формата пакета его минимальная длина становится в десять раз короче. Таким образом в 10 раз уменьшается допустимая величина двойного времени прохождения сигнала по сети (5,12 мкс против 51,2 мкс в Ethernet).

Для передачи информации в сети Ethernet применяется стандартный манчестерский код.

Доступ к сети Ethernet осуществляется по случайному методу CSMA/CD, обеспечивающему равноправие абонентов. В сети используются пакеты переменной длины со структурой, представленной на рис. 7.2. (цифры показывают количество байт).

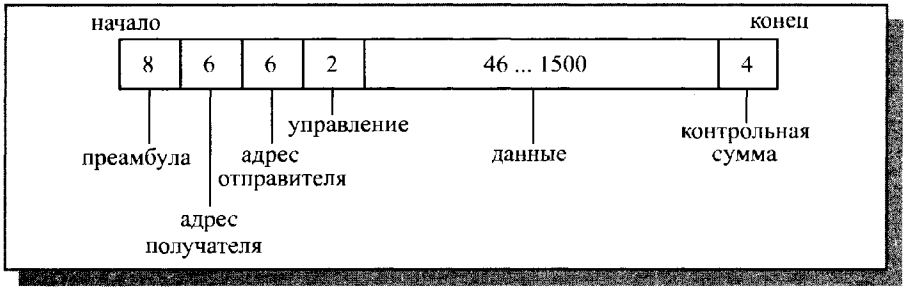



**Рис. 7.2.** Структура пакета сети Ethernet

Длина кадра Ethernet (то есть пакета без преамбулы) должна быть не менее 512 битовых интервалов или 51,2 мкс (именно такова предельная величина двойного времени прохождения в сети). Предусмотрена индивидуальная, групповая и широковещательная адресация.

В пакет Ethernet входят следующие поля:

- Преамбула состоит из 8 байт: первые семь представляют собой код 10101010, а последний байт – код 10101011. В стандарте IEEE 802.3 восьмой байт называется признаком начала кадра (SFD – Start of Frame Delimiter) и образует отдельное поле пакета.
- Адреса получателя (приемника) и отправителя (передатчика) включают по 6 байт и строятся по стандарту, описанному в разделе 3.2. Эти адресные поля обрабатываются аппаратурой абонентов.
- Поле управления (L/T – Length/Type) содержит информацию о длине поля данных. Оно может также определять тип используемого протокола. Принято считать, что если значение этого поля не больше 1500, то оно указывает на длину поля данных. Если же его значение больше 1500, то оно определяет тип кадра. Поле управления обрабатывается программно.
- Поле данных должно включать в себя от 46 до 1500 байт данных. Если пакет должен содержать менее 46 байт данных, то поле данных дополняется байтами заполнения. Согласно стандарту IEEE 802.3, в структуре пакета выделяется специальное поле заполнения (pad data – незначащие данные), которое может иметь нулевую длину, когда данных достаточно (больше 46 байт).

- Поле контрольной суммы (FCS – Frame Check Sequence) содержит 32-разрядную циклическую контрольную сумму пакета (CRC) и служит для проверки правильности передачи пакета.

Таким образом, минимальная длина кадра (пакета без преамбулы) составляет 64 байта (512 бит). Именно эта величина определяет максимально допустимую двойную задержку распространения сигнала по сети в 512 битовых интервалов (51,2 мкс для Ethernet или 5,12 мкс для Fast Ethernet). Стандарт предполагает, что преамбула может уменьшаться при прохождении пакета через различные сетевые устройства, поэтому она не учитывается. Максимальная длина кадра равна 1518 байтам (12144 бита, то есть 1214,4 мкс для Ethernet, 121,44 мкс для Fast Ethernet). Это важно для выбора размера буферной памяти сетевого оборудования и для оценки общей загруженности сети.

Выбор формата преамбулы не случаен. Дело в том, что последовательность чередующихся единиц и нулей (101010...10) в манчестерском коде характеризуется тем, что имеет переходы только в середине битовых интервалов (см. раздел 2.6.3), то есть только информационные переходы. Безусловно, приемнику просто настроиться (синхронизоваться) при такой последовательности, даже если она по какой-то причине укорачивается на несколько бит. Последние два единичные бита преамбулы (11) существенно отличаются от последовательности 101010...10 (появляются переходы еще и на границе битовых интервалов). Поэтому уже настроившийся приемник легко может выделить их и детектировать тем самым начало полезной информации (начало кадра).

Для сети Ethernet, работающей на скорости 10 Мбит/с, стандарт определяет четыре основных типа сегментов сети, ориентированных на различные среды передачи информации:

- 10BASE5 (толстый коаксиальный кабель);
- 10 BASE2 (тонкий коаксиальный кабель);
- 10BASE-T (витая пара);
- 10BASE-FL (оптоволоконный кабель).

Наименование сегмента включает в себя три элемента: цифра «10» означает скорость передачи 10 Мбит/с, слово BASE – передачу в основной полосе частот (то есть без модуляции высокочастотного сигнала), а последний элемент – допустимую длину сегмента: «5» – 500 метров, «2» – 200 метров (точнее, 185 метров) или тип линии связи: «T» – витая пара (от английского «twisted pair»), «F» – оптоволоконный кабель (от английского «fiber optic»).

Точно так же для сети Ethernet, работающей на скорости 100 Мбит/с (Fast Ethernet) стандарт определяет три типа сегментов, отличающихся типами среды передачи:

- 100BASE-T4 (счетверенная витая пара);

- 100BASE-TX (сдвоенная витая пара);
- 100BASE-FX (оптоволоконный кабель).

Здесь цифра «100» означает скорость передачи 100 Мбит/с, буква «T» – витую пару, буква «F» – оптоволоконный кабель. Типы 100BASE-TX и 100BASE-FX иногда объединяют под именем 100BASE-X, а 100BASE-T4 и 100BASE-TX – под именем 100BASE-T.

Подробнее особенности аппаратуры Ethernet, а также алгоритма управления обменом CSMA/CD и алгоритма вычисления циклической контрольной суммы (CRC) будут рассмотрены далее в специальных разделах книги. Здесь следует отметить только то, что сеть Ethernet не отличается ни рекордными характеристиками, ни оптимальными алгоритмами, она уступает по ряду параметров другим стандартным сетям. Но благодаря мощной поддержке, высочайшему уровню стандартизации, огромным объемам выпуска технических средств, Ethernet выгодно выделяется среди других стандартных сетей, и поэтому любую другую сетевую технологию принято сравнивать именно с Ethernet.

Развитие технологии Ethernet идет по пути все большего отхода от первоначального стандарта. Применение новых сред передачи и коммутаторов позволяет существенно увеличить размер сети. Отказ от манчестерского кода (в сети Fast Ethernet и Gigabit Ethernet) обеспечивает увеличение скорости передачи данных и снижение требований к кабелю. Отказ от метода управления CSMA/CD (при полнодуплексном режиме обмена) дает возможность резко повысить эффективность работы и снять ограничения с длины сети. Тем не менее, все новые разновидности сети также называются сетью Ethernet.

## Сеть Token-Ring

Сеть Token-Ring (маркерное кольцо) была предложена компанией IBM в 1985 году (первый вариант появился в 1980 году). Она предназначалась для объединения в сеть всех типов компьютеров, выпускаемых IBM. Уже тот факт, что ее поддерживает компания IBM, крупнейший производитель компьютерной техники, говорит о том, что ей необходимо уделить особое внимание. Но не менее важно и то, что Token-Ring является в настоящее время международным стандартом IEEE 802.5 (хотя между Token-Ring и IEEE 802.5 есть незначительные отличия). Это ставит данную сеть на один уровень по статусу с Ethernet.

Разрабатывалась Token-Ring как надежная альтернатива Ethernet. И хотя сейчас Ethernet вытесняет все остальные сети, Token-Ring нельзя считать безнадежно устаревшей. Более 10 миллионов компьютеров по всему миру объединены этой сетью.

Компания IBM сделала все для максимально широкого распространения своей сети: была выпущена подробная документация вплоть до принципиальных схем адаптеров. В результате многие компании, например, 3COM, Novell, Western Digital, Proteon и другие приступили к производству адаптеров. Кстати, специально для этой сети, а также для другой сети IBM PC Network была разработана концепция NetBIOS. Если в созданной ранее сети PC Network программы NetBIOS хранились во встроенной в адаптер постоянной памяти, то в сети Token-Ring уже применялась эмулирующая NetBIOS программа. Это позволило более гибко реагировать на особенности аппаратуры и поддерживать совместимость с программами более высокого уровня.

Сеть Token-Ring имеет топологию «кольцо», хотя внешне она больше напоминает звезду. Это связано с тем, что отдельные абоненты (компьютеры) присоединяются к сети не напрямую, а через специальные концентраторы или многостанционные устройства доступа (MSAU или MAU – Multistation Access Unit). Физически сеть образует звездно-кольцевую топологию (рис. 7.3). В действительности же абоненты объединяются все-таки в кольцо, то есть каждый из них передает информацию одному соседнему абоненту, а принимает информацию от другого.

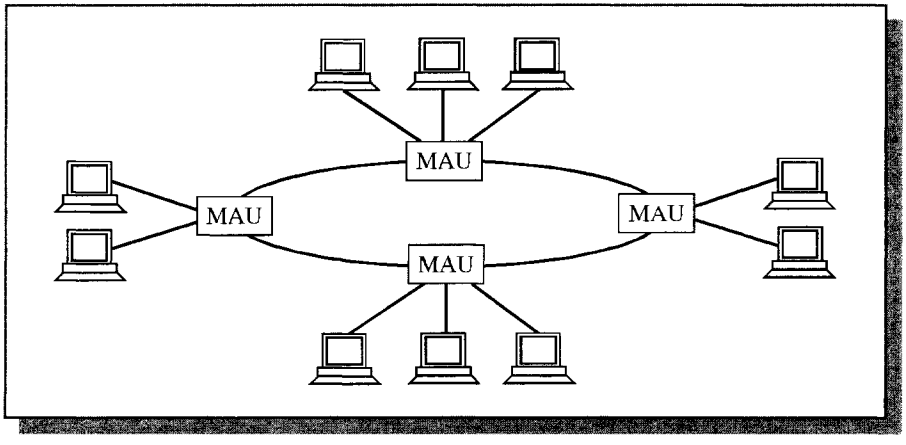



**Рис. 7.3.** Звездно-кольцевая топология сети Token-Ring

Концентратор (MAU) при этом позволяет централизовать задание конфигурации, отключение неисправных абонентов, контроль работы сети и т.д. (рис. 7.4). Никакой обработки информации он не производит.

Для каждого абонента в составе концентратора применяется специальный блок подключения к магистрали (TCU – Trunk Coupling Unit), который обеспечивает автоматическое включение абонента в кольцо, если он подключен к концентратору и исправен. Если абонент отключается от

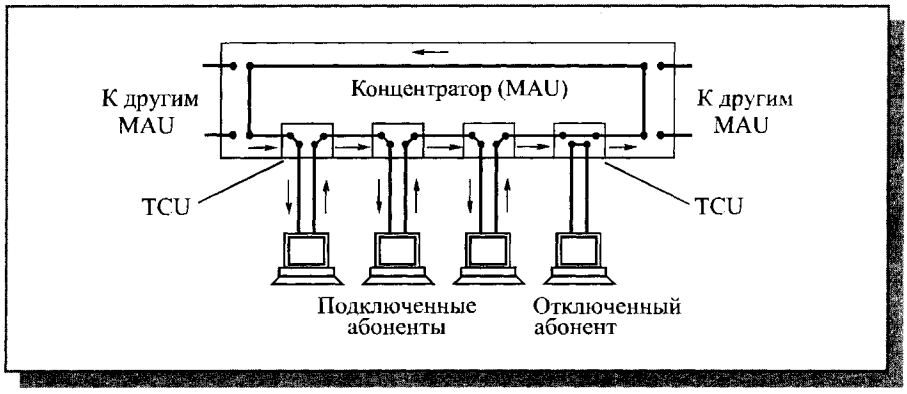



**Рис. 7.4.** Соединение абонентов сети Token-Ring в кольцо с помощью концентратора (MAU)

концентратора или же он неисправен, то блок TCU автоматически восстанавливает целостность кольца без участия данного абонента. Срабатывает TCU по сигналу постоянного тока (так называемый «фантомный» ток), который приходит от абонента, желающего включиться в кольцо. Абонент может также отключиться от кольца и провести процедуру самотестирования (крайний правый абонент на рис. 7.4). «Фантомный» ток никак не влияет на информационный сигнал, так как сигнал в кольце не имеет постоянной составляющей.

Конструктивно концентратор представляет собой автономный блок с десятью разъемами на передней панели (рис. 7.5).

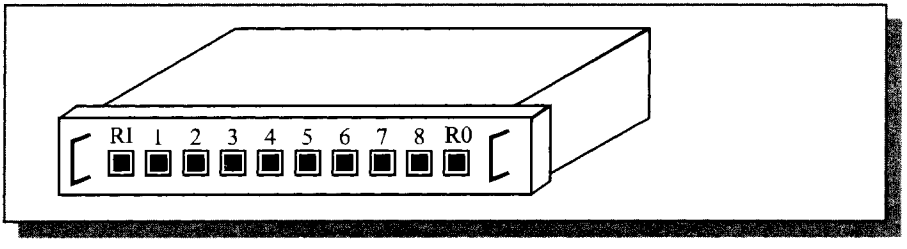



**Рис. 7.5.** Концентратор Token-Ring (8228 MAU)

Восемь центральных разъемов (1...8) предназначены для подключения абонентов (компьютеров) с помощью адаптерных (Adapter Cable) или радиальных кабелей. Два крайних разъема: входной RI (Ring In) и выходной RO (Ring Out) служат для подключения к другим концентраторам с помощью специальных магистральных кабелей (Path cable). Предлагаются настенный и настольный варианты концентратора.

Существуют как пассивные, так и активные концентраторы MAU. Активный концентратор восстанавливает сигнал, приходящий от абонента (то есть работает, как концентратор Ethernet). Пассивный концентратор не выполняет восстановление сигнала, он только перекоммутирует линии связи.

Концентратор в сети может быть единственным (как на рис. 7.4), в этом случае в кольцо замыкаются только абоненты, подключенные к нему. Внешне такая топология выглядит, как звезда. Если же нужно подключить к сети более восьми абонентов, то несколько концентраторов соединяются магистральными кабелями и образуют звездно-кольцевую топологию.

Как уже отмечалось, кольцевая топология очень чувствительна к обрывам кабеля кольца. Для повышения живучести сети, в Token-Ring предусмотрен режим так называемого сворачивания кольца, что позволяет обойти место обрыва.

В нормальном режиме концентраторы соединены в кольцо двумя параллельными кабелями, но передача информации производится при этом только по одному из них (рис. 7.6).

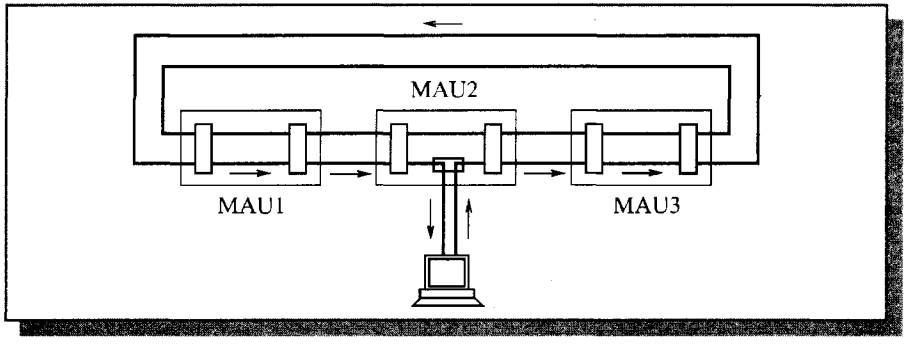



**Рис. 7.6.** Объединение концентраторов MAU в нормальном режиме

В случае одиночного повреждения (обрыва) кабеля сеть осуществляет передачу по обоим кабелям, обходя тем самым поврежденный участок. При этом даже сохраняется порядок обхода абонентов, подключенных к концентраторам (рис. 7.7). Правда, увеличивается суммарная длина кольца.

В случае множественных повреждений кабеля сеть распадается на несколько частей (сегментов), не связанных между собой, но сохраняющих полную работоспособность (рис. 7.8). Максимальная часть сети остается при этом связанной, как и прежде. Конечно, это уже не спасает сеть в целом, но позволяет при правильном распределении абонентов по концентраторам сохранять значительную часть функций поврежденной сети.

Несколько концентраторов может конструктивно объединяться в группу, кластер (cluster), внутри которого абоненты также соединены в кольцо. Применение кластеров позволяет увеличивать количество або-

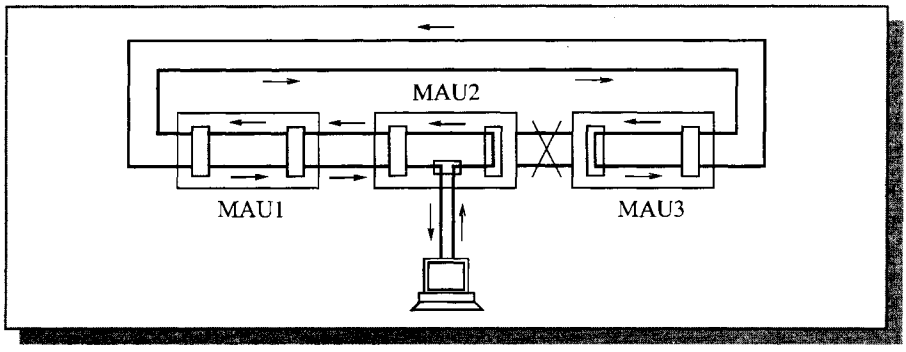



**Рис. 7.7.** Сворачивание кольца при повреждении кабеля

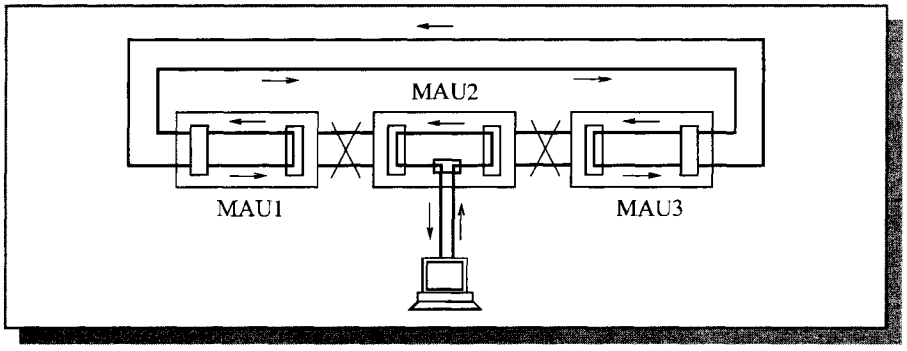



**Рис. 7.8.** Распад кольца при множественных повреждениях кабеля

нентов, подключенных к одному центру, например, до 16 (если в кластер входит два концентратора).

В качестве среды передачи в сети IBM Token-Ring сначала применялась витая пара — как неэкранированная (UTP), так и экранированная (STP), но затем появились варианты аппаратуры для коаксиального кабеля, а также для оптоволоконного кабеля в стандарте FDDI.

Основные технические характеристики классического варианта сети Token-Ring:

- максимальное количество концентраторов типа IBM 8228 MAU – 12;
- максимальное количество абонентов в сети – 96;
- максимальная длина кабеля между абонентом и концентратором – 45 метров;
- максимальная длина кабеля между концентраторами – 45 метров;
- максимальная длина кабеля, соединяющего все концентраторы – 120 метров;
- скорость передачи данных – 4 Мбит/с и 16 Мбит/с.

Все приведенные характеристики относятся к случаю использования неэкранированной витой пары. Если применяется другая среда передачи, характеристики сети могут отличаться. Например, при использовании экранированной витой пары (STP) количество абонентов может быть увеличено до 260 (вместо 96), длина кабеля – до 100 метров (вместо 45), количество концентраторов – до 33, а полная длина кольца, соединяющего концентраторы – до 200 метров. Оптоволоконный кабель позволяет увеличивать длину кабеля до двух километров.

Для передачи информации в Token-Ring применяется бифазный код (точнее, его вариант с обязательным переходом в центре битового интервала). Как и в любой звездообразной топологии, никаких дополнительных мер по электрическому согласованию и внешнему заземлению не требуется. Согласование выполняется аппаратурой сетевых адаптеров и концентраторов.

Для присоединения кабелей в Token-Ring используются разъемы RJ-45 (для неэкранированной витой пары), а также MIC и DB9P. Провода в кабеле соединяют одноименные контакты разъемов (то есть используются так называемые «прямые» кабели).

Сеть Token-Ring в классическом варианте уступает сети Ethernet как по допустимому размеру, так и по максимальному количеству абонентов. Что касается скорости передачи, то в настоящее время имеются версии Token-Ring на скорость 100 Мбит/с (High Speed Token-Ring, HSTR) и на 1000 Мбит/с (Gigabit Token-Ring). Компании, поддерживающие Token-Ring (среди которых IBM, Olicom, Madge), не намерены отказываться от своей сети, рассматривая ее как достойного конкурента Ethernet.

По сравнению с аппаратурой Ethernet аппаратура Token-Ring заметно дороже, так как используется более сложный метод управления обменом, поэтому сеть Token-Ring не получила столь широкого распространения.

Однако в отличие от Ethernet сеть Token-Ring значительно лучше держит высокий уровень нагрузки (более 30–40%) и обеспечивает гарантированное время доступа. Это необходимо, например, в сетях производственного назначения, в которых задержка реакции на внешнее событие может привести к серьезным авариям.

В сети Token-Ring используется классический маркерный метод доступа, то есть по кольцу постоянно циркулирует маркер, к которому абоненты могут присоединять свои пакеты данных (см. рис. 4.15). Отсюда следует такое важное достоинство данной сети, как отсутствие конфликтов, но есть и недостатки, в частности необходимость контроля целостности маркера и зависимость функционирования сети от каждого абонента (в случае неисправности абонент обязательно должен быть исключен из кольца).

Предельное время передачи пакета в Token-Ring — 10 мс. При максимальном количестве абонентов 260 полный цикл работы кольца соста-

вит 260 × 10 мс = 2,6 с. За это время все 260 абонентов смогут передать свои пакеты (если, конечно, им есть что передавать). За это же время свободный маркер обязательно дойдет до каждого абонента. Этот же интервал является верхним пределом времени доступа Token-Ring.

Каждый абонент сети (его сетевой адаптер) должен выполнять следующие функции:

- выявление ошибок передачи;
- контроль конфигурации сети (восстановление сети при выходе из строя того абонента, который предшествует ему в кольце);
- контроль многочисленных временных соотношений, принятых в сети.

Большое количество функций, конечно, усложняет и удорожает аппаратуру сетевого адаптера.

Для контроля целостности маркера в сети используется один из абонентов (так называемый *активный монитор*). При этом его аппаратура ничем не отличается от остальных, но его программные средства следят за временными соотношениями в сети и формируют в случае необходимости новый маркер.

Активный монитор выполняет следующие функции:

- запускает в кольцо маркер в начале работы и при его исчезновении;
- регулярно (раз в 7 с) сообщает о своем присутствии специальным управляющим пакетом (AMP – Active Monitor Present);
- удаляет из кольца пакет, который не был удален пославшим его абонентом;
- следит за допустимым временем передачи пакета.

Активный монитор выбирается при инициализации сети, им может быть любой компьютер сети, но, как правило, им становится первый включенный в сеть абонент. Абонент, ставший активным монитором, включает в сеть свой буфер (сдвиговый регистр), который гарантирует, что маркер будет умещаться в кольце даже при минимальной длине кольца. Размер этого буфера – 24 бита для скорости 4 Мбит/с и 32 бита для скорости 16 Мбит/с.

Каждый абонент постоянно следит за тем, как активный монитор выполняет свои обязанности. Если активный монитор по какой-то причине выходит из строя, то включается специальный механизм, посредством которого все другие абоненты (запасные, резервные мониторы) принимают решение о назначении нового активного монитора. Для этого абонент, обнаруживший аварию активного монитора, передает по кольцу управляющий пакет (пакет запроса маркера) со своим MAC-адресом. Каждый следующий абонент сравнивает MAC-адрес из пакета с собственным. Если его собственный адрес меньше, он передает пакет дальше без изменений. Если же больше, то он устанавливает в пакете свой MAC-адрес. Активным монитором станет тот абонент, у которого значение MAC-адреса больше,

чем у остальных (он должен трижды получить обратно пакет со своим MAC-адресом). Признаком выхода из строя активного монитора является невыполнение им одной из перечисленных функций.

Маркер сети Token-Ring представляет собой управляющий пакет, содержащий всего три байта (рис. 7.9): байт начального разделителя (SD – Start Delimiter), байт управления доступом (AC – Access Control) и байт конечного разделителя (ED – End Delimiter). Все эти три байта входят также в состав информационного пакета, правда, функции их в маркере и в пакете несколько различаются.

Начальный и конечный разделители представляют собой не просто последовательность нулей и единиц, а содержат сигналы специального вида. Это было сделано для того, чтобы разделители нельзя было спутать ни с какими другими байтами пакетов.

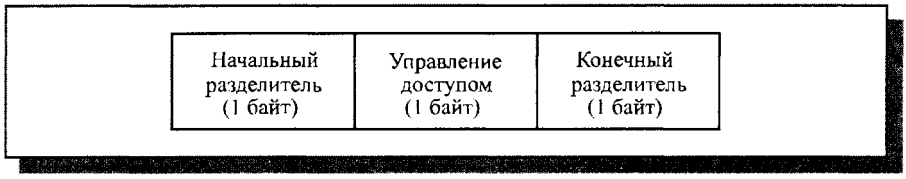



**Рис. 7.9.** Формат маркера сети Token-Ring

Начальный разделитель SD содержит четыре нестандартных битовых интервала (рис. 7.10). Два из них, обозначающихся J, представляют собой низкий уровень сигнала в течение всего битового интервала. Два других бита, обозначающихся K, представляют собой высокий уровень сигнала в течение всего битового интервала. Понятно, что такие сбои в синхронизации легко выявляются приемником. Биты J и K никогда не могут встречаться среди битов полезной информации.

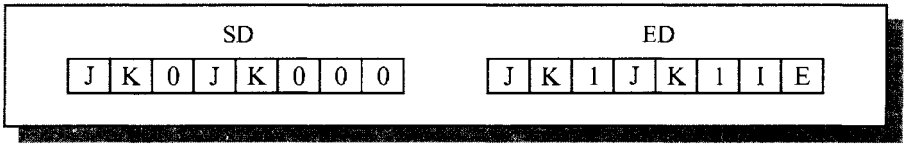



**Рис. 7.10.** Форматы начального (SD) и конечного (ED) разделителей

Конечный разделитель ED также содержит в себе четыре бита специального вида (два бита J и два бита K), а также два единичных бита. Но, кроме того, в него входят и два информационных бита, которые имеют смысл только в составе информационного пакета:

- Бит I (Intermediate) представляет собой признак промежуточного пакета (1 соответствует первому в цепочке или промежуточному пакету, 0 – последнему в цепочке или единственному пакету).

- Бит E (Error) является признаком обнаруженной ошибки (0 соответствует отсутствию ошибок, 1 – их наличию).

Байт управления доступом (AC – Access Control) разделен на четыре поля (рис. 7.11): поле приоритета (три бита), бит маркера, бит монитора и поле резервирования (три бита).

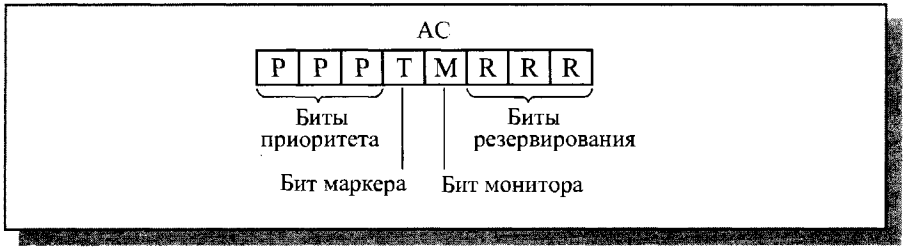



**Рис. 7.11.** Формат байта управления доступом

Биты (поле) приоритета позволяют абоненту присваивать приоритет своим пакетам или маркеру (приоритет может быть от 0 до 7, причем 7 соответствует наивысшему приоритету, а 0 – низшему). Абонент может присоединить к маркеру свой пакет только тогда, когда его собственный приоритет (приоритет его пакетов) такой же или выше приоритета маркера.

Бит маркера определяет, присоединен ли к маркеру пакет или нет (единица соответствует маркеру без пакета, нуль – маркеру с пакетом). Бит монитора, установленный в единицу, говорит о том, что данный маркер передан активным монитором.

Биты (поле) резервирования позволяют абоненту зарезервировать свое право на дальнейший захват сети, то есть занять очередь на обслуживание. Если приоритет абонента (приоритет его пакетов) выше, чем текущее значение поля резервирования, то он может записать туда свой приоритет вместо прежнего. После обхода по кольцу в поле резервирования будет записан наивысший приоритет из всех абонентов. Содержимое поля резервирования аналогично содержимому поля приоритета, но говорит о будущем приоритете.

В результате использования полей приоритета и резервирования обеспечивается возможность доступа к сети только абонентам, имеющим пакеты для передачи с наивысшим приоритетом. Менее приоритетные пакеты будут обслуживаться только по исчерпании более приоритетных пакетов.

Формат информационного пакета (кадра) Token-Ring представлен на рис. 7.12. Помимо начального и конечного разделителей, а также байта управления доступом в этот пакет входят также байт управления пакетом, сетевые адреса приемника и передатчика, данные, контрольная сумма и байт состояния пакета.


**Рис. 7.12.** Формат пакета (кадра) сети Token-Ring (длина полей дана в байтах)

Назначение полей пакета (кадра):

- Начальный разделитель (SD) является признаком начала пакета, формат – такой же, как и в маркере.
- Байт управления доступом (AC) имеет тот же формат, что и в маркере.
- Байт управления пакетом (FC – Frame Control) определяет тип пакета (кадра).
- Шестибайтовые MAC-адреса отправителя и получателя пакета имеют стандартный формат, описанный в разделе 3.2.
- Поле данных (Data) включает в себя передаваемые данные (в информационном пакете) или информацию для управления обменом (в управляющем пакете).
- Поле контрольной суммы (FCS – Frame Check Sequence) представляет собой 32-разрядную циклическую контрольную сумму пакета (CRC).
- Конечный разделитель (ED), как и в маркере, указывает на конец пакета. Кроме того, он определяет, является ли данный пакет промежуточным или заключительным в последовательности передаваемых пакетов, а также содержит признак ошибочности пакета (см. рис. 7.10).
- Байт состояния пакета (FS – Frame Status) говорит о том, что происходило с данным пакетом: был ли он увиден приемником (то есть, существует ли приемник с заданным адресом) и скопирован в память приемника. По нему отправитель пакета узнает, дошел ли пакет по назначению и без ошибок или его надо передавать заново.

Следует отметить, что больший допустимый размер передаваемых данных в одном пакете по сравнению с сетью Ethernet может стать решающим фактором для увеличения производительности сети. Теоретически для скоростей передачи 16 Мбит/с и 100 Мбит/с длина поля данных может достигать даже 18 Кбайт, что принципиально при передаче больших объемов данных. Но даже при скорости 4 Мбит/с благодаря маркерному методу доступа сеть Token-Ring часто обеспечивает большую фактическую скорость передачи, чем сеть Ethernet (10 Мбит/с). Особенно заметно преимущество Token-Ring при боль-

ших нагрузках (свыше 30–40%), так как в этом случае метод CSMA/CD требует много времени на разрешение повторных конфликтов.

Абонент, желающий передавать пакет, ждет прихода свободного маркера и захватывает его. Захваченный маркер превращается в обрамление информационного пакета. Затем абонент передает информационный пакет в кольцо и ждет его возвращения. После этого он освобождает маркер и снова посылает его в сеть.

Помимо маркера и обычного пакета в сети Token-Ring может передаваться специальный управляющий пакет, служащий для прерывания передачи (Abort). Он может быть послан в любой момент и в любом месте потока данных. Пакет этот состоит из двух однобайтовых полей – начального (SD) и конечного (ED) разделителей описанного формата.

Интересно, что в более быстрой версии Token-Ring (16 Мбит/с и выше) применяется так называемый метод раннего формирования маркера (ETR – Early Token Release). Он позволяет избежать непроизводительного использования сети в то время, пока пакет данных не вернется по кольцу к своему отправителю.

Метод ETR сводится к тому, что сразу после передачи своего пакета, присоединенного к маркеру, любой абонент выдает в сеть новый свободный маркер. Другие абоненты могут начинать передачу своих пакетов сразу же после окончания пакета предыдущего абонента, не дожидаясь, пока он завершит обход всего кольца сети. В результате в сети может находиться несколько пакетов одновременно, но всегда будет не более одного свободного маркера. Этот конвейер особенно эффективен в сетях большой протяженности, имеющих значительную задержку распространения.

При подключении абонента к концентратору он выполняет процедуру автономного самотестирования и тестирования кабеля (в кольцо он пока не включается, так как нет сигнала «фантомного» тока). Абонент посылает сам себе ряд пакетов и проверяет правильность их прохождения (его вход напрямую соединен с его же выходом блоком TCU, как показано на рис. 7.4). После этого абонент включает себя в кольцо, посылая «фантомный» ток. В момент включения передаваемый по кольцу пакет может быть испорчен. Далее абонент настраивает синхронизацию и проверяет наличие в сети активного монитора. Если активного монитора нет, абонент начинает состязание за право стать им. Затем абонент проверяет уникальность собственного адреса в кольце и собирает информацию о других абонентах.,после чего он становится полноправным участником обмена по сети.

В процессе обмена каждый абонент следит за исправностью предыдущего абонента (по кольцу). Если он подозревает отказ предыдущего абонента, он запускает процедуру автоматического восстановления кольца. Специальный управляющий пакет (бакен) говорит предыдущему абоненту о необходимости провести самотестирование и, возможно, отключиться от кольца.

В сети Token-Ring предусмотрено также использование мостов и коммутаторов. Они применяются для разделения большого кольца на несколько кольцевых сегментов, имеющих возможность обмена пакетами между собой. Это позволяет снизить нагрузку на каждый сегмент и увеличить долю времени, предоставляемую каждому абоненту.

В результате можно сформировать распределенное кольцо, то есть объединение нескольких кольцевых сегментов одним большим магистральным кольцом (рис. 7.13) или же звездно-кольцевую структуру с центральным коммутатором, к которому подключены кольцевые сегменты (рис. 7.14).

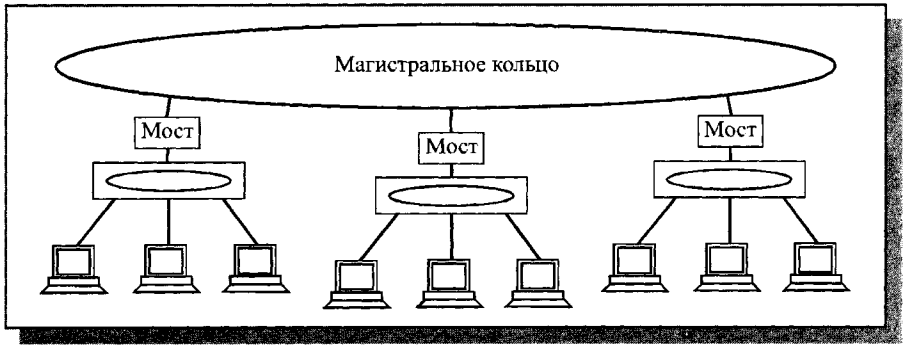



**Рис. 7.13.** Объединение сегментов магистральным кольцом с помощью мостов

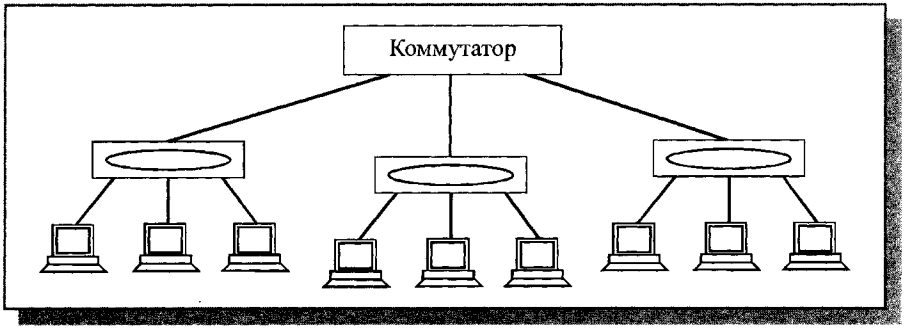



**Рис. 7.14.** Объединение сегментов центральным коммутатором

## Сеть Arcnet

Сеть Arcnet (или ARCnet от английского Attached Resource Computer Net, компьютерная сеть соединенных ресурсов) – это одна из старейших сетей. Она была разработана компанией Datapoint Corporation еще в 1977

году. Международные стандарты на эту сеть отсутствуют, хотя именно она считается родоначальницей метода маркерного доступа. Несмотря на отсутствие стандартов, сеть Arcnet до недавнего времени (в 1980–1990 гг.) пользовалась популярностью и, даже серьезно конкурировала с Ethernet. Большое количество компаний (например, Datapoint, Standard Microsystems, Xircom и др.) производили аппаратуру для сети этого типа. Но сейчас производство аппаратуры Arcnet практически прекращено.

Среди основных достоинств сети Arcnet по сравнению с Ethernet можно назвать ограниченную величину времени доступа, высокую надежность связи, простоту диагностики, а также сравнительно низкую стоимость адаптеров. К наиболее существенным недостаткам сети относятся низкая скорость передачи информации (2,5 Мбит/с), система адресации и формат пакета.

Для передачи информации в сети Arcnet используется довольно редкий код, в котором логической единице соответствуют два импульса в течение битового интервала, а логическому нулю – один импульс. Очевидно, что это самосинхронизирующийся код, который требует еще большей пропускной способности кабеля, чем даже манчестерский.

В качестве среды передачи в сети используется коаксиальный кабель с волновым сопротивлением 93 Ом, к примеру, марки RG-62A/U. Варианты с витой парой (экранированной и неэкранированной) не получили широкого распространения. Были предложены и варианты на оптоволоконном кабеле, но и они также не спасли Arcnet.

В качестве топологии сеть Arcnet использует классическую шину (Arcnet-BUS), а также пассивную звезду (Arcnet-STAR). В звезде применяются концентраторы (хабы). Возможно объединение с помощью концентраторов шинных и звездных сегментов в древовидную топологию (как и в Ethernet). Главное ограничение – в топологии не должно быть замкнутых путей (петель). Еще одно ограничение: количество сегментов, соединенных последовательной цепочкой с помощью концентраторов, не должно превышать трех.

Концентраторы бывают двух видов:

- Активные концентраторы (восстанавливают форму приходящих сигналов и усиливают их). Количество портов – от 4 до 64. Активные концентраторы могут соединяться между собой (каскадироваться).
- Пассивные концентраторы (просто смешивают приходящие сигналы без усиления). Количество портов – 4. Пассивные концентраторы не могут соединяться между собой. Они могут связывать только активные концентраторы и/или сетевые адаптеры.

Шинные сегменты могут подключаться только к активным концентраторам.

Сетевые адаптеры также бывают двух видов:

- Высокоимпедансные (Bus), предназначенные для использования в шинных сегментах:
- Низкоимпедансные (Star), предназначенные для использования в пассивной звезде.

Низкоимпедансные адаптеры отличаются от высокоимпедансных тем, что они содержат в своем составе согласующие 93-омные терминаторы. При их применении внешнее согласование не требуется. В шинных сегментах низкоимпедансные адаптеры могут использоваться как оконечные для согласования шины. Высоимпедансные адаптеры требуют применения внешних 93-омных терминаторов. Некоторые сетевые адаптеры имеют возможность переключения из высокоимпедансного состояния в низкоимпедансное, они могут работать и в шине, и в звезде.

Таким образом, топология сети Arcnet имеет следующий вид (рис. 7.15).

Основные технические характеристики сети Arcnet следующие:

- Среда передачи – коаксиальный кабель, витая пара.
- Максимальная длина сети – 6 километров.
- Максимальная длина кабеля от абонента до пассивного концентратора – 30 метров.
- Максимальная длина кабеля от абонента до активного концентратора – 600 метров.
- Максимальная длина кабеля между активным и пассивным концентраторами – 30 метров.
- Максимальная длина кабеля между активными концентраторами – 600 метров.
- Максимальное количество абонентов в сети – 255.
- Максимальное количество абонентов на шинном сегменте – 8.
- Минимальное расстояние между абонентами в шине – 1 метр.
- Максимальная длина шинного сегмента – 300 метров.
- Скорость передачи данных – 2,5 Мбит/с.

При создании сложных топологий необходимо следить за тем, чтобы задержка распространения сигналов в сети между абонентами не превышала 30 мкс. Максимальное затухание сигнала в кабеле на частоте 5 МГц не должно превышать 11 дБ.

В сети Arcnet используется маркерный метод доступа (метод передачи права), но он несколько отличается от аналогичного в сети Token-Ring. Ближе всего этот метод к тому, который предусмотрен в стандарте IEEE 802.4. Последовательность действий абонентов при данном методе:

1. Абонент, желающий передавать, ждет прихода маркера.
2. Получив маркер, он посылает запрос на передачу абоненту-приемнику информации (спрашивает, готов ли приемник принять его пакет).
3. Приемник, получив запрос, посылает ответ (подтверждает свою готовность).

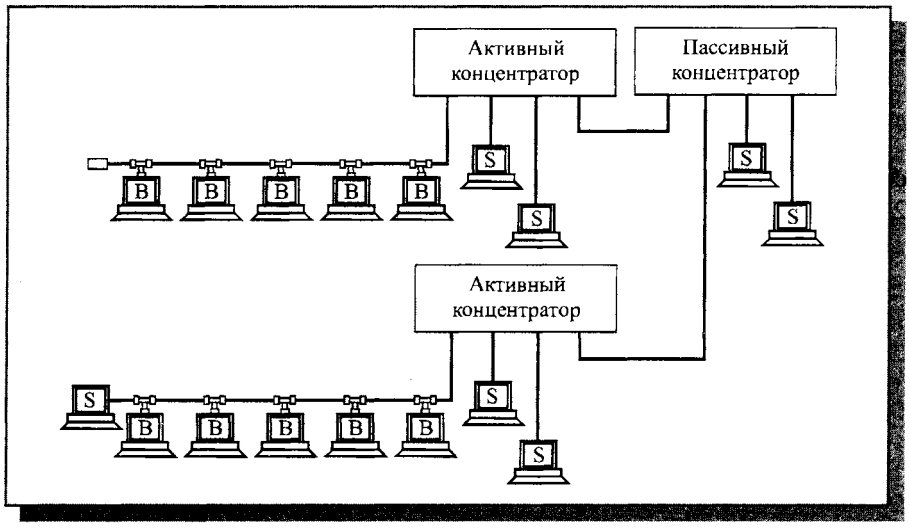



**Рис. 7.15.** Топология сети Arcnet типа шина
(B – адаптеры для работы в шине, S – адаптеры для работы в звезде)

4. Получив подтверждение готовности, абонент-передатчик посылает свой пакет.
5. Получив пакет, приемник посылает подтверждение приема пакета.
6. Передатчик, получив подтверждение приема пакета, заканчивает свой сеанс связи. После этого маркер передается следующему абоненту по порядку убывания сетевых адресов.

Таким образом, в данном случае пакет передается только тогда, когда есть уверенность в готовности приемника принять его. Это существенно увеличивает надежность передачи.

Так же, как и в случае Token-Ring, конфликты в Arcnet полностью исключены. Как и любая маркерная сеть, Arcnet хорошо держит нагрузку и гарантирует величину времени доступа к сети (в отличие от Ethernet). Полное время обхода маркером всех абонентов составляет 840 мс. Соответственно, этот же интервал определяет верхний предел времени доступа к сети.

Маркер формируется специальным абонентом – контроллером сети. Им является абонент с минимальным (нулевым) адресом.

Если абонент не получает свободный маркер в течение 840 мс, то он посылает в сеть длинную битовую последовательность (для гарантированного уничтожения испорченного старого маркера). После этого производится процедура контроля сети и назначения (при необходимости) нового контроллера.

Размер пакета сети Arcnet составляет 0,5 Кбайта. Помимо поля данных в него входят также 8-битные адреса приемника и передатчика и

16-битная циклическая контрольная сумма (CRC). Такой небольшой размер пакета оказывается не слишком удобным при высокой интенсивности обмена по сети.

Адаптеры сети Arcnet отличаются от адаптеров других сетей тем, что в них необходимо с помощью переключателей или перемычек установить собственный сетевой адрес (всего их может быть 255, так как последний, 256-й адрес применяется в сети для режима широкого вещания). Контроль уникальности каждого адреса сети полностью возлагается на пользователей сети. Подключение новых абонентов становится при этом довольно сложным, так как необходимо задавать тот адрес, который еще не использовался. Выбор 8-битного формата адреса ограничивает допустимое количество абонентов в сети – 255, что может быть недостаточно для крупных компаний.

В результате все это привело к практически полному отказу от сети Arcnet. Существовали варианты сети Arcnet, рассчитанные на скорость передачи 20 Мбит/с, но они не получили широкого распространения.

# Лекция 8. Скоростные и беспроводные сети

**В этой лекции представлен материал о последних разработках в области локальных сетей, скоростных и сверхскоростных стандартных локальных сетях, а также о беспроводных стандартных сетях, их особенностях, достоинствах и недостатках.**

**Ключевые слова:** FDDI, 100VG-AnyLAN, Gigabit Ethernet, ATM, WLAN, Wi-Fi, методы управления, форматы пакетов, среды передачи.

## Сеть FDDI

Сеть FDDI (от английского Fiber Distributed Data Interface, оптоволоконный распределенный интерфейс данных) – это одна из новейших разработок стандартов локальных сетей. Стандарт FDDI был предложен Американским национальным институтом стандартов ANSI (спецификация ANSI X3T9.5). Затем был принят стандарт ISO 9314, соответствующий спецификациям ANSI. Уровень стандартизации сети достаточно высок.

В отличие от других стандартных локальных сетей, стандарт FDDI изначально ориентировался на высокую скорость передачи (100 Мбит/с) и на применение наиболее перспективного оптоволоконного кабеля. Поэтому в данном случае разработчики не были стеснены рамками старых стандартов, ориентировавшихся на низкие скорости и электрический кабель.

Выбор оптоволокна в качестве среды передачи определил такие преимущества новой сети, как высокая помехозащищенность, максимальная секретность передачи информации и прекрасная гальваническая развязка абонентов. Высокая скорость передачи, которая в случае оптоволоконного кабеля достигается гораздо проще, позволяет решать многие задачи, недоступные менее скоростным сетям, например, передачу изображений в реальном масштабе времени. Кроме того, оптоволоконный кабель легко решает проблему передачи данных на расстояние нескольких километров без ретрансляции, что позволяет строить большие по размерам сети, охватывающие даже целые города и имеющие при этом все преимущества локальных сетей (в частности, низкий уровень ошибок). Все это определило популярность сети FDDI, хотя она распространена еще не так широко, как Ethernet и Token-Ring.

За основу стандарта FDDI был взят метод маркерного доступа, предусмотренный международным стандартом IEEE 802.5 (Token-Ring). Несущественные отличия от этого стандарта определяются необходимостью обеспечить высокую скорость передачи информации на большие расстояния. Топология сети FDDI – это кольцо, наиболее подходящая топо-

логия для оптоволоконного кабеля. В сети применяется два разнонаправленных оптоволоконных кабеля, один из которых обычно находится в резерве, однако такое решение позволяет использовать и полнодуплексную передачу информации (одновременно в двух направлениях) с удвоенной эффективной скоростью в 200 Мбит/с (при этом каждый из двух каналов работает на скорости 100 Мбит/с). Применяется и звездно-кольцевая топология с концентраторами, включенными в кольцо (как в Token-Ring).

Основные технические характеристики сети FDDI:

- Максимальное количество абонентов сети – 1000.
- Максимальная протяженность кольца сети – 20 километров.
- Максимальное расстояние между абонентами сети – 2 километра.
- Среда передачи – многомодовый оптоволоконный кабель (возможно применение электрической витой пары).
- Метод доступа – маркерный.
- Скорость передачи информации – 100 Мбит/с (200 Мбит/с для дуплексного режима передачи).

Стандарт FDDI имеет значительные преимущества по сравнению со всеми рассмотренными ранее сетями. Например, сеть Fast Ethernet, имеющая такую же пропускную способность 100 Мбит/с, не может сравниться с FDDI по допустимым размерам сети. К тому же маркерный метод доступа FDDI обеспечивает в отличие от CSMA/CD гарантированное время доступа и отсутствие конфликтов при любом уровне нагрузки.

Ограничение на общую длину сети в 20 км связано не с затуханием сигналов в кабеле, а с необходимостью ограничения времени полного прохождения сигнала по кольцу для обеспечения предельно допустимого времени доступа. А вот максимальное расстояние между абонентами (2 км при многомодовом кабеле) определяется как раз затуханием сигналов в кабеле (оно не должно превышать 11 дБ). Предусмотрена также возможность применения одномодового кабеля, и в этом случае расстояние между абонентами может достигать 45 километров, а полная длина кольца – 200 километров.

Имеется также реализация FDDI на электрическом кабеле (CDDI – Copper Distributed Data Interface или TPDDI – Twisted Pair Distributed Data Interface). При этом используется кабель категории 5 с разъемами RJ-45. Максимальное расстояние между абонентами в этом случае должно быть не более 100 метров. Стоимость оборудования сети на электрическом кабеле в несколько раз меньше. Но эта версия сети уже не имеет столь очевидных преимуществ перед конкурентами, как изначальная оптоволоконная FDDI. Электрические версии FDDI стандартизованы гораздо хуже оптоволоконных, поэтому совместимость оборудования разных производителей не гарантируется.

**Таблица 8.1.** Код 4B/5B

| Информация | Код 4B/5B | Информация | Код 4B/5B |
|---|---|---|---|
| 0000 | 11110 | 1000 | 10010 |
| 0001 | 01001 | 1001 | 10011 |
| 0010 | 10100 | 1010 | 10110 |
| 0011 | 10101 | 1011 | 10111 |
| 0100 | 01010 | 1100 | 11010 |
| 0101 | 01011 | 1101 | 11011 |
| 0110 | 01110 | 1110 | 11100 |
| 0111 | 01111 | 1111 | 11101 |

Для передачи данных в FDDI применяется уже упоминавшийся в первой главе код 4B/5B (см. табл. 8.1), специально разработанный для этого стандарта. Главный принцип кода – избежать длинных последовательностей нулей и единиц. Код 4B/5B обеспечивает скорость передачи 100 Мбит/с при пропускной способности кабеля 125 миллионов сигналов в секунду (или 125 МБод), а не 200 МБод, как в случае манчестерского кода. При этом каждым четырем битам передаваемой информации (каждому полубайту или ниббл) ставится в соответствие пять передаваемых по кабелю битов. Это позволяет приемнику восстанавливать синхронизацию приходящих данных один раз на четыре принятых бита. Таким образом, достигается компромисс между простейшим кодом NRZ и самосинхронизирующимся на каждом бите манчестерского кода. Дополнительно сигналы кодируются кодом NRZI (в случае TPDDI) и MLT-3 (в случае FDDI).

Стандарт FDDI для достижения высокой гибкости сети предусматривает включение в кольцо абонентов двух типов:

- Абоненты (станции) класса A (абоненты двойного подключения, DAS – Dual Attachment Stations) подключаются к обоим (внутреннему и внешнему) кольцам сети. При этом реализуется возможность обмена со скоростью до 200 Мбит/с или резервирования кабеля сети (при повреждении основного кабеля используется резервный). Аппаратура этого класса применяется в самых критичных с точки зрения быстродействия частях сети.
- Абоненты (станции) класса B (абоненты одинарного подключения, SAS – Single Attachment Stations) подключаются только к одному (внешнему) кольцу сети. Они более простые и дешевые, по сравнению с адаптерами класса A, но не имеют их возможностей. В сеть

они могут включаться только через концентратор или обходной коммутатор, отключающий их в случае аварии.

Кроме собственно абонентов (компьютеров, терминалов и т.д.) в сети используются связные концентраторы (Wiring Concentrators), включение которых позволяет собрать в одно место все точки подключения с целью контроля работы сети, диагностики неисправностей и упрощения реконфигурации. При применении кабелей разных типов (например, оптоволоконного кабеля и витой пары) концентратор выполняет также функцию преобразования электрических сигналов в оптические и наоборот. Концентраторы также бывают двойного подключения (DAC – Dual Attachment Concentrator) и одинарного подключения (SAC – Single Attachment Concentrator).

Пример конфигурации сети FDDI представлен на рис. 8.1. Принцип объединения устройств сети иллюстрируется на рис. 8.2.

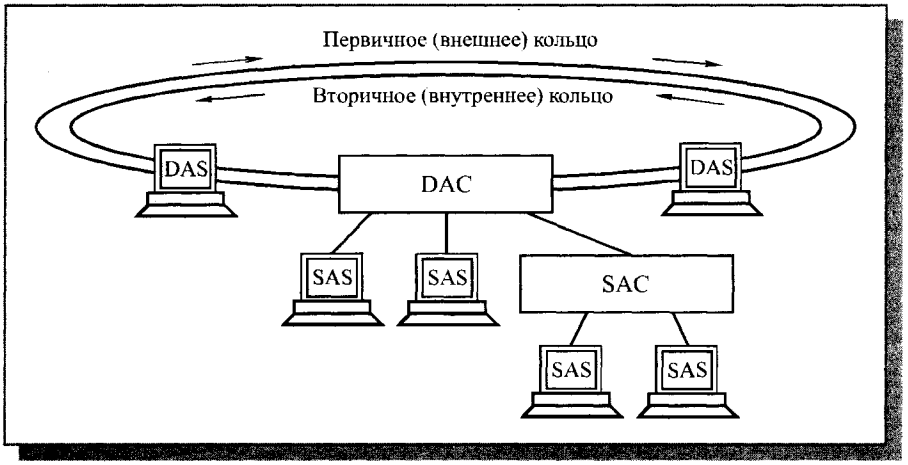



**Рис. 8.1.** Пример конфигурации сети FDDI

FDDI определяет четыре типа портов абонентов ( рис. 8.2):

- Порт A определен только для устройств двойного подключения, его вход подключается к первичному (внешнему) кольцу, а выход – к вторичному (внутреннему) кольцу.
- Порт B определен только для устройств двойного подключения, его вход подключается к вторичному (внутреннему) кольцу, а выход – к первичному (внешнему) кольцу. Порт A обычно соединяется с портом B, а порт B – с портом A.
- Порт M (Master) определен для концентраторов и соединяет два концентратора между собой или концентратор с абонентом при одном кольце. Порт M, как правило, соединяется с портом S.

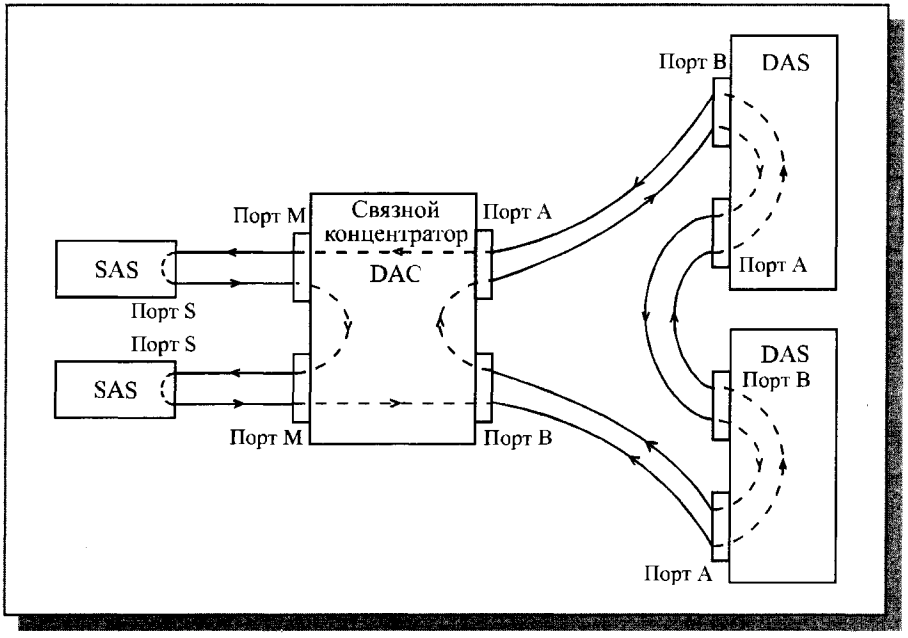



**Рис. 8.2.** Объединение устройств сети FDDI

- Порт S (Slave) определен только для устройств одинарного подключения (концентраторов и абонентов). Порт S обычно соединяется с портом M.

Структура портов для абонентов DAS и SAS, а также концентратора DAC видна на рис. 8.2. Концентратор SAC имеет один порт S для включения в одинарное кольцо и несколько портов M для подключения абонентов SAS.

Стандарт FDDI предусматривает также возможность реконфигурации сети с целью сохранения ее работоспособности в случае повреждения кабеля (рис. 8.3).

В показанном на рисунке случае поврежденный участок кабеля исключается из кольца, но целостность сети при этом не нарушается вследствие перехода на одно кольцо вместо двух (то есть абоненты DAS начинают работать, как абоненты SAS). Это равносильно процедуре сворачивания кольца в сети Token-Ring.

Кроме абонентов (станций) и концентраторов в сети FDDI применяются обходные коммутаторы (Bypass Switch). Обходные коммутаторы включаются между абонентом и кольцом и позволяют отключить абонента от кольца в случае его неисправности. Управляется обходной коммутатор электрическим сигналом от абонента. В зависимости от управляющего сигнала

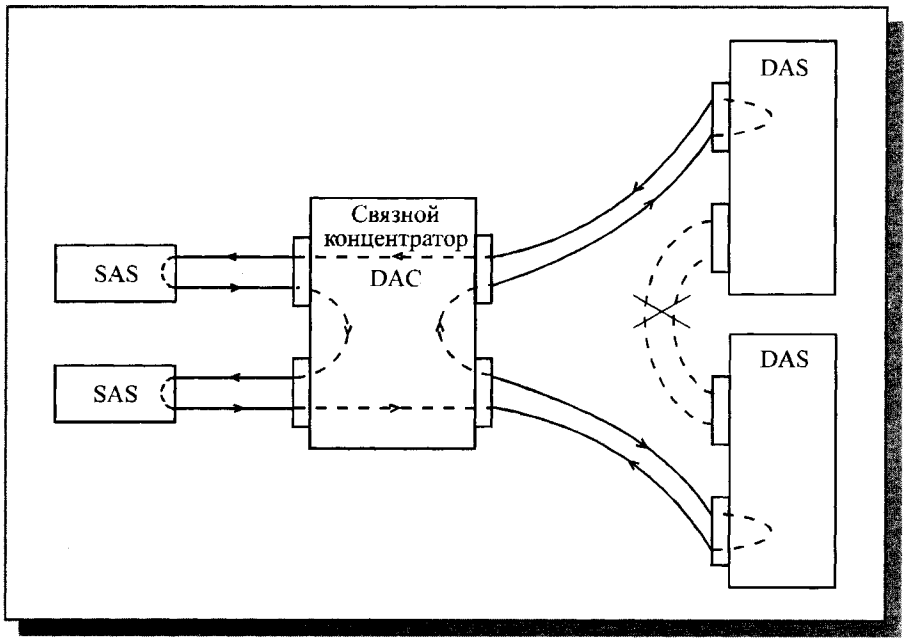



**Рис. 8.3.** Реконфигурация сети FDDI при повреждении кабеля

он или включает абонента в кольцо или же исключает его из кольца, замыкая его на самого себя (рис. 8.4).

При использовании обходных коммутаторов необходимо учитывать дополнительные затухания, вносимые ими (около 2,5 дБ на один коммутатор).

В отличие от метода доступа, предлагаемого стандартом IEEE 802.5, в FDDI применяется так называемая множественная передача маркера. Если в случае сети Token-Ring новый (свободный) маркер передается абонентом только после возвращения к нему его пакета, то в FDDI новый маркер передается абонентом сразу же после окончания передачи им пакета (подобно тому, как это делается при методе ETR в сети Token-Ring). Последовательность действий здесь следующая:

1. Абонент, желающий передавать, ждет маркера, который идет за каждым пакетом.
2. Когда маркер пришел, абонент удаляет его из сети и передает свой пакет. Таким образом, в сети может быть одновременно несколько пакетов, но только один маркер.
3. Сразу после передачи своего пакета абонент посылает новый маркер.
4. Абонент-получатель, которому адресован пакет, копирует его из сети и, сделав пометку в поле статуса пакета, отправляет его дальше по кольцу.

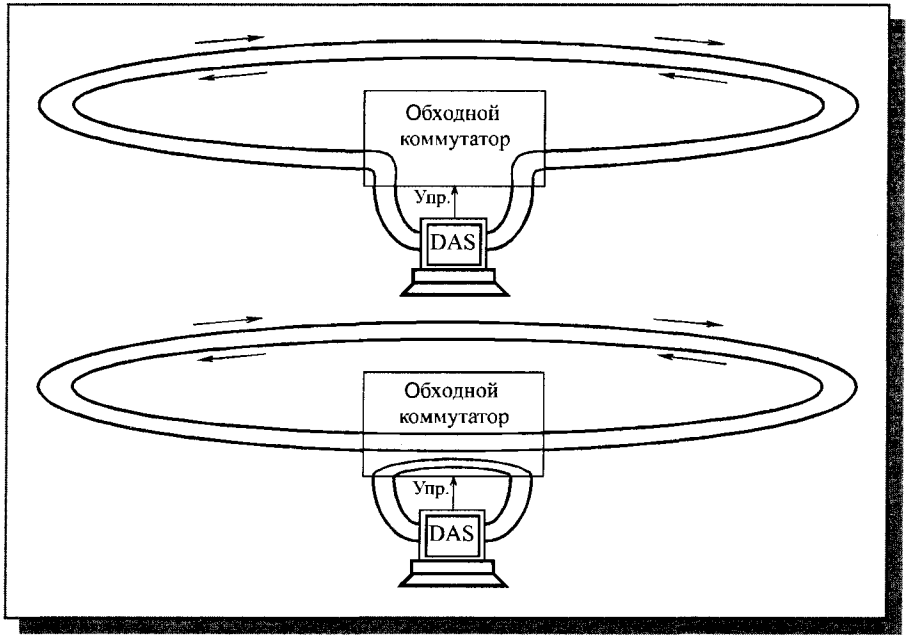



**Рис. 8.4.** Включение обходного коммутатора

5. Получив обратно по кольцу свой пакет, абонент уничтожает его. В поле статуса пакета он имеет информацию о том, были ли ошибки, и получил ли пакет приемник.

В сети FDDI не используется система приоритетов и резервирования, как в Token-Ring, но предусмотрен механизм адаптивного планирования нагрузки.

Каждый абонент ведет свой отсчет времени, сравнивая реальное время обращения маркера по кольцу (TRT – Token-Rotation Time) с заранее установленным контрольным (операционным) временем его прибытия (T_OPR).

Если маркер возвращается раньше, чем установлено T_OPR, то делается вывод о том, что сеть загружена мало, и, следовательно, абонент может передавать всю информацию в асинхронном режиме, то есть независимо от других. Для этого абонент может использовать весь оставшийся временной интервал (T_OPR –TRT).

Если же маркер возвращается позже, чем установлено T_OPR, то сеть загружена сильно, и абонент может передавать только самую важную информацию в течение того интервала времени, который отводится ему в синхронном режиме.

Величина T_OPR выбирается на этапе инициализации сети всеми абонентами в процессе состязания.

Такой механизм позволяет абонентам гибко реагировать на загрузку сети и автоматически поддерживать ее на оптимальном уровне.

Для правильной работы сети задержка прохождения сигнала по кольцу должна быть ограничена. Так, в случае максимальной длины кольца 200 км и максимальном количестве абонентов 1000 полное время задержки не должно превышать 1,617 мс.

Форматы маркера (рис. 8.5) и пакета (рис. 8.6) сети FDDI несколько отличаются от форматов, используемых в сети Token-Ring. Назначение полей:

- Преамбула (Preamble) используется для синхронизации. Первоначально она содержит 64 бита, но абоненты, через которых проходит пакет, могут менять ее размер.
- Начальный разделитель (SD — Start Delimiter) выполняет функцию признака начала кадра.
- Байт управления (FC – Frame Control) содержит информацию о пакете (размер поля адреса, синхронная/асинхронная передача, тип пакета – служебный или информационный, код команды).
- Адреса приемника и источника (SA – Source Address и DA – Destination Address) могут быть 6-байтовыми (аналогично Ethernet и Token-Ring) или 2-байтовыми.

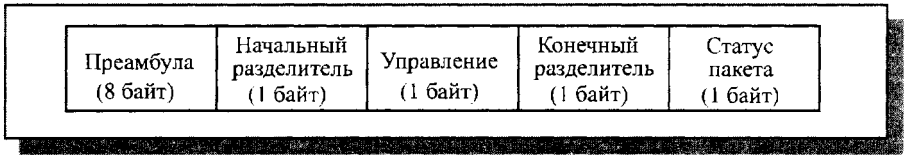



**Рис. 8.5.** Формат маркера FDDI

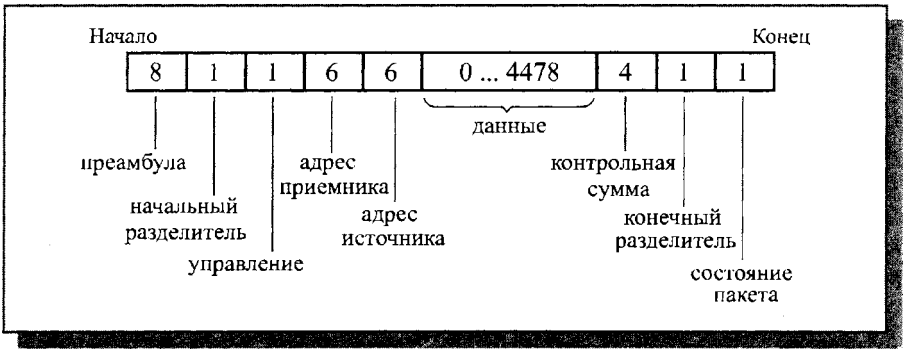



**Рис. 8.6.** Формат пакета FDDI

- Поле данных (Info) имеет переменную длину (от 0 до 4478 байт). В служебных (командных) пакетах поле данных обладает нулевой длиной.
- Поле контрольной суммы (FCS – Frame Check Sequence) содержит 32-битную циклическую контрольную сумму пакета (CRC).
- Конечный разделитель (ED – End Delimiter) определяет конец кадра.
- Байт состояния пакета (FS – Frame Status) включает в себя бит обнаружения ошибки, бит распознавания адреса и бит копирования (аналогично Token-Ring).

Формат байта управления сети FDDI (рис. 8.7):

- Бит класса пакета определяет тип пакета: синхронный или асинхронный.
- Бит длины адреса устанавливает, какой адрес (6-байтовый или 2-байтовый) используется в данном пакете.
- Поле типа пакета (два бита) определяет, управляющий это пакет или информационный.
- Поле кода команды (четыре бита) указывает на то, какую команду должен выполнить приемник (если это управляющий пакет).

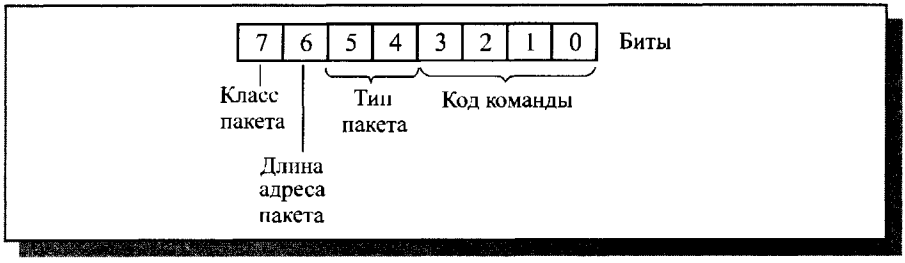



**Рис. 8.7.** Формат байта управления

В заключение следует отметить, что несмотря на очевидные преимущества FDDI данная сеть не получила широкого распространения, что связано главным образом с высокой стоимостью ее аппаратуры (порядка нескольких сот и даже тысяч долларов). Основная область применения FDDI сейчас – это базовые, опорные (Backbone) сети, объединяющие несколько сетей. Применяется FDDI также для соединения мощных рабочих станций или серверов, требующих высокоскоростного обмена. Предполагается, что сеть Fast Ethernet может потеснить FDDI, однако преимущества оптоволоконного кабеля, маркерного метода управления и рекордный допустимый размер сети ставят в настоящее время FDDI вне конкуренции. А в тех случаях, когда стоимость аппаратуры имеет решающее значение, можно на некритичных участках применять версию FDDI на основе витой пары (TPDDI). К тому же стоимость аппаратуры FDDI может сильно уменьшиться с ростом объема ее выпуска.

# Сеть 100VG-AnyLAN

Сеть 100VG-AnyLAN – это одна из последних разработок высокоскоростных локальных сетей, недавно появившаяся на рынке. Она разработана компаниями Hewlett-Packard и IBM и соответствует международному стандарту IEEE 802.12, так что уровень ее стандартизации достаточно высокий.

Главными достоинствами ее являются большая скорость обмена, сравнительно невысокая стоимость аппаратуры (примерно вдвое дороже оборудования наиболее популярной сети Ethernet 10BASE-T), централизованный метод управления обменом без конфликтов, а также совместимость на уровне форматов пакетов с сетями Ethernet и Token-Ring.

В названии сети 100VG-AnyLAN цифра 100 соответствует скорости 100 Мбит/с, буквы VG обозначают дешевую неэкранированную витую пару категории 3 (Voice Grade), а AnyLAN (любая сеть) обозначает то, что сеть совместима с двумя самыми распространенными сетями.

Основные технические характеристики сети 100VG-AnyLAN:

- Скорость передачи – 100 Мбит/с.
- Топология – звезда с возможностью наращивания (дерево). Количество уровней каскадирования концентраторов (хабов) – до 5.
- Метод доступа – централизованный, бесконфликтный (Demand Priority – с запросом приоритета).
- Среда передачи – счетверенная неэкранированная витая пара (кабели UTP категории 3, 4 или 5), сдвоенная витая пара (кабель UTP категории 5), сдвоенная экранированная витая пара (STP), а также оптоволоконный кабель. Сейчас в основном распространена счетверенная витая пара.
- Максимальная длина кабеля между концентратором и абонентом и между концентраторами – 100 метров (для UTP кабеля категории 3), 200 метров (для UTP кабеля категории 5 и экранированного кабеля), 2 километра (для оптоволоконного кабеля). Максимально возможный размер сети – 2 километра (определяется допустимыми задержками).
- Максимальное количество абонентов – 1024, рекомендуемое – до 250.

Таким образом, параметры сети 100VG-AnyLAN довольно близки к параметрам сети Fast Ethernet. Однако главное преимущество Fast Ethernet – это полная совместимость с наиболее распространенной сетью Ethernet (в случае 100VG-AnyLAN для этого требуется мост). В то же время, централизованное управление 100VG-AnyLAN, исключающее конфликты и гарантирующее предельную величину времени доступа (чего не предусмотрено в сети Ethernet), также нельзя сбрасывать со счетов.

Пример структуры сети 100VG-AnyLAN показан на рис. 8.8.

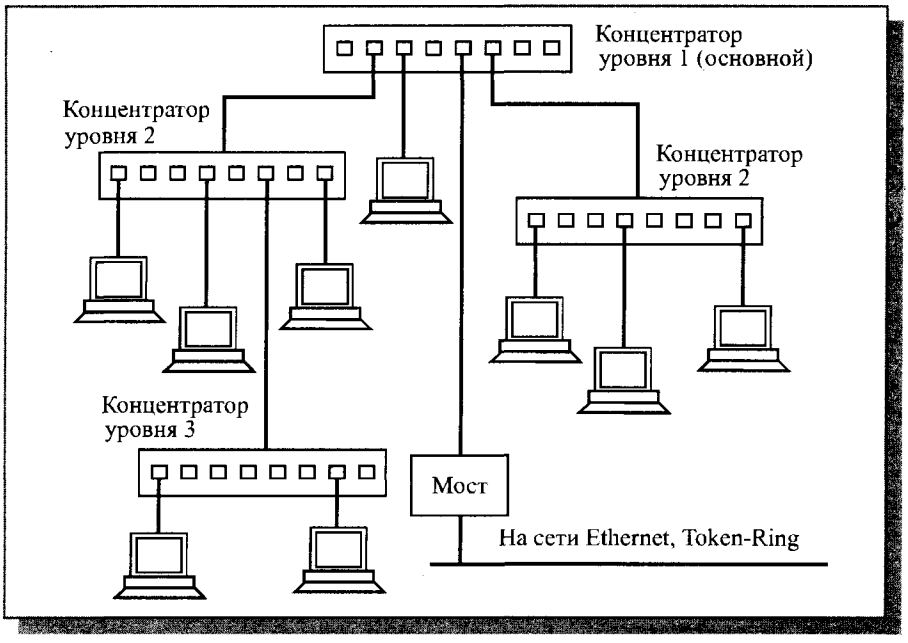



**Рис. 8.8.** Структура сети 100VG-AnyLAN

Сеть 100VG-AnyLAN состоит из центрального (основного, корневого) концентратора уровня 1, к которому могут подключаться как отдельные абоненты, так и концентраторы уровня 2, к которым в свою очередь подключаются абоненты и концентраторы уровня 3 и т.д. При этом сеть может иметь не более пяти таких уровней (в первоначальном варианте было не более трех). Максимальный размер сети может составлять 1000 метров для неэкранированной витой пары.

В отличие от неинтеллектуальных концентраторов других сетей (например, Ethernet, Token-Ring, FDDI), концентраторы сети 100VG-AnyLAN – это интеллектуальные контроллеры, которые управляют доступом к сети. Для этого они непрерывно контролируют запросы, поступающие на все порты. Концентраторы принимают приходящие пакеты и отправляют их только тем абонентам, которым они адресованы. Однако никакой обработки информации они не производят, то есть в данном случае получается все-таки не активная, но и не пассивная звезда. Полноценными абонентами концентраторы назвать нельзя.

Каждый из концентраторов может быть настроен на работу с форматами пакетов Ethernet или Token-Ring. При этом концентраторы всей сети должны работать с пакетами только какого-нибудь одного формата.

Для связи с сетями Ethernet и Token-Ring необходимы мосты, но мосты довольно простые.

Концентраторы имеют один порт верхнего уровня (для присоединения его к концентратору более высокого уровня) и несколько портов нижнего уровня (для присоединения абонентов). В качестве абонента может выступать компьютер (рабочая станция), сервер, мост, маршрутизатор, коммутатор. К порту нижнего уровня может также присоединяться другой концентратор.

Каждый порт концентратора может быть установлен в один из двух возможных режимов работы:

- Нормальный режим предполагает пересылку абоненту, присоединенному к порту, только пакетов, адресованных лично ему.
- Мониторный режим предполагает пересылку абоненту, присоединенному к порту, всех пакетов, приходящих на концентратор. Этот режим позволяет одному из абонентов контролировать работу всей сети в целом (выполнять функцию мониторинга).

Метод доступа к сети 100VG-AnyLAN типичен для сетей с топологией «звезда» и состоит в следующем.

Каждый желающий передавать абонент посылает концентратору свой запрос на передачу. Концентратор циклически прослушивает всех абонентов по очереди и дает право передачи абоненту, следующему по порядку за тем, который закончил передачу. Величина времени доступа гарантирована. Приоритет у абонентов – географический, то есть определяется номером порта нижнего уровня, к которому подключен абонент. Однако этот простейший алгоритм усложнен в сети 100VG-AnyLAN, так как запросы на передачу могут иметь два уровня приоритета:

- нормальный уровень приоритета, используетмый для обычных приложений;
- высокий уровень приоритета, используемый для приложений, требующих быстрого обслуживания.

Запросы с высоким уровнем приоритета (высокоприоритетные) обслуживаются раньше, чем запросы с нормальным приоритетом (низкоприоритетные). Если приходит запрос высокого приоритета, то нормальный порядок обслуживания прерывается, и после окончания приема текущего пакета обслуживается запрос высокого приоритета. Если таких высокоприоритетных запросов несколько, то возврат к нормальной процедуре обслуживания происходит только после полной обработки всех этих запросов. Можно сказать, что высокоприоритетные запросы обслуживаются вне очереди, но они также образуют свою очередь.

При этом концентратор следит за тем, чтобы не была превышена установленная величина гарантированного времени доступа для низкоприоритетных запросов. Если высокоприоритетных запросов слишком мно-

го, то запросы с нормальным приоритетом автоматически переводятся им в ранг высокоприоритетных. Типичная величина времени повышения приоритета равна 200–300 мс (устанавливается при конфигурировании сети). Таким образом, даже низкоприоритетные запросы не будут ждать своей очереди слишком долго.

Концентраторы более низких уровней также анализируют запросы абонентов, присоединенных к ним, и в случае необходимости пересылают их запросы концентратору более высокого уровня. За один раз концентратор более низкого уровня может передать концентратору более высокого уровня не один пакет (как обычный абонент), а столько пакетов, сколько абонентов присоединено к нему.

Так, для примера на рис. 8.9 в случае одновременного возникновения заявок на передачу у всех абонентов (компьютеров) порядок обслуживания будет такой: компьютер 1-2, затем 1-3, потом 2-1, 2-4, 2-8, и далее 1-6. Однако так будет только при одинаковом (нормальном) приоритете всех запросов. Если же, например, от компьютеров 1-2, 2-4 и 2-8 поступят высокоприоритетные запросы, то порядок обслуживания будет таким: 1-2, 2-4, 2-8, 1-3, 2-1, 1-6.

Каждый концентратор содержит во внутренней памяти таблицу MAC-адресов всех абонентов, подключенных к его портам нижнего уровня. Это позволяет ему перенаправлять полученные пакеты именно тем

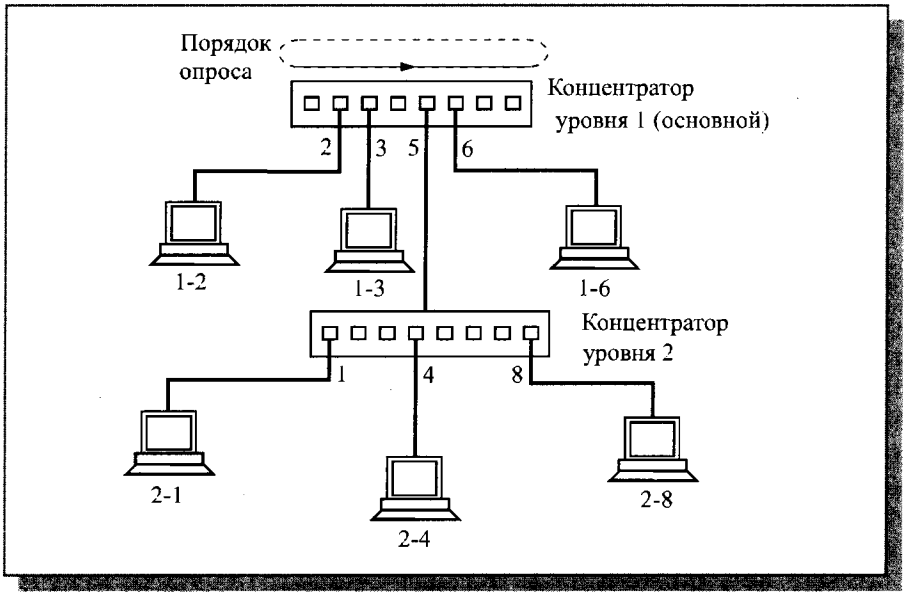



**Рис. 8.9.** Порядок обслуживания запросов абонентов на различных уровнях сети

абонентам, которым они адресованы. Концентраторы верхних уровней хранят таблицы адресов и тех абонентов, которые подключены к концентраторам более низких уровней. Таким образом, основной (корневой) концентратор содержит в себе информацию о всех абонентах сети. Таблица адресов формируется на этапе инициализации сети.

Помимо собственно передачи пакетов и пересылки запросов на передачу в сети применяется также специальная процедура подготовки к связи (Link Training), во время которой концентратор и абоненты обмениваются между собой управляющими пакетами специального формата. При этом проверяется правильность присоединения линий связи и их исправность, а также уровень ошибок: если 24 пакета подряд не проходят без ошибок, то абонент не включается в работу. Одновременно концентратор получает информацию об особенностях абонентов, подключенных к нему, их назначении и сетевых адресах, которые он заносит в таблицу. Запускается данная процедура абонентом при включении питания или после подключения к концентратору, а также автоматически при большом уровне ошибок.

Интересно решена в сети 100VG-AnyLAN проблема кодирования передаваемых данных.

Вся передаваемая информация проходит следующие этапы обработки:

- Разделение на квинтеты (группы по 5 бит).
- Перемешивание, скремблирование (scrambling) полученных квинтетов.
- Кодирование квинтетов специальным кодом 5B/6B (этот код обеспечивает в выходной последовательности не более трех единиц или нулей подряд, что используется для детектирования ошибок).
- Добавление начального и конечного разделителей кадра.

Сформированные таким образом кадры передаются в 4 линии передачи (при использовании счетверенной витой пары). При сдвоенной витой паре и оптоволоконном кабеле применяется временное мультиплексирование информации в каналах.

В результате всех этих действий достигается рандомизация сигналов, то есть выравнивание количества передаваемых единиц и нулей, снижение взаимовлияния кабелей друг на друга и самосинхронизация передаваемых сигналов без удвоения требуемой полосы пропускания, как в случае манчестерского кода.

При использовании счетверенной витой пары передача по каждой из четырех витых пар производится со скоростью 30 Мбит/с (рис. 8.10). Суммарная скорость передачи составляет 120 Мбит/с. Однако полезная информация вследствие использования кода 5B/6B передается всего лишь со скоростью 100 Мбит/с. Таким образом, пропускная способность кабеля должна быть не менее 15 МГц. Этому требованию удовлетворяет кабель с витыми парами категории 3 (полоса пропускания – 16 МГц).

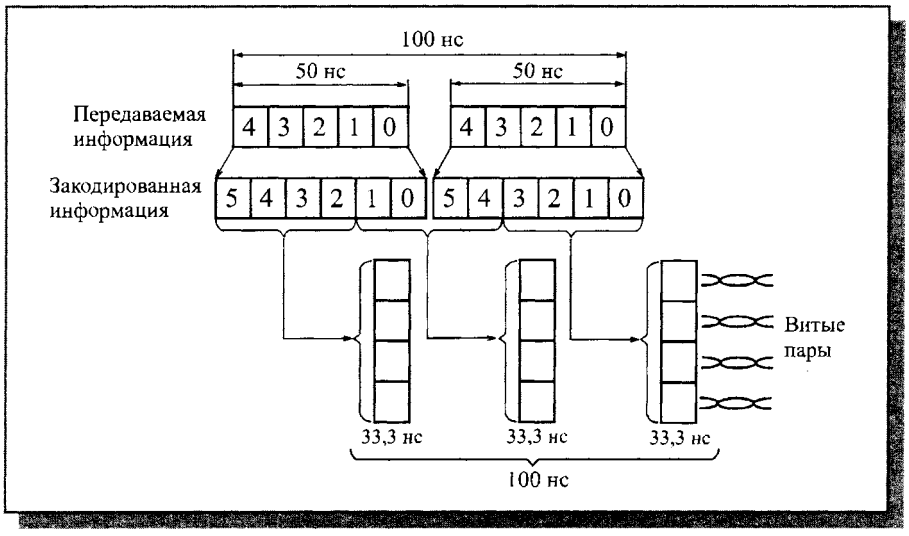



**Рис. 8.10.** Кодирование информации в сети 100VG-AnyLAN

В сети 100VG-AnyLAN предусмотрены два режима обмена: полудуплексный и полнодуплексный.

При полудуплексном обмене все четыре витые пары используются для передачи одновременно в одном направлении (от абонента к концентратору или наоборот). Данный режим используется для передачи пакетов.

При полнодуплексном обмене две витые пары (1 и 4) передают в одном направлении, а две другие (2 и 3) – в другом направлении. Этот режим используется для передачи управляющих сигналов.

Для управления используются два тональных сигнала. Первый из них представляет собой последовательность из 16 логических единиц и 16 логических нулей, следующих со скоростью 30 Мбит/с (в результате частота сигнала равна 0,9375 МГц). Второй тональный сигнал имеет вдвое большую частоту (1,875 МГц) и образуется чередованием восьми логических единиц и восьми логических нулей. Все управление сетью осуществляется комбинациями этих двух тональных сигналов.

В таблице 8.2 приведена расшифровка различных комбинаций этих сигналов, передаваемых абоненту и концентратору.

Когда ни у абонента, ни у концентратора нет информации для передачи, оба они посылают по обеим линиям первый тоновый сигнал (комбинация 1—1). Если принимаемый концентратором пакет может быть адресован данному абоненту, ему посылается комбинация сигналов 1—2. При этом абонент должен прекратить передачу управляющих сигналов концентратору и освободить эти две линии связи для пересылки информаци-

**Таблица 8.2.** Расшифровка комбинаций управляющих тональных сигналов

| Передаваемые сигналы | Расшифровка абонентом | Расшифровка концентратором |
|---|---|---|
| 1 – 1 | Нет информации для передачи | Нет информации для передачи |
| 1 – 2 | Концентратор принимает пакет | Запрос нормального приоритета |
| 2 – 1 | Зарезервировано | Высокоприоритетный запрос |
| 2 – 2 | Запрос процедуры подготовки к связи | Запрос процедуры подготовки к связи |

онных пакетов. Такая же комбинация (1—2), полученная концентратором, означает запрос на передачу пакета с нормальным приоритетом. Запрос на передачу пакета с высоким приоритетом передается комбинацией 2—1. Наконец, комбинация 2—2 сообщает как абоненту, так и концентратору о необходимости перейти к процедуре подготовки к связи (Link Training).

Таким образом, сеть 100VG-AnyLAN представляет собой доступное решение для увеличения скорости передачи до 100 Мбит/с. Однако она не обладает полной совместимостью ни с одной из стандартных сетей, поэтому ее дальнейшая судьба проблематична. К тому же, в отличие от сети FDDI, она не имеет никаких рекордных параметров. Скорее всего, 100VG-AnyLAN несмотря на поддержку солидных фирм и высокий уровень стандартизации останется всего лишь примером интересных технических решений.

Если говорить о наиболее распространенной 100-мегабитной сети Fast Ethernet, то 100VG-AnyLAN обеспечивает вдвое большую длину кабеля UTP категории 5 (до 200 метров), а также бесконфликтный метод управления обменом.

## Сверхвысокоскоростные сети

Быстродействие сети Fast Ethernet и других сетей, работающих на скорости в 100 Мбит/с, в настоящее время удовлетворяет требованиям большинства задач, но в ряде случаев даже его оказывается недостаточно. Особенно в тех ситуациях, когда необходимо подключать к сети современные высокопроизводительные серверы или строить сети с большим количеством абонентов, требующих высокой интенсивности обмена. Например, все более широко применяется сетевая обработка трехмерных

динамических изображений. Скорость компьютеров непрерывно растет, они обеспечивают все более высокие темпы обмена с внешними устройствами. В результате сеть может оказаться наиболее слабым местом системы, и ее пропускная способность будет основным сдерживающим фактором в увеличении быстродействия.

Работы по достижению скорости передачи в 1 Гбит/с (1000 Мбит/с) в последние годы ведутся довольно интенсивно несколькими компаниями. Однако, скорее всего, наиболее перспективной окажется сеть Gigabit Ethernet. Это связано, прежде всего, с тем, что переход на нее окажется наиболее безболезненным, самым дешевым и психологически приемлемым. Ведь сеть Ethernet и ее версия Fast Ethernet сегодня далеко опережают всех своих конкурентов по объему продаж и распространенности в мире.

Сеть Gigabit Ethernet – это естественный, эволюционный путь развития концепции, заложенной в стандартной сети Ethernet. Безусловно, она наследует и все недостатки своих прямых предшественников, например, негарантированное время доступа к сети. Однако огромная пропускная способность приводит к тому, что загрузить сеть до тех уровней, когда этот фактор становится определяющим, довольно трудно. Зато сохранение преемственности позволяет достаточно просто соединять сегменты Ethernet, Fast Ethernet и Gigabit Ethernet в сеть, и, самое главное, переходить к новым скоростям постепенно, вводя гигабитные сегменты только на самых напряженных участках сети (к тому же далеко не везде такая высокая пропускная способность действительно необходима). Если же говорить о конкурирующих гигабитных сетях, то их применение может потребовать полной замены сетевой аппаратуры, что сразу же приведет к большим затратам средств.

В сети Gigabit Ethernet сохраняется все тот же хорошо зарекомендовавший себя в предыдущих версиях метод доступа CSMA/CD, используются те же форматы пакетов (кадров) и те же их размеры. Не требуется никакого преобразования протоколов в местах соединения с сегментами Ethernet и Fast Ethernet. Единственно, что нужно, – это согласование скоростей обмена, поэтому главной областью применения Gigabit Ethernet станет в первую очередь соединение концентраторов Ethernet и Fast Ethernet между собой.

С появлением сверхбыстродействующих серверов и распространением наиболее совершенных персональных компьютеров класса «hi-end» преимущества Gigabit Ethernet становятся все более явными. Так, 64-разрядная системная магистраль PCI, уже фактический стандарт, вполне достигает требуемой для такой сети скорости передачи данных.

Работы по созданию сети Gigabit Ethernet ведутся с 1995 года. В 1998 году принят стандарт, получивший наименование IEEE 802.3z (1000BASE-SX, 1000BASE-LX и 1000BASE-CX). Разработкой занимается специально

созданный альянс (Gigabit Ethernet Alliance), в который, в частности, входит такая известная компания, занимающаяся сетевой аппаратурой, как 3Com. В 1999 году принят стандарт IEEE 802.3ab (1000BASE-T).

Номенклатура сегментов сети Gigabit Ethernet в настоящее время включает в себя следующие типы:

- 1000BASE-SX – сегмент на мультимодовом оптоволоконном кабеле с длиной волны светового сигнала 850 нм (длиной до 500 метров). Используются лазерные передатчики.
- 1000BASE-LX – сегмент на мультимодовом (длиной до 500 метров) и одномодовом (длиной до 2000 метров) оптоволоконном кабеле с длиной волны светового сигнала 1300 нм. Используются лазерные передатчики.
- 1000BASE-CX – сегмент на экранированной витой паре (длиной до 25 метров).
- 1000BASE-T (стандарт IEEE 802.3ab) – сегмент на счетверенной неэкранированной витой паре категории 5 (длиной до 100 метров). Используется 5-уровневое кодирование (PAM-5), причем в полнодуплексном режиме передача ведется по каждой паре в двух направлениях.

Специально для сети Gigabit Ethernet предложен метод кодирования передаваемой информации 8B/10B, построенный по тому же принципу, что и код 4B/5B сети FDDI (кроме 1000BASE-T). Таким образом, восьми битам информации, которую нужно передать, ставится в соответствие 10 бит, передаваемых по сети. Этот код позволяет сохранить самосинхронизацию, легко обнаруживать несущую (факт передачи), но не требует удвоения полосы пропускания, как в случае манчестерского кода.

Для увеличения 512-битного интервала сети Ethernet, соответствующего минимальной длине пакета (51,2 мкс в сети Ethernet и 5,12 мкс в сети Fast Ethernet), разработаны специальные методы. В частности, минимальная длина пакета увеличена до 512 байт (4096 бит). В противном случае временной интервал 0,512 мкс чрезмерно ограничивал бы предельную длину сети Gigabit Ethernet. Все пакеты с длиной меньше 512 байт расширяются до 512 байт. Поле расширения вставляется в пакет после поля контрольной суммы. Это требует дополнительной обработки пакетов, но зато максимально допустимый размер сети становится в 8 раз больше, чем без принятия таких мер.

Кроме того, в Gigabit Ethernet предусмотрена возможность блочного режима передачи пакетов (Frame Bursting). При этом абонент, получивший право передавать и имеющий для передачи несколько пакетов, может передать не один, а несколько пакетов, последовательно, причем адресованных разным абонентам-получателям. Дополнительные передаваемые пакеты могут быть только короткими, а суммарная длина всех пакетов блока не должна превышать 8192 байта. Такое решение позволяет

снизить количество захватов сети и уменьшить число коллизий. При использовании блочного режима до 512 байт расширяется только первый пакет блока — для того, чтобы проверить, нет ли в сети коллизий. Остальные пакеты до 512 байт могут не расширяться.

Передача в сети Gigabit Ethernet производится как в полудуплексном режиме (с сохранением метода доступа CSMA/CD), так и в более быстром полнодуплексном режиме (аналогично предшествующей сети Fast Ethernet). Ожидается, что полнодуплексный режим, не налагающий ограничений на длину сети (кроме ограничений в связи с затуханием сигнала в кабеле) и обеспечивающий отсутствие конфликтов, станет в будущем основным для Gigabit Ethernet. Подробнее о полнодуплексном режиме будет рассказано в главе 9.

Сеть Gigabit Ethernet, прежде всего, находит применение в сетях, объединяющих компьютеры крупных предприятий, которые располагаются в нескольких зданиях. Она позволяет с помощью соответствующих коммутаторов, преобразующих скорости передачи, обеспечить каналы связи с высокой пропускной способностью между отдельными частями сложной сети (рис. 8.11) или линии связи коммутаторов со сверхбыстродействующими серверами (рис. 8.12).

Вероятно, в ряде случаев Gigabit Ethernet будет вытеснять оптоволоконную сеть FDDI, которая в настоящее время все чаще используется для объединения в сеть нескольких локальных сетей, в том числе, и Ethernet.

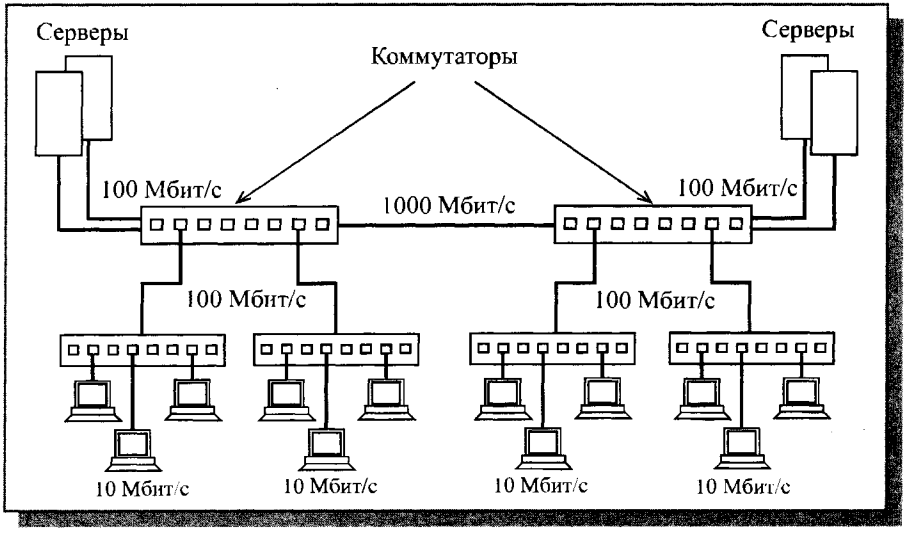



**Рис. 8.11.** Использование сети Gigabit Ethernet для соединения групп компьютеров

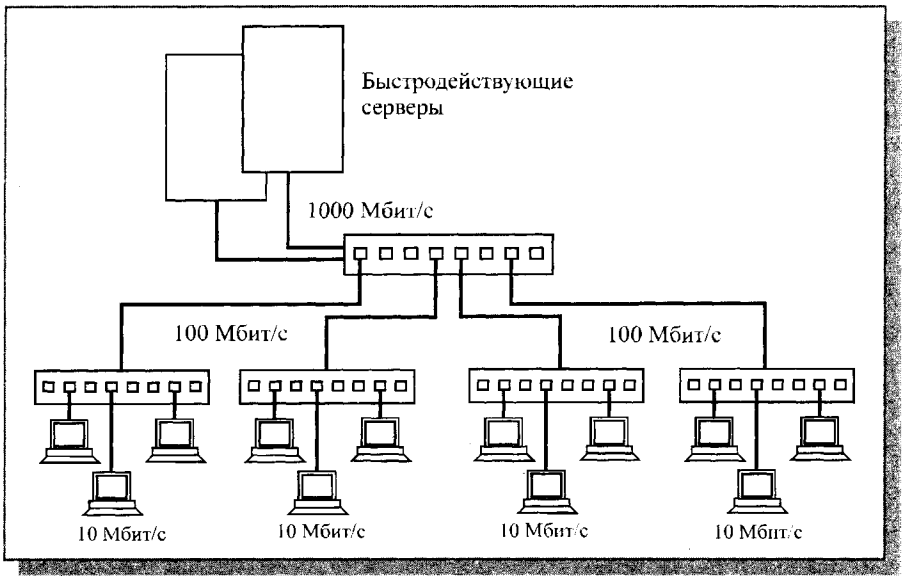



**Рис. 8.12.** Использование сети Gigabit Ethernet для подключения быстродействующих серверов

Правда, FDDI может связывать абонентов, находящихся гораздо дальше друг от друга, но по скорости передачи информации Gigabit Ethernet существенно превосходит FDDI.

Но даже сеть Gigabit Ethernet не может решить некоторых задач. Уже предлагается и 10-гигабитная версия Ethernet, называемая 10Gigabit Ethernet (стандарт IEEE 802.3ae, принятый в 2002 году). Она принципиально отличается от предыдущих версий. В качестве среды передачи используется исключительно оптоволоконный кабель. Электрический кабель может иногда применяться только для связи на короткие расстояния (порядка 10 метров). Режим обмена – полнодуплексный. Формат пакета Ethernet — прежний. Это, наверное, единственное, что остается от изначального стандарта Ethernet (IEEE 802.3).

В заключение раздела — несколько слов об альтернативном решении сверхбыстродействующей сети. Речь идет о сети с технологией ATM (Asynchronous Transfer Mode). Данная технология используется как в локальных, так и в глобальных сетях. Основная идея – передача цифровых, голосовых и мультимедийных данных по одним и тем же каналам. Строго говоря, жесткого стандарта на аппаратуру ATM не предполагает.

Первоначально была выбрана скорость передачи 155 Мбит/с (для настольных систем – 25 Мбит/с), затем – 662 Мбит/с, а сейчас ведутся работы по повышению скорости до 2488 Мбит/с. По скорости ATM успешно

конкурирует с Gigabit Ethernet. Кстати, появилась ATM раньше, чем Gigabit Ethernet.В качестве среды передачи информации в локальной сети технология ATM предполагает использование оптоволоконного кабеля и неэкранированной витой пары. Используемые коды – 4B/5B и 8B/10B.

Принципиальное отличие ATM от остальных сетей состоит в отказе от привычных пакетов с полями адресации, управления и данных. Вся передаваемая информация упакована в микропакеты (ячейки, cells) длиной 53 байта. Каждая ячейка имеет 5-байтовый заголовок, который позволяет интеллектуальным распределительным устройствам сортировать ячейки и следить за тем, чтобы они передавались в нужной последовательности. Каждая ячейка имеет 48 байт информации. Их минимальный размер позволяет осуществлять коррекцию ошибок и маршрутизацию на аппаратном уровне. Он же обеспечивает равномерность всех информационных потоков сети и минимальное время ожидания доступа к сети.

Заголовок включает в себя идентификаторы пути, канала доставки, типа информации, указатель приоритета доставки, а также контрольную сумму заголовка, позволяющую определить наличие ошибок передачи.

Главный недостаток сетей с технологией ATM состоит в их полной несовместимости ни с одной из имеющихся сетей. Плавный переход на ATM в принципе невозможен, нужно менять сразу все оборудование, а стоимость его пока что очень высока. Правда, работы по обеспечению совместимости ведутся, снижается и стоимость оборудования. Тем более что задач по передаче изображений по компьютерным сетям становится все больше и больше.

Технология ATM еще в недалеком прошлом считалась перспективной и универсальной, способной потеснить привычные локальные сети. Однако в настоящий момент вследствие успешного развития традиционных локальных сетей применение ATM ограничено только глобальными и магистральными сетями.

## Беспроводные сети

До недавнего времени беспроводная связь в локальных сетях практически не применялась. Однако с конца XX века наблюдается настоящий бум беспроводных локальных сетей (WLAN – Wireless LAN). Это связано в первую очередь с успехами технологии и с теми удобствами, которые способны предоставить беспроводные сети. По имеющимся прогнозам, число пользователей беспроводных сетей в 2005 году достигнет 44 миллионов, а 80% всех мобильных компьютеров будут оснащены встроенными средствами доступа к таким сетям.

В 1997 году был принят стандарт для беспроводных сетей IEEE 802.11. Сейчас этот стандарт активно развивается и включает в себя уже

несколько разделов, в том числе три локальные сети (802.11a, 802.11b и 802.11g). Стандарт содержит следующие спецификации:

- 802.11 – первоначальный стандарт WLAN. Поддерживает передачу данных со скоростями от 1 до 2 Мбит/с.
- 802.11a – высокоскоростной стандарт WLAN для частоты 5 ГГц. Поддерживает скорость передачи данных 54 Мбит/с.
- 802.11b – стандарт WLAN для частоты 2,4 ГГц. Поддерживает скорость передачи данных 11 Мбит/с.
- 802.11e – устанавливает требования качества запроса, необходимо для всех радио-интерфейсов IEEE WLAN.
- 802.11f – описывает порядок связи между равнозначными точками доступа.
- 802.11g – устанавливает дополнительную технику модуляции для частоты 2,4 ГГц. Предназначен для обеспечения скоростей передачи данных до 54 Мбит/с.
- v802.11h – описывает управление спектром частоты 5 ГГц для использования в Европе и Азии.
- 802.11i – исправляет существующие проблемы безопасности в областях аутентификации и протоколов шифрования.

Разработкой и поддержкой стандарта IEEE 802.11 занимается комитет Wi-Fi Alliance. Термин Wi-Fi (Wireless Fidelity) используется в качестве общего имени для стандартов 802.11a и 802.11b, а также всех последующих, относящихся к беспроводным локальным сетям (WLAN).

Оборудование беспроводных сетей включает в себя точки беспроводного доступа (Access Point) и беспроводные адаптеры для каждого абонента.

Точки доступа выполняют роль концентраторов, обеспечивающих связь между абонентами и между собой, а также функцию мостов, осуществляющих связь с кабельной локальной сетью и с Интернетом. Несколько близкорасположенных точек доступа образуют зону доступа Wi-Fi, в пределах которой все абоненты, снабженные беспроводными адаптерами, получают доступ к сети. Такие зоны доступа (Hotspot) создаются в местах массового скопления людей: в аэропортах, студенческих городках, библиотеках, магазинах, бизнес-центрах и т.д.

Каждая точка доступа может обслуживать несколько абонентов, но чем больше абонентов, тем меньше эффективная скорость передачи для каждого из них. Метод доступа к сети – CSMA/CA. Сеть строится по сотовому принципу. В сети предусмотрен механизм роуминга, то есть поддерживается автоматическое подключение к точке доступа и переключение между точками доступа при перемещении абонентов, хотя строгих правил роуминга стандарт не устанавливает.

Поскольку радиоканал не обеспечивает высокой степени защиты от прослушивания, в сети Wi-Fi используется специальный встроенный ме-

ханизм защиты информации. Он включает средства и процедуры аутентификации для противодействия несанкционированному доступу к сети и шифрование для предотвращения перехвата информации.

Стандарт **IEEE 802.11b** был принят в 1999 г. и благодаря ориентации на освоенный диапазон 2,4 ГГц завоевал наибольшую популярность у производителей оборудования. В качестве базовой радиотехнологии в нем используется метод DSSS (Direct Sequence Spread Spectrum), который отличается высокой устойчивостью к искажению данных, помехам, в том числе преднамеренным, а также к обнаружению. Поскольку оборудование 802.11b, работающее на максимальной скорости 11 Мбит/с, имеет меньший радиус действия, чем на более низких скоростях, то стандартом 802.11b предусмотрено автоматическое понижение скорости при ухудшении качества сигнала. Пропускная способность (теоретическая — 11 Мбит/с, реальная – от 1 до 6 Мбит/с) отвечает требованиям большинства приложений. Расстояния – до 300 метров, но обычно – до 160 метров.

Стандарт **IEEE 802.11a** рассчитан на работу в частотном диапазоне 5 ГГц. Скорость передачи данных до 54 Мбит/с, то есть примерно в пять раз быстрее сетей 802.11b. Это наиболее широкополосный из семейства стандартов 802.11. Определены три обязательные скорости – 6, 12 и 24 Мбит/с и пять необязательных – 9, 18, 36, 48 и 54 Мбит/с. В качестве метода модуляции сигнала принято ортогональное частотное мультиплексирование (OFDM). Его наиболее существенное отличие от методов DSSS заключается в том, что OFDM предполагает параллельную передачу полезного сигнала одновременно по нескольким частотам диапазона, в то время как технологии расширения спектра передают сигналы последовательно. В результате повышается пропускная способность канала и качество сигнала. К недостаткам 802.11a относятся большая потребляемая мощность радиопередатчиков для частот 5 ГГц, а также меньший радиус действия (около 100 м). Кроме того, устройства для 802.11a дороже, но со временем ценовой разрыв между продуктами 802.11b и 802.11a будет уменьшаться.

Стандарт **IEEE 802.11g** является новым стандартом, регламентирующим метод построения WLAN, функционирующих в нелицензируемом частотном диапазоне 2,4 ГГц. Благодаря применению технологии ортогонального частотного мультиплексирования (OFDM) максимальная скорость передачи данных в беспроводных сетях IEEE 802.11g составляет 54 Мбит/с. Оборудование, поддерживающее стандарт IEEE 802.11g, например точки доступа беспроводных сетей, обеспечивает одновременное подключение к сети беспроводных устройств стандартов IEEE 802.11g и IEEE 802.11b. Стандарт 802.11g представляет собой развитие 802.11b и обратно совместим с 802.11b. Теоретически 802.11g обладает достоинствами двух своих предшественников. В числе преимуществ 802.11g надо отме-

тить низкую потребляемую мощность, большие расстояния (до 300 м) и высокую проникающую способность сигнала.

Спецификация IEEE 802.11d устанавливает универсальные требования к физическому уровню (процедуры формирования каналов, псевдослучайные последовательности частот и т. д.). Стандарт 802.11d пока находится в стадии разработки.

Спецификация IEEE 802.11e позволит создавать мультисервисные беспроводные сети для корпораций и индивидуальных потребителей. При сохранении полной совместимости с действующими стандартами 802.11a и b она расширит их функциональность за счет обслуживания потоковых мультимедиа-данных и гарантированного качества услуг. Пока утвержден предварительный вариант спецификаций 802.11e.

Спецификация IEEE 802.11f описывает протокол обмена служебной информацией между точками доступа (Inter-Access Point Protocol, IAPP), что необходимо для построения распределенных беспроводных сетей передачи данных. Находится в стадии разработки.

Спецификация IEEE 802.11h предусматривает возможность дополнения действующих алгоритмами эффективного выбора частот для офисных и уличных беспроводных сетей, а также средствами управления использованием спектра, контроля излучаемой мощности и генерации соответствующих отчетов. Находится в стадии разработки.

Среди изготовителей Wi-Fi оборудования — такие известные компании, как Cisco Systems, Intel, Texas Instruments и Proxim.

Таким образом, беспроводные сети весьма перспективны. Несмотря на свои недостатки, главный из которых – незащищенность среды передачи, они обеспечивают простое подключение абонентов, не требующее кабелей, а также мобильность, гибкость и масштабируемость сети. К тому же, что немаловажно, от пользователей не требуется знания сетевых технологий.

# Глава 6. Защита информации в локальных сетях

## Лекция 9. Защита информации в локальных сетях

**В этой лекции рассматриваются классификация угроз, методов и средств защиты информации, определения основных понятий в области криптографии, классические методы шифрования и стандартные криптографические системы, а также программные средства защиты информации (встроенные в ОС и внешние).**

**Ключевые слова:** защита информации, каналы утечки информации, криптография, симметричное и несимметричное шифрование.

Судя по растущему количеству публикаций и компаний, профессионально занимающихся защитой информации в компьютерных системах, решению этой задачи придается большое значение. Одной из наиболее очевидных причин нарушения системы защиты является умышленный несанкционированный доступ (НСД) к конфиденциальной информации со стороны нелегальных пользователей и последующие нежелательные манипуляции с этой информацией. Защита информации – это комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации и т.п. Поскольку утрата информации может происходить по сугубо техническим, объективным и неумышленным причинам, под это определение подпадают также и мероприятия, связанные с повышением надежности сервера из-за отказов или сбоев в работе винчестеров, недостатков в используемом программном обеспечении и т.д.

Следует заметить, что наряду с термином «защита информации» (применительно к компьютерным сетям) широко используется, как правило, в близком значении, термин «компьютерная безопасность».

Переход от работы на персональных компьютерах к работе в сети усложняет защиту информации по следующим причинам:

1. Большое число пользователей в сети и их переменный состав. Защита на уровне имени и пароля пользователя недостаточна для предотвращения входа в сеть посторонних лиц.
2. Значительная протяженность сети и наличие многих потенциальных каналов проникновения в сеть.
3. Уже отмеченные недостатки в аппаратном и программном обеспечении, которые зачастую обнаруживаются не на предпродажном этапе, называемом бета-тестированием, а в процессе эксплуатации. В том

числе неидеальны встроенные средства защиты информации даже в таких известных и «мощных» сетевых ОС, как Windows NT или NetWare.

Остроту проблемы, связанной с большой протяженностью сети для одного из ее сегментов на коаксиальном кабеле, иллюстрирует рис. 9.1. В сети имеется много физических мест и каналов несанкционированного доступа к информации в сети. Каждое устройство в сети является потенциальным источником электромагнитного излучения из-за того, что соответствующие поля, особенно на высоких частотах, экранированы не идеально. Система заземления вместе с кабельной системой и сетью электропитания может служить каналом доступа к информации в сети, в том числе на участках, находящихся вне зоны контролируемого доступа и потому особенно уязвимых. Кроме электромагнитного излучения, потенциальную угрозу представляет бесконтактное электромагнитное воздействие на кабельную систему. Безусловно, в случае использования проводных соединений типа коаксиальных кабелей или витых пар, называемых часто медными кабелями, возможно и непосредственное физическое подключение к кабельной системе. Если пароли для входа в сеть стали известны или подобраны, становится возможным несанкционированный вход в сеть с файл-сервера или с одной из рабочих станций. Наконец, возможна утечка информации по каналам, находящимся вне сети:

- хранилище носителей информации,
- элементы строительных конструкций и окна помещений, которые образуют каналы утечки конфиденциальной информации за счет так называемого микрофонного эффекта,
- телефонные, радио-, а также иные проводные и беспроводные каналы (в том числе каналы мобильной связи).

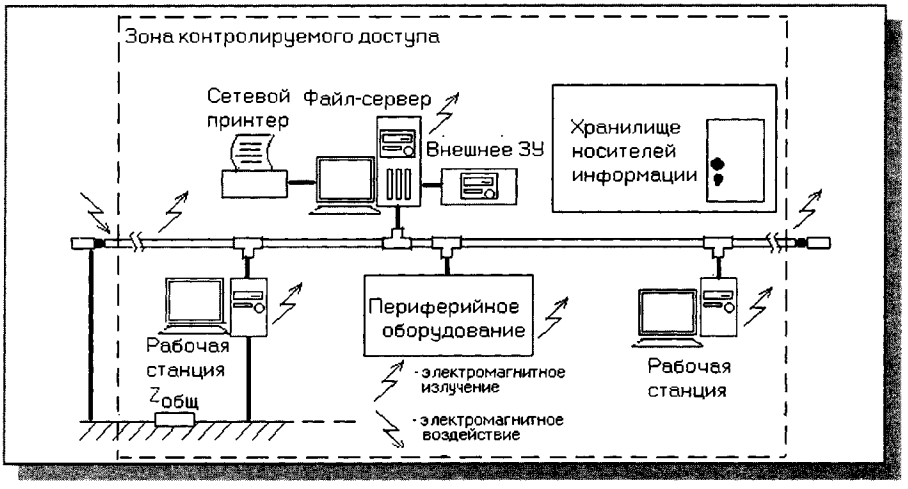



**Рис. 9.1.** Места и каналы возможного несанкционированного доступа к информации в компьютерной сети

Любые дополнительные соединения с другими сегментами или подключение к Интернету порождают новые проблемы. Атаки на локальную сеть через подключение к Интернету для того, чтобы получить доступ к конфиденциальной информации, в последнее время получили широкое распространение, что связано с недостатками встроенной системы защиты информации в протоколах TCP/IP. *Сетевые атаки* через Интернет могут быть классифицированы следующим образом:

- Сниффер пакетов (sniffer – в данном случае в значении *фильтрация*) – прикладная программа, которая использует сетевую карту, работающую в режиме promiscuous (не делающий различия) mode (в этом режиме все пакеты, полученные по физическим каналам, сетевой адаптер отправляет приложению для обработки).
- IP-спуфинг (spoof – обман, мистификация) – происходит, когда хакер, находящийся внутри корпорации или вне ее, выдает себя за санкционированного пользователя.
- Отказ в обслуживании (Denial of Service – DoS). Атака DoS делает сеть недоступной для обычного использования за счет превышения допустимых пределов функционирования сети, операционной системы или приложения.
- Парольные атаки – попытка подбора пароля легального пользователя для входа в сеть.
- Атаки типа Man-in-the-Middle – непосредственный доступ к пакетам, передаваемым по сети.
- Атаки на уровне приложений.
- Сетевая разведка – сбор информации о сети с помощью общедоступных данных и приложений.
- Злоупотребление доверием внутри сети.
- Несанкционированный доступ (НСД), который не может считаться отдельным типом атаки, так как большинство сетевых атак проводятся ради получения несанкционированного доступа.
- Вирусы и приложения типа «троянский конь».

## Классификация средств защиты информации

Защита информации в сети на рис. 9.1 может быть улучшена за счет использования специальных генераторов шума, маскирующих побочные электромагнитные излучения и наводки, помехоподавляющих сетевых фильтров, устройств зашумления сети питания, скремблеров (шифраторов телефонных переговоров), подавителей работы сотовых телефонов и т.д. Кардинальным решением является переход к соединениям на основе оптоволокна, свободным от влияния электромагнитных полей и позволяющим обнаружить факт несанкционированного подключения.

В целом средства обеспечения защиты информации в части предотвращения преднамеренных действий в зависимости от способа реализации можно разделить на группы:

1. Технические (аппаратные) средства. Это различные по типу устройства (механические, электромеханические, электронные и др.), которые аппаратными средствами решают задачи защиты информации. Они либо препятствуют физическому проникновению (либо, если проникновение все же состоялось) доступу к информации, в том числе с помощью ее маскировки. Первую часть задачи решают замки, решетки на окнах, защитная сигнализация и др. Вторую – упоминавшиеся выше генераторы шума, сетевые фильтры, сканирующие радиоприемники и множество других устройств, «перекрывающих» потенциальные каналы утечки информации или позволяющих их обнаружить. Преимущества технических средств связаны с их надежностью, независимостью от субъективных факторов, высокой устойчивостью к модификации. Слабые стороны – недостаточная гибкость, относительно большие объем и масса, высокая стоимость.
2. Программные средства включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и др. Преимущества программных средств – универсальность, гибкость, надежность, простота установки, способность к модификации и развитию. Недостатки – ограниченная функциональность сети, использование части ресурсов файл-сервера и рабочих станций, высокая чувствительность к случайным или преднамеренным изменениям, возможная зависимость от типов компьютеров (их аппаратных средств).
4. Смешанные *аппаратно-программные* средства реализуют те же функции, что аппаратные и программные средства в отдельности, и имеют промежуточные свойства.
5. Организационные средства складываются из организационно-технических (подготовка помещений с компьютерами, прокладка кабельной системы с учетом требований ограничения доступа к ней и др.) и организационно-правовых (национальные законодательства и правила работы, устанавливаемые руководством конкретного предприятия). Преимущества организационных средств состоят в том, что они позволяют решать множество разнородных проблем, просты в реализации, быстро реагируют на нежелательные действия в сети, имеют неограниченные возможности модификации и развития. Недостатки – высокая зависимость от субъективных факторов, в том числе от общей организации работы в конкретном подразделении.

По степени распространения и доступности выделяются программные средства, поэтому далее они рассматриваются более подробно (см. «Стандартные методы шифрования и криптографические системы» и «Программные

средства защиты информации»). Другие средства применяются в тех случаях, когда требуется обеспечить дополнительный уровень защиты информации.

**Шифрование** данных представляет собой разновидность программных средств защиты информации и имеет особое значение на практике как единственная надежная защита информации, передаваемой по протяженным последовательным линиям, от утечки. Шифрование образует последний, практически непреодолимый «рубеж» защиты от НСД. Понятие «шифрование» часто употребляется в связи с более общим понятием криптографии. **Криптография** включает способы и средства обеспечения конфиденциальности информации (в том числе с помощью шифрования) и аутентификации. **Конфиденциальность** – защищенность информации от ознакомления с ее содержанием со стороны лиц, не имеющих права доступа к ней. В свою очередь **аутентификация** представляет собой установление подлинности различных аспектов информационного взаимодействия: сеанса связи, сторон (идентификация), содержания (имитозащита) и источника (установление авторства с помощью цифровой подписи).

Число используемых программ шифрования ограничено, причем некоторые из них являются стандартами де-факто или де-юре. Однако даже если алгоритм шифрования не представляет собой секрета, произвести дешифрование (расшифрование) без знания закрытого ключа чрезвычайно сложно. Это свойство в современных программах шифрования обеспечивается в процессе многоступенчатого преобразования исходной открытой информации (plain text в англоязычной литературе) с использованием ключа (или двух ключей – по одному для шифрования и дешифрования). В конечном счете, любой сложный метод (алгоритм) шифрования представляет собой комбинацию относительно простых методов.

## Классические алгоритмы шифрования данных

Имеются следующие «классические» методы шифрования:

- подстановка (простая – одноалфавитная, многоалфавитная однопетлевая, многоалфавитная многопетлевая);
- перестановка (простая, усложненная);
- гаммирование (смешивание с короткой, длинной или неограниченной маской).

Устойчивость каждого из перечисленных методов к дешифрованию без знания ключа характеризуется количественно с помощью показателя Sk, представляющего собой минимальный объем зашифрованного текста, который может быть дешифрован посредством статистического анализа.

Подстановка предполагает использование альтернативного алфавита (или нескольких) вместо исходного. В случае простой подстановки для символов английского алфавита можно предложить, например, следующую замену (см. табл. 9.1).

**Таблица 9.1.** Пример замены символов при подстановке

| Исходный алфавит | A | B | C | D | E | F | G | H | I | J | K | L | ... | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Альтернативный алфавит | S | O | U | H | K | T | L | X | N | W | M | Y | ... | A | P | J |

Тогда слово «cache» в зашифрованном виде представляется как «usuxk».

Существует, однако, возможность дешифрования сообщения с помощью известной статистической частоты повторяемости символов в произвольном, достаточно длинном тексте. Символ E встречается чаще всего – в среднем 123 раза на каждые 1000 символов или в 12,3% случаев, далее следуют символы T – 9,6%, A – 8,1%, O – 7,9%, N – 7,2%, I – 7,2%, S – 6,6%, R – 6,0%, H – 5,1%, L – 4,0% и т.д. Приведенные цифры могут, конечно, несколько варьироваться в зависимости от источника информации, из которого они были взяты, что не изменяет принципиально ситуации. Показатель устойчивости к дешифрованию Sk не превышает 20...30. При многоалфавитной подстановке можно добиться того, что в зашифрованном тексте все символы будут встречаться примерно с одинаковой частотой, что существенно затруднит дешифрование без знания альтернативных алфавитов и порядка, в котором они использовались при шифровании.

**Перестановка** потенциально обеспечивает большую по сравнению с подстановкой устойчивость к дешифрованию и выполняется с использованием цифрового ключа или эквивалентного ключевого слова, как это показано на следующем примере (см. табл. 9.2). Цифровой ключ состоит из неповторяющихся цифр, а соответствующее ему ключевое слово – из неповторяющихся символов. Исходный текст (plain text) записывается под ключом построчно. Зашифрованное сообщение (cipher text) выписывается по

**Таблица 9.2.** Пример использования простой перестановки

| Ключевое слово | S | E | C | U | R | I | T | Y |
|---|---|---|---|---|---|---|---|---|
| Цифровой ключ | 5 | 2 | 1 | 7 | 4 | 3 | 6 | 8 |
| Исходный текст (plain text), записанный построчно | T | R | A | N | S | P | O | S |
| | I | T | I | O | N | α | I | S |
| | α | T | H | E | α | E | N | C |
| | I | P | H | E | R | α | M | E |
| | T | H | O | D | α | α | α | α |

α – служебный символ, в данном случае означает пробел

столбцам в том порядке, как это предписывают цифры ключа или в том порядке, в котором расположены отдельные символы ключевого слова.

Для рассматриваемого примера зашифрованное сообщение будет выглядеть следующим образом:

AIHHORTTPHPαEααα...SSCEα.

**Гаммирование** (смешивание с маской) основано на побитном сложении по модулю 2 (в соответствии с логикой ИСКЛЮЧАЮЩЕЕ ИЛИ) исходного сообщения с заранее выбранной двоичной последовательностью (маской). Компактным представлением маски могут служить числа в десятичной системе счисления или некоторый текст (в данном случае рассматривается внутренние коды символов – для английского текста таблица ASCII). На рис. 9.2 показано, как исходный символ «A» при сложении с маской $0110\ 1001_2$ переходит в символ «(» в зашифрованном сообщении.

$$\begin{array}{ll} & "A" \rightarrow 41_{16} = 0100\ 0001_2 \\ \oplus & \text{маска} \rightarrow 69_{16} = 0110\ 1001_2 \\ \hline & "(" \rightarrow 28_{16} = 0010\ 1000_2 \end{array}$$

**Рис. 9.2.** Пример использования гаммирования

Операция суммирования по модулю 2 (ИСКЛЮЧАЮЩЕЕ ИЛИ) является обратимой, так что при сложении с той же маской (ключом) зашифрованного сообщения получается исходный текст (происходит дешифрование). В качестве маски (ключа) могут использоваться константы типа $\pi$ или $e$ и тогда маска будет иметь конечную длину. Наибольшую устойчивость к дешифрованию может обеспечить применение маски с бесконечной длиной, которая образована генератором случайных (точнее, псевдослучайных) последовательностей. Такой генератор легко реализуется аппаратными или программными средствами, например, с помощью сдвигового регистра с обратными связями, который используется при вычислении помехоустойчивого циклического кода. Точное воспроизведение псевдослучайной последовательности в генераторе на приемном конце линии обеспечивается при установке такого же исходного состояния (содержимого сдвигового регистра) и той же структуры обратных связей, что и в генераторе на передающем конце.

Перечисленные «классические» методы шифрования (подстановка, перестановка и гаммирование) являются линейными в том смысле, что длина зашифрованного сообщения равна длине исходного текста. Возможно *нелинейное преобразование* типа подстановки вместо исходных символов (или целых слов, фраз, предложений) заранее выбранных комбинаций символов другой длины. Эффективна также защита информации методом рассечения-разнесения, когда исходные данные разбиваются на блоки, каждый из кото-

рых не несет полезной информации, и эти блоки хранятся и передаются независимо друг от друга. Для текстовой информации отбор данных для таких блоков может производиться по группам, которые включают фиксированное число бит, меньшее, чем число бит на символ в таблице кодировки. В последнее время становится популярной так называемая *компьютерная стеганография* (от греческих слов steganos – секрет, тайна и graphy – запись), представляющая собой сокрытие сообщения или файла в другом сообщении или файле. Например, можно спрятать зашифрованный аудио- или видеофайл в большом информационном или графическом файле. Объем файла – контейнера должен быть больше объема исходного файла не менее чем в восемь раз. Примерами распространенных программ, реализующих компьютерную стеганографию, являются S – Tools (для ОС Windows'95/NT) и Steganos for Windows'95. Собственно шифрование информации осуществляется с применением стандартных или нестандартных алгоритмов.

Стандартные методы шифрования (национальные или международные) для повышения степени устойчивости к дешифрованию реализуют несколько этапов (шагов) шифрования, на каждом из которых используются различные «классические» методы шифрования в соответствии с выбранным ключом (или ключами). Существуют две принципиально различные группы стандартных методов шифрования:

- шифрование с применением одних и тех же ключей (шифров) при шифровании и дешифровании (симметричное шифрование или системы с закрытыми ключами – private-key systems);
- шифрование с использованием открытых ключей для шифрования и закрытых – для дешифрования (несимметричное шифрование или системы с открытыми ключами – public-key systems).

Строгое математическое описание алгоритмов стандартных методов шифрования слишком сложно. Для пользователей важны в первую очередь «потребительские» свойства различных методов (степень устойчивости к дешифрованию, скорость шифрования и дешифрования, порядок и удобство распространения ключей), которые и рассматриваются ниже.

Для дальнейшего повышения устойчивости к дешифрованию могут применяться последовательно несколько стандартных методов или один метод шифрования (но с разными ключами).

## Стандартные методы шифрования и криптографические системы

Стандарт шифрования США **DES** (Data Encryption Standard – стандарт шифрования данных) относится к группе методов симметричного шифрования и действует с 1976 года. Число шагов – 16. Длина ключа – 56 бит, из которых 8 бит – проверочные разряды четности/нечетности. Дол-

гое время степень устойчивости к дешифрованию этого метода считалась достаточной, однако в настоящее время он устарел. Вместо DES предлагается «тройной DES» – **3DES**, в котором алгоритм DES используется 3 раза, обычно в последовательности «шифрование – дешифрование – шифрование» с тремя разными ключами на каждом этапе.

Надежным считается алгоритм **IDEA** (International Data Encryption Algorithm), разработанный в Швейцарии и имеющий длину ключа 128 бит.

Отечественный **ГОСТ28147-89** – это аналог DES, но с длиной ключа 256 бит, так что его степень устойчивости к дешифрованию изначально существенно выше. Важно также и то, что в данном случае предусматривается целая система защиты, которая преодолевает «родовой» недостаток симметричных методов шифрования – возможность подмены сообщений. Такие усовершенствования, как имитовставки, хэш-функции и электронные цифровые подписи позволяют «авторизовать» передаваемые сообщения.

К достоинствам симметричных методов шифрования относится высокая скорость шифрования и дешифрования, к недостаткам – малая степень защиты в случае, если ключ стал доступен третьему лицу.

Довольно популярны, особенно при использовании электронной почты, несимметричные методы шифрования или системы с открытыми ключами – public-key systems. К этой группе методов относится, в частности, **PGP** (Pretty Good Privacy – достаточно хорошая секретность). Каждый пользователь имеет пару ключей. Открытые ключи предназначены для шифрования и свободно рассылаются по сети, но не позволяют произвести дешифрование. Для этого нужны секретные (закрытые) ключи. Принцип шифрования в данном случае основывается на использовании так называемых односторонних функций. Прямая функция $x \rightarrow f(x)$ легко вычисляется на основании открытого алгоритма (ключа). Обратное преобразование. $f(x) \rightarrow x$ без знания закрытого ключа затруднено и должно занимать довольно длительное время, которое и определяет степень «трудновычислимости» односторонней функции.

Идея системы с открытыми ключами может быть пояснена следующим образом (табл. 9.3). Для шифрования сообщений можно взять обычную телефонную книгу, в которой имена абонентов расположены в алфавитном порядке и предшествуют телефонным номерам. У пользователя имеется возможность выбора соответствия между символом в исходном тексте и именем абонента, то есть это многоалфавитная система. Ее степень устойчивости к дешифрованию выше. Легальный пользователь имеет «обратный» телефонный справочник, в котором в первом столбце располагаются телефонные номера по возрастанию, и легко производит дешифрование. Если же такового нет, то пользователю предстоит утомительное и многократное просматривание доступного прямого справочника в поисках нужных телефонных номеров. Это и есть практическая реализация трудно-

**Таблица 9.3.** Пример шифрования в системе с открытыми ключами

| Исходное слово | Выбранное имя абонента | Зашифрованное сообщение (телефонные номера) |
|---|---|---|
| S | Scott | 3541920 |
| A | Adleman | 4002132 |
| U | Ullman | 7384502 |
| N | Nivat | 5768115 |
| A | Aho | 7721443 |

вычислимой функции. Сам по себе метод шифрования на основе телефонных справочников вряд ли перспективен хотя бы из-за того, что никто не мешает потенциальному взломщику составить «обратный» телефонный справочник. Однако в используемых на практике методах шифрования данной группы в смысле надежности защиты все обстоит благополучно.

Другая известная система с открытыми ключами – **RSA.**

Несимметричные методы шифрования имеют преимущества и недостатки, обратные тем, которыми обладают симметричные методы. В частности, в несимметричных методах с помощью посылки и анализа специальных служебных сообщений может быть реализована процедура аутентификации (проверки легальности источника информации) и целостности (отсутствия подмены) данных. При этом выполняются операции шифрования и дешифрования с участием открытых ключей и секретного ключа данного пользователя. Таким образом, симметричные системы можно с достаточным основанием отнести к полноценным криптографическим системам. В отличие от симметричных методов шифрования, проблема рассылки ключей в несимметричных методах решается проще – пары ключей (открытый и закрытый) генерируются «на месте» с помощью специальных программ. Для рассылки открытых ключей используются такие технологии как **LDAP** (Lightweight Directory Access Protocol – протокол облегченного доступа к справочнику). Рассылаемые ключи могут быть предварительно зашифрованы с помощью одного из симметричных методов шифрования.

Традиционные и обязательные для современных криптографических систем способы обеспечения аутентификации и проверки целостности получаемых данных (хэш-функции и цифровые подписи), которые реализуются непосредственными участниками обмена, не являются единственно возможными. Распространен также способ, осуществляемый с участием сторонней организации, которой доверяют все участники обменов. Речь идет об использовании так называемых цифровых сертификатов – посылаемых по сети сообщений с цифровой подписью, удос-

товеряющей подлинность открытых ключей.

## Программные средства защиты информации

**Встроенные средства защиты информации в сетевых ОС** доступны, но не всегда, как уже отмечалось, могут полностью решить возникающие на практике проблемы. Например, сетевые ОС NetWare 3.x, 4.x позволяют осуществить надежную «эшелонированную» защиту данных от аппаратных сбоев и повреждений. Система SFT (System Fault Tolerance – система устойчивости к отказам) компании Novell включает три основные уровня:

- SFT Level I предусматривает, в частности, создание дополнительных копий FAT и Directory Entries Tables, немедленную верификацию каждого вновь записанного на файловый сервер блока данных, а также резервирование на каждом жестком диске около 2% от объема диска. При обнаружении сбоя данные перенаправляются в зарезервированную область диска, а сбойный блок помечается как «плохой» и в дальнейшем не используется.
- SFT Level II содержит дополнительные возможности создания «зеркальных» дисков, а также дублирования дисковых контроллеров, источников питания и интерфейсных кабелей.
- SFT Level III позволяет применять в локальной сети дублированные серверы, один из которых является «главным», а второй, содержащий копию всей информации, вступает в работу в случае выхода «главного» сервера из строя.

Система контроля и ограничения прав доступа в сетях NetWare (защита от несанкционированного доступа) также содержит несколько уровней:

- уровень начального доступа (включает имя и пароль пользователя, систему учетных ограничений – таких как явное разрешение или запрещение работы, допустимое время работы в сети, место на жестком диске, занимаемое личными файлами данного пользователя, и т.д.);
- уровень прав пользователей (ограничения на выполнение отдельных операций и/или на работу данного пользователя как члена подразделения, в определенных частях файловой системы сети);
- уровень атрибутов каталогов и файлов (ограничения на выполнение отдельных операций, в том числе удаления, редактирования или создания, идущие со стороны файловой системы и касающиеся всех пользователей, пытающихся работать с данными каталогами или файлами);
- уровень консоли файл-сервера (блокирование клавиатуры файл-сервера на время отсутствия сетевого администратора до ввода им специального пароля).

Однако полагаться на эту часть системы защиты информации в ОС NetWare можно далеко не всегда. Свидетельством тому являются много-

численные инструкции в Интернете и готовые доступные программы, позволяющие взломать те или иные элементы защиты от несанкционированного доступа.

То же замечание справедливо по отношению к более поздним версиям ОС NetWare (вплоть до последней 6-й версии) и к другим «мощным» сетевым ОС со встроенными средствами защиты информации (Windows NT, UNIX,...). Дело в том, что защита информации – это только часть тех многочисленных задач, которые решаются сетевыми ОС. Усовершенствование одной из функций в ущерб другим (при понятных разумных ограничениях на объем, занимаемый данной ОС на жестком диске) не может быть магистральным направлением развития таких программных продуктов общего назначения, которыми являются сетевые ОС. В то же время в связи с остротой проблемы защиты информации наблюдается тенденция интеграции (встраивания) отдельных, хорошо зарекомендовавших себя и ставших стандартными средств в сетевые ОС, или разработка собственных «фирменных» аналогов известным программам защиты информации. Так, в сетевой ОС NetWare 4.1 предусмотрена возможность кодирования данных по принципу «открытого ключа» (алгоритм RSA) с формированием электронной подписи для передаваемых по сети пакетов.

**Специализированные программные средства защиты информации** от несанкционированного доступа обладают в целом лучшими возможностями и характеристиками, чем встроенные средства сетевых ОС. Кроме программ шифрования и криптографических систем, существует много других доступных внешних средств защиты информации. Из наиболее часто упоминаемых решений следует отметить следующие две системы, позволяющие ограничить и контролировать информационные потоки.

1. Firewalls – брандмауэры (дословно firewall – огненная стена). Между локальной и глобальной сетями создаются специальные промежуточные серверы, которые инспектируют и фильтруют весь проходящий через них трафик сетевого/транспортного уровней. Это позволяет резко снизить угрозу несанкционированного доступа извне в корпоративные сети, но не устраняет эту опасность полностью. Более защищенная разновидность метода – это способ маскарада (masquerading), когда весь исходящий из локальной сети трафик посылается от имени firewall-сервера, делая локальную сеть практически невидимой.
2. Proxy-servers (proxy – доверенность, доверенное лицо). Весь трафик сетевого/транспортного уровней между локальной и глобальной сетями запрещается полностью – маршрутизация как таковая отсутствует, а обращения из локальной сети в глобальную происходят через специальные серверы-посредники. Очевидно, что при этом обращения из глобальной сети в локальную становятся невозможными в принципе. Этот метод не дает достаточной защиты против атак на более высоких уровнях – например, на уровне приложения (вирусы, код Java и JavaScript).

# Глава 7. Алгоритмы сети ETHERNET/FAST ETHERNET

## Лекция 10. Алгоритмы сети ETHERNET/FAST ETHERNET

**В данной лекции излагается метод управления обменом CSMA/CD, используемый в широко распространенных сетях семейства Ethernet, и оказывающий существенное влияние на их особенности и характеристики. Кроме того, рассматривается алгоритм формирования и свойства помехоустойчивого циклического кода CRC, который применяется для обнаружения ошибок из-за наводок и помех в получаемых по сети данных.**

**Ключевые слова:** метод управления обменом (метод доступа), коллизия, окно коллизий, показатель использования сети, помехоустойчивые коды, минимальное кодовое расстояние, циклические коды.

В данной главе предлагается подробно рассмотреть два основных алгоритма, применяемых в самой распространенной сегодня сети Ethernet/Fast Ethernet. Речь идет о методе управления обменом (доступа) CSMA/CD и о методе вычисления циклической контрольной суммы (помехоустойчивого циклического кода) пакета CRC.

Эти же самые алгоритмы используются во многих других локальных сетях. Например, метод доступа CSMA/CD применяется в сетях IBM PC Network, AT&T Starlan, Corvus Omninet, PC Net, G-Net и др. Если говорить об алгоритме вычисления циклической контрольной суммы CRC, то он стал фактическим стандартом для любых локальных сетей. Таким образом, все, что представлено в данной главе, относится ко многим локальным сетям.

### Метод управления обменом CSMA/CD

Как уже говорилось в главе 3, метод управления обменом CSMA/CD (Carrier-Sense Multiple Access with Collision Detection – множественный доступ с контролем несущей и обнаружением коллизий) относится к децентрализованным случайным (точнее, квазислучайным) методам. Он используется как в обычных сетях типа Ethernet, так и в высокоскоростных сетях (Fast Ethernet, Gigabit Ethernet). Поскольку характеристики и области применения этих популярных на практике сетей связаны именно с особенностями используемого метода доступа, его стоит рассмотреть более подробно.

Сначала о названии метода. В ранней сети типа Alohanet, работавшей с 1970 года на Гавайских островах, использовался радиоканал и установленный на спутнике ретранслятор (отсюда слово «несущая» в названии метода), а также сравнительно простой метод доступа CSMA (без обнаружения коллизий). В сетях типа Ethernet и Fast Ethernet в качестве несущей выступает синхросигнал, «подмешиваемый» к передаваемым данным таким образом, чтобы обеспечить надежную синхронизацию на приемном конце. Это реализуется за счет организации (при необходимости) дополнительных принудительных переходов сигнала между двумя (как в коде Манчестер-П) или тремя электрическими уровнями (как в коде типа 8B6T, используемом в сегменте Fast Ethernet 100BaseT4 на основе четырех неэкранированных витых пар). По сравнению с классическим методом CSMA в методе CSMA/CD добавлено обнаружение конфликтов (коллизий) во время передачи, что повышает скорость доставки информации.

При описании временных диаграмм сетей типа Ethernet и Fast Ethernet, а также предельных размеров пакетов (кадров) широко используются следующие термины:

- IPG (InterPacket Gap, межпакетная щель) – минимальный промежуток времени между передаваемыми пакетами (9,6 мкс для Ethernet / 0,96 мкс для Fast Ethernet). Другое название – межкадровый интервал.
- BT (Bit Time, время бита) – интервал времени для передачи одного бита (100 нс для Ethernet / 10 нс для Fast Ethernet).
- PDV (Path Delay Value, значение задержки в пути) – время прохождения сигнала между двумя узлами сети (круговое, то есть удвоенное). Учитывает суммарную задержку в кабельной системе, сетевых адаптерах, повторителях и других сетевых устройствах.
- Collision window (окно коллизий) – максимальное значение PDV для данного сегмента.
- Collision domain (область коллизий, зона конфликта) – часть сети, на которую распространяется ситуация коллизии, конфликта.
- Slot time (время канала) – максимально допустимое окно коллизий для сегмента (512 • BT).
- Minimum frame size – минимальный размер кадра (512 бит).
- Maximum frame size – максимальный размер кадра (1518 байт).
- Maximum network diameter (максимальный диаметр сети) — максимальная допустимая длина сегмента, при которой его окно коллизий не превышает slot time, времени канала.
- Truncated binary exponential back off (усеченная двоичная экспоненциальная отсрочка) – задержка перед следующей попыткой передачи пакета после коллизии (допускается максимум 16 попыток). Вычисляется она по следующей формуле:

$$RAND(0,2^{min(N,10)}) \times 512 \times BT$$

где N – значение счетчика попыток, RAND(a, b) – генератор случайных нормально распределенных целых чисел в диапазоне a...b, включая крайние значения. Дискрет изменения данного параметра равен минимальной длине пакета или максимально допустимой двойной задержке распространения сигнала в сети (PDV).

### Алгоритм доступа к сети

На рис. 10.1 показана структурная схема алгоритма доступа к сети в соответствии с методом CSMA/CD для одного из абонентов, имеющих данные (кадры) для передачи.

В начале из кадра, предназначенного для передачи, абонент (узел) формирует пакет. Далее при обозначении блоков информации, передаваемых по сети при использовании алгоритма CSMA/CD, понятия «кадр» и «пакет» не различаются, что не совсем правильно, но соответствует сложившейся практике.

Если после подготовки пакета сеть свободна, то абонент (узел) имеет право начать передачу. Но в первую очередь он должен проверить, прошло ли минимально допустимое время IPG после предыдущей передачи (блок 1 на рисунке). Только по окончании времени IPG абонент может начать передачу битов своего пакета (блок 2 на рисунке).

После передачи каждого бита абонент поверяет наличие конфликта (коллизии) в сети. Если коллизий нет, передача битов продолжается до окончания пакета (блок 4 на рисунке). В этом случае считается, что передача прошла успешно.

Если после передачи какого-то бита обнаружена коллизия, то передача пакета прекращается. Абонент (узел) усиливает коллизию, передавая 32-битовый сигнал ПРОБКА (JAM) и начинает готовиться к следующей попытке передачи (блок 3 на рисунке). Сигнал ПРОБКА гарантирует, что факт наличия коллизии обнаружат все абоненты, участвующие в конфликте.

После передачи сигнала ПРОБКА абонент, обнаруживший коллизию, увеличивает значение счетчика числа попыток (перед началом передачи счетчик был сброшен в нуль). Максимальное число попыток передачи должно быть не более 16, поэтому если счетчик попыток переполнился, то попытки передать пакет прекращаются. Считается, что в этом случае сеть сильно перегружена, в ней слишком много коллизий. Эта ситуация – аварийная, и обрабатывается она на более высоких уровнях протоколов обмена.

Если же количество попыток не превысило 16, то производится вычисление величины задержки по приведенной формуле, а затем и выдерж-

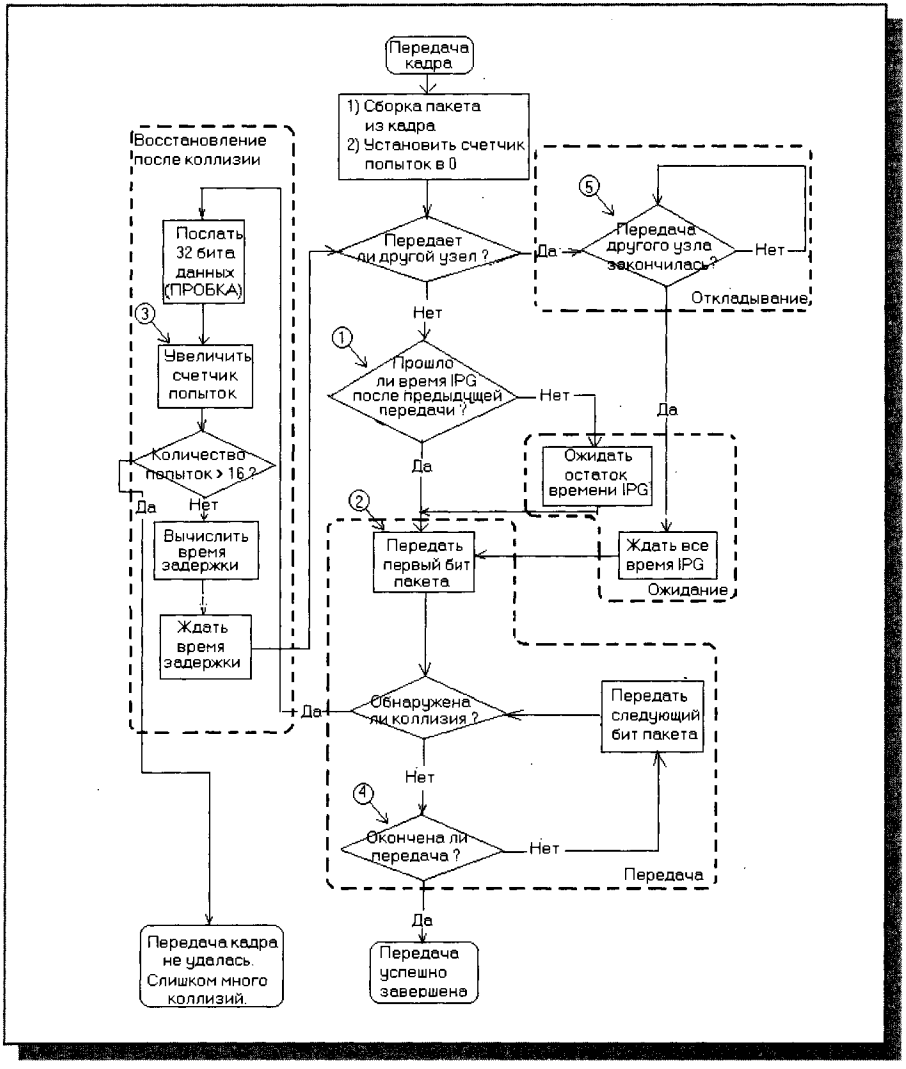



**Рис. 10.1.** Структурная схема алгоритма доступа к сети в соответствии с методом CSMA/CD

ка вычисленного временного интервала. Случайный характер величины задержки с высокой степенью вероятности гарантирует, что у всех абонентов, участвующих в конфликте, задержки будут различными. Затем попытка передать пакет повторяется с начала. Абонент, у которого вычисленная задержка будет меньше, начнет следующую передачу первым и заблокирует все остальные передачи.

Если в момент возникновения заявки на передачу (после окончания подготовки пакета) сеть занята другим абонентом, ведущим передачу, то данный абонент ждет освобождения сети (блок 5 на рисунке). После освобождения сети он должен выждать время IPG после предыдущей передачи по сети до начала собственной передачи. Это связано с конечным быстродействием узлов, осуществляющих проверку наличия несущей (занятости среды каким-либо передающим абонентом).

Таким образом, получается, что метод CSMA/CD не только не предотвращает коллизии, наоборот, он их предполагает и даже провоцирует, а затем разрешает. Например, если заявки на передачу возникли у нескольких абонентов во время занятости сети, то после ее освобождения все эти абоненты одновременно начнут передачу и образуют коллизию. Коллизия появляются и в случае свободной сети, если заявки на передачу возникают у нескольких абонентов одновременно. В обоих случаях под словом «одновременно» понимается «в пределах интервала двойного прохождения сигнала по сети», то есть в пределах 512-битовых интервалов. Точно также в пределах 512-битовых интервалов обнаруживаются все коллизии в сети.

Если коллизия обнаруживается раньше 480–битового интервала, то в результате в сети образуются пакеты, длина которых меньше нижнего установленного предела в 512–битовых интервалов (64 байта) даже с добавлением сигнала ПРОБКА. Такие пакеты (кадры) называются карликовыми (runt frames). Если же коллизия обнаруживается в конце 512-битового интервала (после 480–битового интервала), то в результате может получиться пакет допустимой длины (вместе с сигналом ПРОБКА). Такие пакеты называть карликовыми не совсем корректно. Сигнал ПРОБКА, образующий 32 последних бита пакета, выступает в виде контрольной суммы пакета. Однако вероятность того, что ПРОБКА будет соответствовать правильной контрольной сумме пакета, бесконечно мала (примерно 1 случай на 4,2 миллиарда).

Коллизии (наложения пакетов в процессе передачи) могут и должны обнаруживаться до окончания передачи. Действительно, анализ принятого в конце каждого пакета поля FCS, фактически содержащего помехоустойчивый циклический код CRC (Cyclic Redundancy Check), привел бы к неоправданному снижению скорости передачи.

Практически коллизии обнаруживаются либо самим передающим абонентом, либо повторителями в сети, возможно, задолго до окончания передачи заведомо испорченного пакета. Если учесть, что длина пакетов в локальной сети типа Ethernet / Fast Ethernet может лежать в диапазоне от 64 до 1518 байт, то досрочное прекращение передачи и освобождение линии означает заметное повышение эффективности использования ее пропускной способности.

Первым признаком возникновения коллизии является факт получения сигнала ПРОБКА передающим абонентом во время передачи пакета. Другие признаки связаны с неверным форматом пакетов, передача которых была досрочно прекращена из-за возникновения коллизии:

- длина пакета меньше 64 байт (512 бит);
- пакет имеет неверную контрольную сумму FCS (точнее, неверный циклический код);
- длина пакета не кратна восьми.

Наконец, в таких сетях как Ethernet используется код Манчестер-П и аппаратный способ определения коллизии, основанный на анализе отклонения среднего значения сигнала от нуля.

Даже при загруженной сети для одного абонента число следующих подряд коллизий обычно не превышает 3. Этому способствует случайный характер возникновения запроса на передачу и случайная дискретная величина отсрочки следующей попытки передачи при возникновении коллизии. Число коллизий тем больше, чем больше диаметр (размер) сегмента и чем дальше расположены друг от друга абоненты с интенсивным трафиком.

## Оценка производительности сети

Вопрос об оценке производительности сетей, использующих случайный метод доступа CSMA/CD, не очевиден из-за того, что существуют несколько различных показателей. Прежде всего, следует упомянуть три связанные между собой показателя, характеризующие производительность сети в идеальном случае – при отсутствии коллизий и при передаче непрерывного потока пакетов, разделенных только межпакетным интервалом IPG. Очевидно, такой режим реализуется, если один из абонентов активен и передает пакеты с максимально возможной скоростью. Неполное использование пропускной способности в этом случае связано, кроме существования интервала IPG, с наличием служебных полей в пакете Ethernet (см. рис. 10.2).

Пакет максимальной длины является наименее избыточным по относительной доле служебной информации. Он содержит 12304 бит (включая интервал IPG), из которых 12000 являются полезными данными.

Поэтому максимальная скорость передачи пакетов (или, иначе, *скорость в кабеле* – wire speed) составит в случае сети Fast Ethernet

$10^8$ бит/с/ 12304 бит $\cong$ 8127,44 пакет/с.

*Пропускная способность* представляет собой скорость передачи полезной информации и в данном случае будет равна

8127,44 пакет/с $\times$ 1500 байта $\cong$ 12,2 Мбайт/с.

Наконец, *эффективность использования* физической скорости пере-

дачи сети, в случае Fast Ethernet равной 100 Мбит/с, по отношению только к полезным данным составит

$$8127{,}44 \text{ пакет/с} \times 12000 \text{ бит/ } 10^8 \text{ бит/с} \cong 98\%.$$

При передаче пакетов минимальной длины существенно возрастает скорость в кабеле, что означает всего лишь факт передачи большого числа коротких пакетов. В то же время пропускная способность и эффективность заметно (почти в два раза) ухудшаются из-за возрастания относительной доли служебной информации.

Для реальных сетей, в частности Fast Ethernet с большим числом активных абонентов N пропускная способность на уровне 12,2 Мбайт/с для какого-либо абонента является пиковым, редко реализуемым значением. При одинаковой активности всех абонентов средняя пропускная способность для каждого из них составит 12,2/N Мбайт/с, а на самом деле может оказаться еще меньше из-за возникновения коллизий, ошибок в работе сетевого оборудования и влияния помех (в случае работы локальной сети в условиях, когда кабельная система подвержена влиянию больших внешних электромагнитных наводок). Влияние помех, так же как и поздних конфликтов (late collision) в некорректных сетях, отслеживается с помощью анализа поля FCS–пакета.

Для реальных сетей более информативен такой показатель производительности, как *показатель использования сети* (network utilization), который представляет собой долю в процентах от суммарной пропускной способности (не поделенной между отдельными абонентами). Он учитывает коллизии и другие факторы. Ни сервер, ни рабочие станции не содержат средств для определения показателя использования сети. Этой цели служат специальные, не всегда доступные из-за высокой стоимости такие аппаратно-программные средства, как анализаторы протоколов.

Считается, что для загруженных систем Ethernet и Fast Ethernet хорошим значением показателя использования сети является 30%. Это значение соответствует отсутствию длительных простоев в работе сети и обеспечивает достаточный запас в случае пикового повышения нагрузки. Однако если показатель использования сети значительное время составляет 80...90% и более, то это свидетельствует о практически полностью используемых (в данное время) ресурсах, но не оставляет резерва на будущее. Впрочем, для реальных сетей, к примеру Fast Ethernet, это скорее гипотетическая ситуация.

На рис. 10.2 приведена зависимость показателя использования сети от времени при условии, что предложенная нагрузка (offered load), то есть текущий запрос на пропускную способность, линейно возрастает. Сначала показатель использования сети также линейно повышается, но затем конкуренция за владение средой передачи порождает коллизии, и рас-

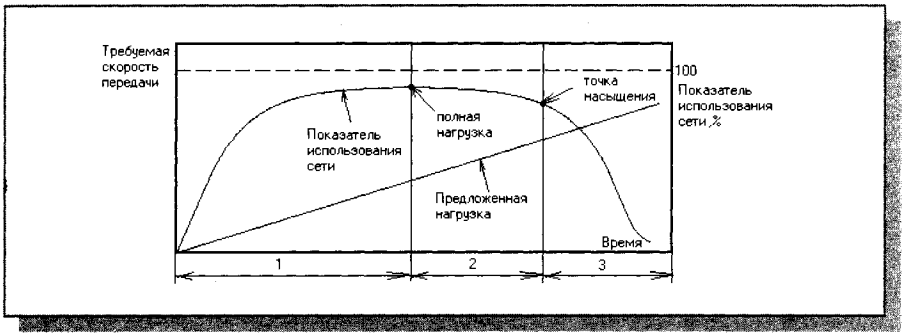



**Рис. 10.2.** Зависимость показателя использования сети от времени при линейном увеличении предложенной нагрузки (1 – наилучшая область работы, 2 – приемлемая, 3 – плохая)

сматриваемый показатель достигает максимума (точка полной нагрузки на графике). При дальнейшем увеличении предложенной нагрузки показатель использования сети начинает уменьшаться, особенно резко после точки насыщения. Это «плохая» область работы сети. Считается, что сеть работает хорошо, если и предложенная нагрузка, и показатель использования сети высоки.

Некоторые авторы предлагают для широко распространенного понятия *«перегрузка»* (overload) сетей на основе метода доступа CSMA/CD следующее определение: сеть перегружена, если она не может работать при полной нагрузке в течение 80% своего времени (при этом 20% времени показатель использования сети недопустимо мал из-за коллизий). После точки насыщения наступает крах Ethernet (Ethernet collapse), когда возрастающая предложенная нагрузка заметно превышает возможности сети. Стоит заметить, что реально маловероятно, чтобы предложенная нагрузка постоянно увеличивалась во времени и надолго превышала пропускную способность сети типа Fast Ethernet. Более того, любой детерминированный метод доступа не может обеспечить реализацию сколь угодно большой предложенной нагрузки, существующей в течение продолжительного времени. Если данный вариант детерминированного метода доступа не использует, как и метод CSMA/CD, систему приоритетов, то ни один из абонентов не может захватить сеть более чем на время передачи одного пакета, однако передача данных отдельными пакетами с долгими паузами между ними ведет к снижению скорости передачи для каждого абонента. Преимущество детерминированных методов состоит в возможности простой организации системы приоритетов, что полезно из-за наличия определенной иерархии в любом крупном коллективе.

# Использование помехоустойчивых кодов для обнаружения ошибок в сети

Сигналы, непосредственно передаваемые по последовательным линиям (типа витой пары, коаксиального кабеля или телефонной линии), подвержены влиянию ряда факторов, воздействие которых может привести к возникновению ошибок в принятой информации. Ошибки могут возникать вследствие влияния на канал связи наводок и помех естественного или искусственного происхождения, а также вследствие изменения конфигурации системы передачи информации с временным нарушением или без нарушения целостности канала связи (например, в случае подключения новых абонентов к существующей локальной информационной сети). Некоторые из ошибок могут быть обнаружены на основании анализа вида принятого сигнала, так как в нем появляются характерные искажения. Примером может служить код Манчестер-II, используемый в сетях Ethernet. На передающем конце линии этот код обязательно содержит переход с низкого электрического уровня на высокий или обратно в середине каждого тактового интервала, требуемого для передачи одного бита информации. Он также имеет среднюю составляющую, близкую к нулю. Эти свойства кода Манчестер-II могут использоваться для обнаружения разного рода ошибок. В частности, отличие средней составляющей сигнала от нуля является одним из признаков возникновения коллизий (наложений пакетов от разных абонентов), характерных для метода доступа CSMA/CD в сетях типа Ethernet. Однако сколько-нибудь серьезную систему обнаружения ошибок, вызванных воздействием помех с непредсказуемым поведением, на этой основе построить невозможно. Стандартные протоколы обмена информации в сетях предусматривают введение обязательного поля для размещения помехоустойчивого (корректирующего) кода. Если в результате обработки принятого пакета обнаружится несоответствие принятого и вновь вычисленного помехоустойчивого кода, с большой долей вероятности можно утверждать, что среди принятых бит имеются ошибочные. Передачу такого пакета нужно будет повторить (в расчете на случайный характер помех).

## Способы снижения числа ошибок в принятой информации

Имеется разрыв между требованиями к верности принимаемой информации и возможностями каналов связи. В частности, стандартами международных организаций ITU-T и МОС установлено, что вероятность ошибки при телеграфной связи не должна превышать $3 \times 10^{-5}$ (на знак), а при передаче данных – $10^{-6}$ (на единичный элемент, бит). На практике допустимая вероятность ошибки при передаче данных может быть еще меньше – $10^{-9}$. В то же время каналы связи (особенно провод-

ные каналы большой протяженности и радиоканалы) обеспечивают вероятность ошибки на уровне $10^{-3}...10^{-4}$ даже при использовании фазовых корректоров, регенеративных ретрансляторов и других устройств, улучшающих качество каналов связи.

Кардинальным способом снижения вероятности ошибок при приеме является введение избыточности в передаваемую информацию. В системах передачи информации без обратной связи данный способ реализуется в виде помехоустойчивого кодирования, многократной передачи информации или одновременной передачи информации по нескольким параллельно работающим каналам. Помехоустойчивое кодирование доступнее, при прочих равных условиях оно позволяет обойтись меньшей избыточностью и за счет этого повысить скорость передачи информации.

## Характеристики и разновидности помехоустойчивых кодов

Помехоустойчивое кодирование предполагает введение в передаваемое сообщение, наряду с информационными, так называемые проверочные разряды, формируемые в устройствах защиты от ошибок (кодерах — на передающем конце, декодерах – на приемном). Избыточность позволяет отличить разрешенную и запрещенную (искаженную за счет ошибок) комбинации при приеме, иначе одна разрешенная комбинация переходила бы в другую.

Помехоустойчивый код характеризуется тройкой чисел (n, k, $d_0$), где n – общее число разрядов в передаваемом сообщении, включая проверочные (r), k=n-r – число информационных разрядов, $d_0$ – минимальное кодовое расстояние между разрешенными кодовыми комбинациями, определяемое как минимальное число различающихся бит в этих комбинациях. Число обнаруживаемых ($t_o$) и (или) исправляемых ($t_и$) ошибок (разрядов) связано с параметром $d_0$ соотношениями:

$$d_0 \geqslant t_o + 1,$$
$$d_0 \geqslant 2t_и + 1,$$
$$d_0 \geqslant t_o + t_и + 1.$$

Иногда используются дополнительные показатели избыточности, производные от приведенных выше характеристик n, k: R = r / n – относительная избыточность, v = k / n – относительная скорость передачи.

Существующие помехоустойчивые коды можно разделить на ряд групп, из которых лишь часть применяются для обнаружения ошибок в передаваемых по сети пакетах (на рис. 10.3 используемые для этой цели группы выделены утолщенными стрелками). В группе систематических (линейных) кодов общим свойством является то, что любая разрешенная комби-

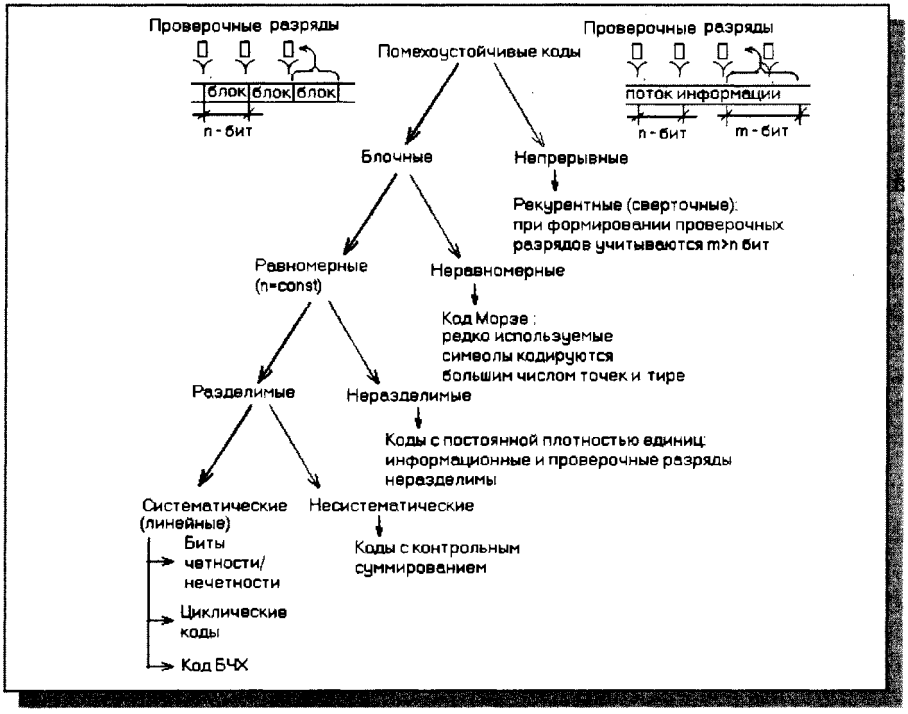



**Рис. 10.3.** Классификация помехоустойчивых кодов

нация может быть получена в результате линейных операций над линейно-независимыми векторами. Это способствует упрощению аппаратной и программной реализации данных кодов, повышает скорость выполнения необходимых операций. Простейшими систематическими кодами являются биты четности/нечетности. Они не позволяют обнаружить ошибки четной кратности (то есть ошибки одновременно в двух, четырех и т.д. битах) и поэтому используются при невысоких требованиях к верности принимаемых данных (или при малой вероятности ошибок в линии передачи). Примером может служить бит Parity (соответствие) в установках режимов работы последовательного порта с помощью команды MODE (MS DOS). Несмотря на ограниченные возможности обнаружения ошибок, биты четности/нечетности имеют большое значение в теории помехоустойчивого кодирования. Одни из первых математически обоснованных и практически использованных ранее для защиты информации в запоминающих устройствах помехоустойчивых кодов – коды Хэмминга представляют собой простую совокупность перекрестных проверок на четность/нечетность. Циклические коды могут рассматриваться как обобщенные проверки на четность/нечетность (см. далее).

## Циклические коды (CRC)

Циклические коды – это семейство помехоустойчивых кодов, включающее в себя в качестве одной из разновидностей коды Хэмминга. В целом оно обеспечивает большую гибкость с точки зрения возможности реализации кодов с необходимой способностью обнаружения и исправления ошибок, определяемой параметром $d_0$, по сравнению с кодами Хэмминга (для которых $d_0=3$ или $d_0=4$). Широкое использование циклических кодов на практике обусловлено также простотой реализации соответствующих кодеров и декодеров.

Основные свойства и само название циклических кодов связаны с тем, что все разрешенные комбинации бит в передаваемом сообщении (кодовые слова) могут быть получены путем операции циклического сдвига некоторого исходного кодового слова:

$(a_0 a_1 \ldots a_{n-2} a_{n-1})$;
$(a_{n-1} a_0 a_1 \ldots a_{n-2})$;
.....

Циклические коды задаются с помощью так называемых порождающих полиномов (многочленов) $g(x)$ или их корней. Порождающий полином имеет вид

$$G(x)=g_r x^r + g_{r-1} x^{r-1} + \ldots + g_0$$

где $g_i=\{0,1\}$, $x=2$. Кроме того, вводятся полином исходного сообщения

$$u(x) = u_{k-1} x^{k-1} + u_{k-2} x^{k-2} + \ldots + u_0$$

и кодированного сообщения

$$A(x) = a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \ldots + a_0.$$

Для этих полиномов, представляющих собой по существу альтернативную запись чисел в двоичной системе счисления, определяются операции сложения, умножения и деления, необходимые для организации кодирования и декодирования сообщения. Все операции выполняются по модулю 2.

Последовательность кодирования на примере циклического кода (7,4,3), имеющего $g(x) = x^3 + x + 1$, следующая:

1) информационная часть сообщения записывается в виде полинома:

$$u(x) = u_{k-1} x^{k-1} + u_{k-2} x^{k-2} + \ldots + u_0 .$$

В рассматриваемом примере k=4 и для сообщения 0111 получается

$$u(x) = x^2 + x + 1$$

2) u(x) умножается $x^r$, что соответствует циклическому сдвигу исходного сообщения на r разрядов влево:

$$u(x)\ x^3 = (x^2 + x + 1)\ x^3 = x^5 + x^4 + x^3$$

3) полученный многочлен делится на g(x):

$$\frac{u(x) \cdot x^r}{g(x)} = c(x) \oplus \frac{R(x)}{g(x)}$$

где c(x) — полином-частное с максимальной степенью (k–1); R(x) — полином-остаток с максимальной степенью (r-1); ⊕ – обозначение поразрядной операции суммирования по модулю 2 (исключающее ИЛИ). Кодированное сообщение представляется в виде

$$A(x)=u(x)x^r \oplus R(x)$$

то есть на место младших, освобожденных после домножения на $x^r$ разрядов, записываются проверочные разряды $a_{r-1}$, $a_{r-2}$, $a_0$. Для данного примера:

Таким образом, в этом случае

$$\begin{array}{l} x^5 + x^4 + x^3 \\ \oplus\ x^5 + x^3 + x^2 \\ \hline x^4 + x^2 \\ \oplus\ x^4 + x^2 + x \\ \hline x = R(x) \end{array} \qquad \begin{array}{|l} x^3 + x + 1 \\ \hline x^2 + x = c(x) \end{array}$$

$$A(x) = (x^5 + x^4 + x^3) \oplus x = x^5 + x^4 + x^3 + x$$

Передаваемое кодированное сообщение в обычной двоичной форме имеет вид

0111 010

$\leftarrow\rightarrow$ $\leftarrow\rightarrow$
k - бит r - бит

Один из возможных вариантов аппаратурной реализации кодера для рассматриваемого примера изображен на рис. 10.4 вместе с последовательностью сигналов, подтверждающей получение тех же проверочных разрядов (010) на восьмом такте (r + k + 1=8). Кодер представляет собой сдвиговый регистр с обратными связями, организуемыми с помощью элементов М2 (исключающее ИЛИ, сумматор по модулю 2). Структура обратных связей полностью определяется ненулевыми коэффициентами порождающего полинома g(x). На первых восьми тактах ключ Кл находится в верхнем положении, формируются проверочные разряды. Затем ключ Кл устанавливается в нижнее положение, что соответствует разрыву цепей обратных связей и передаче непосредственно в канал связи или на модулятор проверочных разрядов. Для временного хранения информационной части сообщения с целью последующей ее передачи вместе с проверочными разрядами кодер, очевидно, должен быть дополнен сдвиговым регистром длиной в k разрядов, ключами и соответствующими цепями управления. Однако в целом аппаратурные затраты при реализации кодеров в случае циклических кодов невелики – общее число триггеров и

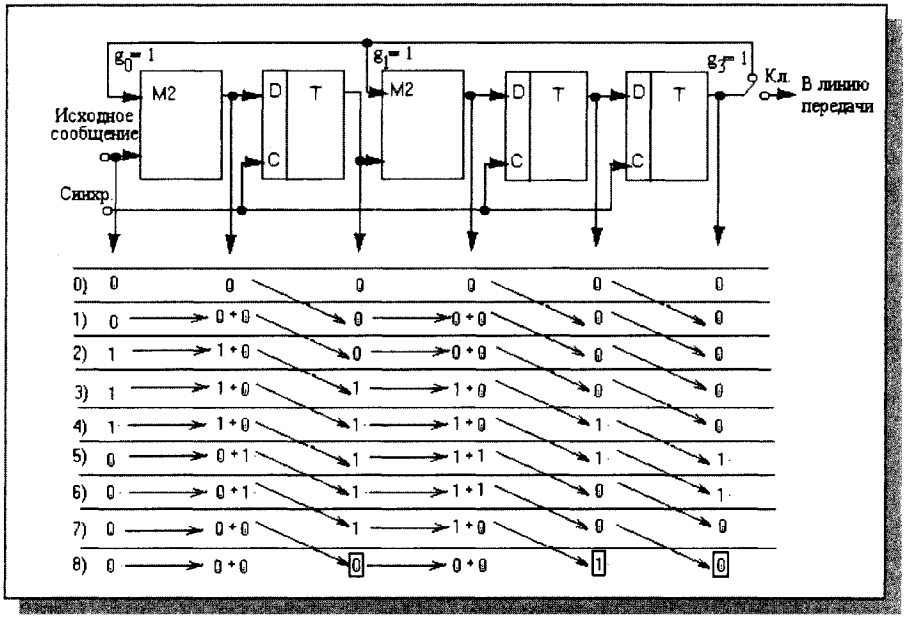



**Рис. 10.4.** Пример формирования циклического кода (сигнал обратной связи отличен от нуля на 5-м и 6-м тактах)

элементов М2 (исключая регистр временного хранения информационной части сообщения) не превышает $2r$ и не зависит от длины информационной части сообщения.

Двухвходовый элемент М2, на один из входов которого подается в последовательной форме сообщение, на выходе формирует бит четности или нечетности (в зависимости от значения сигнала на втором входе элемента М2-0 или 1) для этого сообщения. В схеме кодера (рис. 10.4) элементы М2 включены между отдельными триггерами сдвигового регистра, причем сигналы обратной связи, поступающие на «свободные» входы элементов М2 (не связанные с передачей собственно сообщения через сдвиговый регистр), зависят как от предшествующих разрядов сообщения, так и от структуры обратных связей, принятой в кодере. В результате циклический код, формируемый таким кодером, можно считать совокупностью обобщенных бит четности и нечетности, тип которых (четность или нечетность) не определен заранее и может динамически меняться от такта к такту.

Порождающие полиномы, представляющие собой так называемые неприводимые многочлены (делятся лишь на единицу и на самих себя), табулированы для разных значений $n$, $k$ и $d_0$. Практически в компьютерных сетях используются циклические коды длиною в 2 или 4 байта (16 или 32 бита), а параметры $n$, $k$ и $d_0$ в явном виде не указываются. Это связано с возможностью выбора различной длины поля данных в пакете на этапе установления и выбора параметров соединения при неизменной длине поля циклического кода. Теоретическая вероятность ошибки при приеме в случае использования циклического кода не хуже $p_{ош} \leqslant 1/2^r$, так что для выполнения условия стандарта $p_{ош} \leqslant 10^{-6}$ необходимое число проверочных разрядов $r \geqslant \log_2 10^6 \cong 20$. Кроме случайно распределенных, циклический код позволяет обнаруживать подряд следующие ошибки (так называемые пакеты ошибок) длиною $l = r$ или меньше. Это особенно важно в связи с возможностью возникновения продолжительных во времени помех, действующих на протяженные линии передачи в компьютерных сетях.

Циклические коды обладают способностью исправления ошибок высокой кратности (при большом значении параметра $d_0$) и известны технические решения декодеров с исправлением ошибок, однако практическая реализация таких декодеров на современном этапе представляется затруднительной, особенно в случае широкополосных (высокоскоростных) каналов связи. В настоящее время более распространены декодеры с обнаружением ошибок. При использовании обнаруживающего декодера неверно принятая информация может игнорироваться либо может быть запрошена повторная передача той же информации. В последнем случае предполагается наличие сигнала подтверждения правильности

принятой информации, поступающего от приемника к передатчику. По мере развития элементной базы следует ожидать появления в интегральном исполнении декодеров циклических кодов, способных не только обнаруживать, но и исправлять ошибки.

Кроме систем передачи информации, циклические коды используются в запоминающих устройствах (ЗУ) для обнаружения возможных ошибок в считываемой информации. При записи файлов на диск (в том числе при их архивировании) вместе с файлами формируются и записываются соответствующие циклические коды. При чтении файлов (в том числе при извлечении файлов из архива) вычисленные циклические коды сравниваются с записанными и таким образом обнаруживаются возможные ошибки. Свойства циклического кода лежат в основе сигнатурного анализа (эффективного способа поиска аппаратных неисправностей в цифровых устройствах различной сложности). Варианты практической реализации соответствующих кодеров и сигнатурных анализаторов имеют между собой много общего.

Следует сделать два замечания относительно сложившейся терминологии. Понятие «циклические коды» достаточно широкое, тем не менее на практике его обычно используют для обозначения только одной разновидности, описанной выше и имеющей в англоязычной литературе название CRC (Cyclic Redundancy Check – циклическая избыточная проверка). Более того, поле пакета или кадра, фактически содержащее код CRC, часто называется «контрольной суммой» (FCS – контрольная сумма кадра), что в принципе не верно, так как контрольная сумма формируется иначе. Однако именно этот термин получил широкое распространение.

Перспективными с точки зрения аппаратурной реализации представляются коды БЧХ (коды Боуза – Чаудхури – Хоквингема), также, как и коды Хэмминга, входящие в семейство циклических кодов. Коды БЧХ не слишком большой длины (примерно до n=1023), оптимальны или близки к оптимальным кодам, то есть обеспечивают максимальное значение $d_0$ при минимальной избыточности. Эти коды уже нашли практическое применение в цифровых системах записи звука (речи, музыки), причем в варианте, предусматривающем исправление обнаруженных ошибок. Относительно невысокие частоты дискретизации звуковых сигналов (48 или 96 кГц) не препятствуют проведению дополнительных вычислений так жестко, как в случае высокоскоростных сетей.

# Глава 8. Стандартные сегменты Ethernet и Fast Ethernet

## Лекция 11. Стандартные сегменты Ethernet

**В этой лекции говорится о стандартных сегментах сети Ethernet, их топологиях, аппаратуре, кабелях, разъемах, трансиверах, репитерах, о достоинствах и недостатках.**

**Ключевые слова:** 10BASE5, 10BASE2, 10BASE-T, 10BASE-FL, T-коннектор, Barrel-коннектор, BNC, RJ-45, ST, SC, MAU, FOMAU, AUI, Cheapernet, прямой и перекрестный кабели.

Как уже отмечалось, существует несколько стандартных сегментов сети Ethernet/Fast Ethernet. Каждый из них имеет свои достоинства и недостатки, свои области применения. При установке сети необходимо сделать обоснованный выбор оборудования, с тем чтобы потом не пришлось тратить значительные суммы на его замену.

### Аппаратура 10BASE5

Стандарт 10BASE5 определяет сегмент Ethernet на основе толстого коаксиального кабеля с топологией «шина» длиной до 500 метров.

Толстый коаксиальный кабель – это классический тип кабеля, который использовался в сети Ethernet с самого начала. В настоящее время он не столь широко распространен, хотя и обеспечивает максимальную протяженность сети с топологией «шина». Это связано в первую очередь с большими трудностями монтажа аппаратуры и сравнительно высокой ее стоимостью.

Толстый коаксиальный кабель представляет собой 50-омный кабель диаметром около 1 сантиметра и отличается высокой жесткостью. Он имеет два основных типа оболочки: стандартная PVC желтого цвета (например, кабель Belden 9880) и тефлоновая Teflon оранжево-коричневого цвета (например, кабель Belden 89880). Широко распространен толстый кабель типа RG-11, другой тип – RG-8 (отличие состоит в том, что у RG-11 посеребрена центральная жила). Диаметр центральной жилы – около 2 мм. Толстый кабель – это самая дорогая среда передачи (примерно втрое дороже, чем другие типы). Тем не менее, толстый кабель обладает лучшей помехоустойчивостью, меньшим затуханием и высокой механической прочностью.

По стандарту к одному сегменту (длиной до 500 метров) допустимо подключение не более 100 абонентов. Расстояния между точками их под-

ключения не должно быть меньше, чем 2,5 метра, иначе возникают искажения передаваемых сигналов. Для удобства пользователя на оболочку кабеля часто наносятся черные полоски через каждые 2,5 метра.

Аппаратные средства 10BASE5 представлены на рис. 11.1. Они включают в себя кабель, разъемы, терминаторы, трансиверы и трансиверные кабели. Трансивер представляет собой активный приемопередатчик с детектором коллизий и высоковольтной (до 5 кВ) гальванической развязкой. Кроме того, в трансивере предусмотрена защита от затянувшейся передачи (jabber), подробнее эта функция будет рассмотрена в следующей главе. Трансивер может иметь светодиодные индикаторы питания, передачи, приема и наличия коллизий.

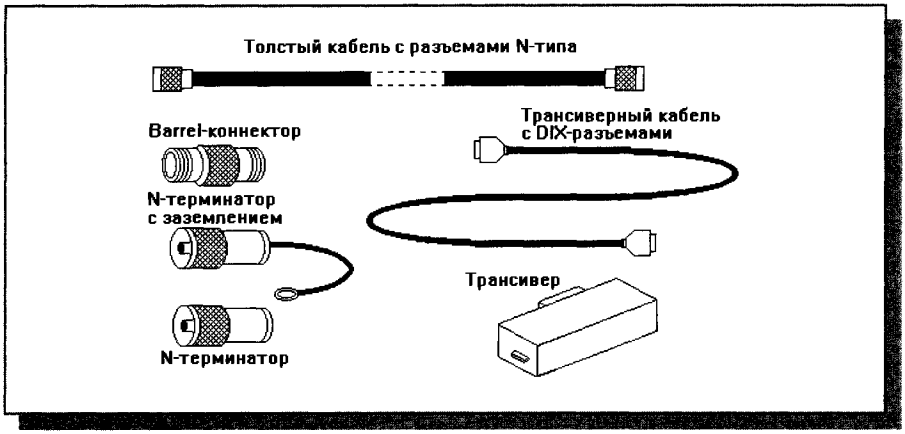



**Рис. 11.1.** Аппаратура 10BASE5

Для соединения кусков толстого коаксиального кабеля между собой, а также терминаторов с таким кабелем используются разъемы N-типа, установка которых довольно сложна и требует специальных инструментов (в противном случае возможны искажения сигналов на стыках). Два разъема N-типа для увеличения длины кабеля могут соединяться с помощью Barrel-коннекторов.

При выполнении сегмента сети на базе толстого кабеля желательно использовать один кусок кабеля или брать все его куски из одной партии одного производителя иначе на стыках разнородных кабелей могут быть искажения сигналов. Если кабель сегмента образуется из нескольких кусков, то с целью снижения отражений сигнала рекомендуется применять куски длиной 23,4 метра, 70,2 метра и 117 метров (с погрешностью 0,5 метра). Никаких ответвлений и разветвлений толстого кабеля не допускается.

На обоих концах кабеля сегмента должны быть установлены 50-омные терминаторы N-типа, один (и только один) из которых надо заземлить.

Толстый кабель никогда не подводят непосредственно к компьютеру сети — это сложно и неудобно для использования, так как компьютеры нельзя будет переместить. Его прокладывают по стене или по полу помещения. Для присоединения сетевых адаптеров к толстому кабелю служат специальные трансиверы (см. рис. 11.2).

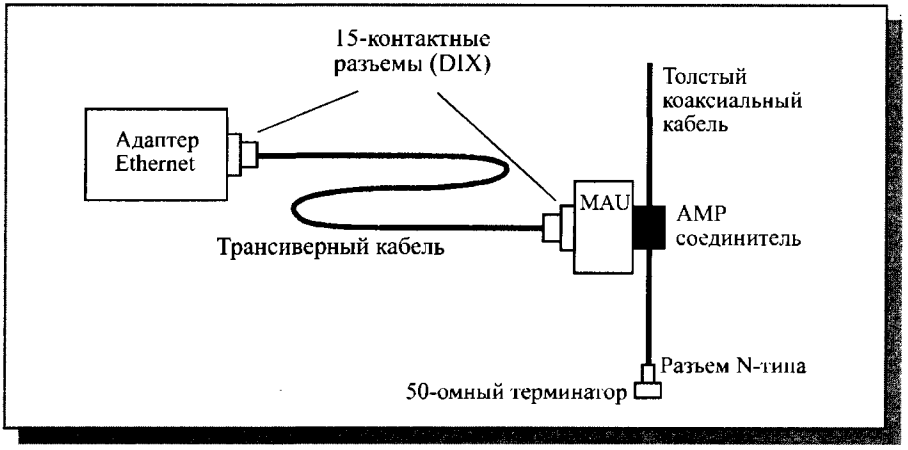



**Рис. 11.2.** Подсоединение адаптера к толстому кабелю

Трансивер (MAU, Medium Attachment Unit – устройство присоединения к среде) устанавливается непосредственно на толстом кабеле и связывается с адаптером трансиверным кабелем.

Для присоединения трансиверов к толстому кабелю чаще всего используются специальные соединительные устройства, предложенные корпорацией AMP, которые не требуют разрезания кабеля в точке присоединения, а просто прокалывают оболочку и изоляцию кабеля и обеспечивают механическое и электрическое соединение как с оплеткой, так и с центральной жилой кабеля. Они носят названия «вампиров». Другой тип соединителя требует разрезания кабеля и установки на оба конца разъемов, поэтому он гораздо менее популярен.

Трансиверный кабель представляет собой гибкий многопроводный кабель диаметром около 1 см, содержащий четыре экранированные витые пары. Длина обычного трансиверного кабеля может достигать 50 метров, а более тонкого и гибкого офисного варианта — 12,5 метров, то есть обеспечивается достаточная свобода перемещения компьютеров. На концах трансиверного кабеля устанавливаются 15-контактные разъемы (DIX-разъемы типа «вилка», DB-15P). Трансиверный кабель называется также AUI–кабелем (Attachment Unit Interface) или Drop–кабелем, спусковым кабелем, а его разъемы – AUI–разъемами. Трансивер работает от внутреннего источника питания компьютера и должен потреблять ток не более 0,5 А от источника +12 В.

Сетевой адаптер, работающий с толстым кабелем, должен иметь внешний 15-контактный AUI-разъем (разъем DIX типа «розетка», DB-15S). Назначение контактов этого разъема приведено в табл. 11.1.

**Таблица 11.1.** Назначение контактов AUI разъема DB15

| Контакт | Назначение |
|---|---|
| 1 | CD экран |
| 2 | CD+ |
| 3 | TX+ |
| 4 | RX экран |
| 5 | RX+ |
| 6 | Земля |
| 7 | Не используется |
| 8 | Не используется |
| 9 | CD- |
| 10 | TX- |
| 11 | TX экран |
| 12 | RX- |
| 13 | Питание (+ 12 В) |
| 14 | Экран питания |
| 15 | Не используется |

Для связи используются три витые экранированные пары проводов, служащие для передачи трех дифференциальных сигналов:

- передаваемая адаптером в сеть информация (TX+,TX- и TX–экран);
- принимаемая из сети в адаптер информация (RX+, RX- и RX–экран);
- сигнал наличия коллизии из трансивера в адаптер (CD+, CD- и CD–экран).

Провод питания также экранируется для уменьшения влияния внешних наводок. Гальваническая развязка в данном случае осуществляется внутри трансивера. Напряжение изоляции между абонентами составляет до 5 киловольт.

Если в структуре сетевого адаптера предусмотрено переключение (тумблерами или перемычками) «Ethernet – Cheapernet», надо переключить его в режим «Ethernet» (то есть 10BASE5). Ведь именно сегмент 10BASE5 считается изначальным стандартным типом Ethernet.

Схема соединения компьютеров сегмента сети на толстом кабеле показана на рис. 11.3.

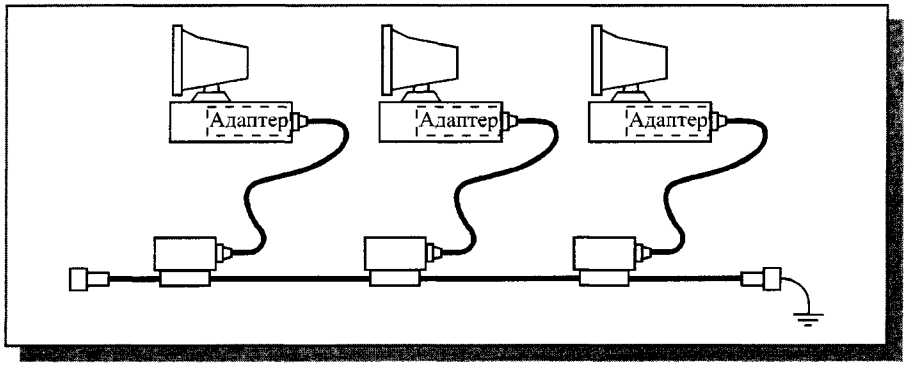



**Рис. 11.3.** Соединение компьютеров сети толстым кабелем

Максимальное количество сегментов при реализации всей сети только на толстом коаксиальном кабеле не должно превышать пяти (общая длина сети – 2,5 километра). Соответственно для соединения пяти сегментов потребуется четыре репитера. При этом должно применяться так называемое правило «5-4-3», то есть не более 5 сегментов, не более 4 репитеров и не более 3 сегментов, к которым могут быть присоединены компьютеры (рис. 11.4).

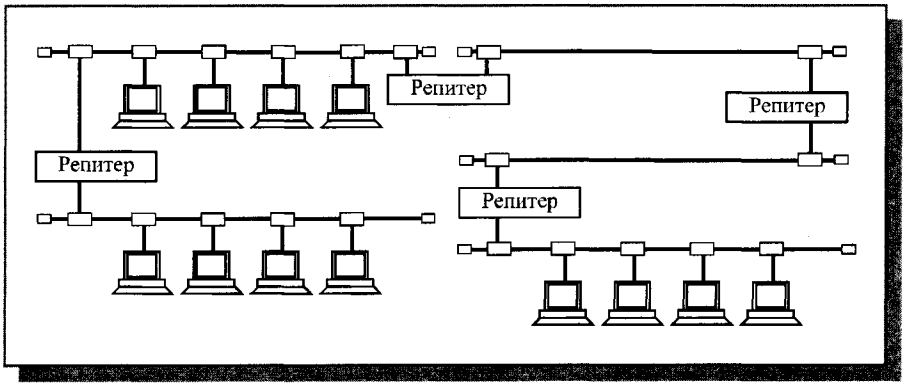



**Рис. 11.4.** Соединение сегментов 10BASE5 по правилу «5-4-3»

Минимальный набор оборудования для односегментной сети на толстом кабеле включает в себя следующие элементы:

- сетевые адаптеры (по числу объединяемых в сеть компьютеров) с AUI–разъемами;
- толстый кабель с разъемами N-типа на концах, общая длина которого достаточна для объединения всех компьютеров сети;

- трансиверные кабели с 15-контактными AUI–разъемами на концах длиной от компьютера до толстого кабеля (по количеству сетевых адаптеров);
- трансиверы (по количеству сетевых адаптеров);
- два Barrel-коннектора N-типа для присоединения терминаторов на концах кабеля;
- один N-терминатор без заземления;
- один N-терминатор с заземлением.

В настоящее время аппаратура 10BASE-5 практически не используется, но в некоторых случаях она еще применяется для организации базовой (Backbone) сети. Доля сетевых адаптеров с AUI–разъемами сейчас не превышает 5%.

## Аппаратура 10BASE2

Стандарт 10BASE2 определяет сегмент Ethernet на основе тонкого коаксиального кабеля с топологией шина длиной до 185 метров (то есть около 200 метров, на это указывает цифра 2 в названии сегмента). Данный тип сегмента появился позже, чем сегмент 10BASE5, как более удобная и дешевая альтернатива классическому варианту Ethernet.

Тонкий коаксиальный кабель отличается от толстого вдвое меньшим диаметром (около 5 мм), значительно большей гибкостью, удобством монтажа, стоимостью (примерно в три раза дешевле толстого). Неудивительно, что сети на его основе получили гораздо большее распространение. Тонкий кабель, как и толстый, имеет волновое сопротивление 50 Ом и требует такого же 50-омного оконечного согласования. Если толстый кабель обязательно должен быть надежно закреплен, например, на стене или на полу помещения, то тонкий кабель вполне может быть проложен навесным монтажом, что позволяет довольно просто перемещать компьютеры в пределах помещения.

Самым большим недостатком тонкого кабеля является меньшая допустимая длина сегмента (до 185 метров). Иногда производители сетевых адаптеров указывают допустимую длину сегмента 200 или даже 300 метров. В последнем случае может оказаться, что такие сетевые адаптеры не способны связываться с адаптерами других изготовителей, так как используют нестандартные уровни сигналов. Наиболее распространенный тип тонкого коаксиального кабеля – это RG-58 A/U. Его электрические параметры (затухание, помехозащищенность) хуже, чем у толстого кабеля, что и определяет меньшую допустимую длину сегмента.

Аппаратура для работы с тонким кабелем (рис. 11.5) гораздо проще, чем в случае толстого кабеля. Помимо сетевых адаптеров требуются только кабели соответствующей длины, разъемы, Т-коннекторы (тройники) и терминаторы (один с заземлением).

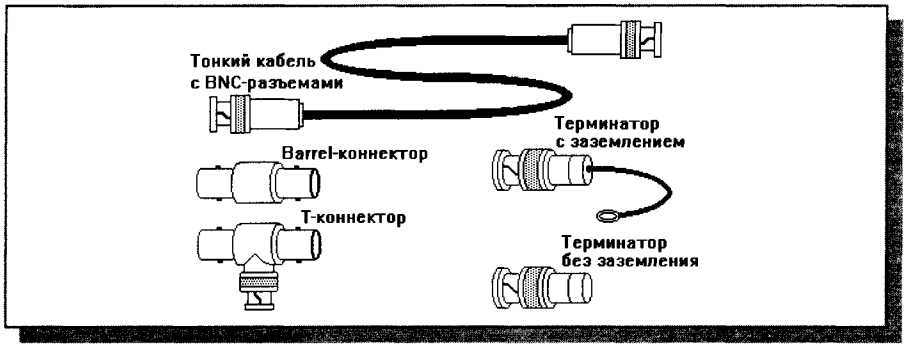



**Рис. 11.5.** Аппаратура 10BASE2

Между каждой парой абонентов прокладывается отдельный кусок кабеля с двумя байонетными разъемами типа BNC на концах. Минимальная длина куска кабеля (минимальное расстояние между абонентами) – 0,5 метра. Общее количество абонентов на одном сегменте не должно превышать 30.

Допускается, хотя и не рекомендуется соединение кусков кабеля между собой с помощью BNC I-коннекторов (Barrel-коннекторов). Разъемы на кабель могут припаиваться, но чаще устанавливаются с помощью специального обжимного инструмента, причем надо следить, чтобы обжимной инструмент соответствовал марке выбранного разъема.

На плате адаптера должен находиться BNC-разъем, к которому присоединяется BNC T-коннектор, связывающий плату с двумя кусками кабеля (рис. 11.6). Гальваническую развязку осуществляет сам адаптер, напряжение изоляции составляет 100–150 вольт, что значительно меньше, чем в случае толстого кабеля. Металлический корпус BNC-разъема гальванически развязан с корпусом компьютера. Соединять их нельзя.

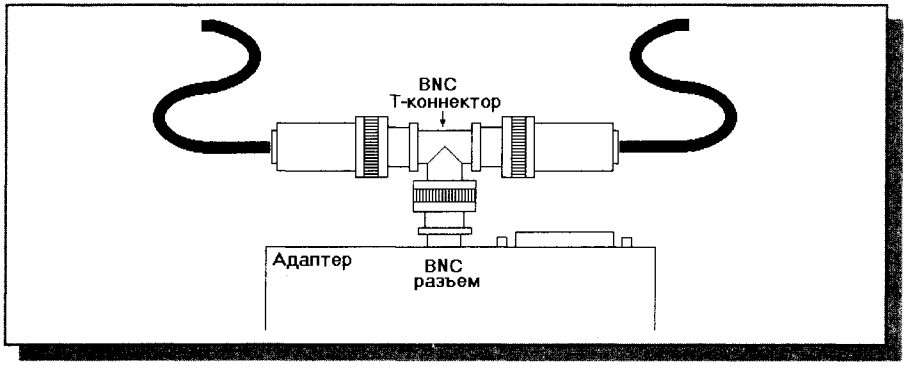



**Рис. 11.6.** Присоединение адаптера к тонкому коаксиальному кабелю

Если в структуре сетевого адаптера предусмотрено переключение режимов (тумблерами или перемычками) «Ethernet – Cheapernet», надо переключить адаптер в режим «Cheapernet» (это распространенное название сегмента 10BASE2 вообще и тонкого коаксиального кабеля в частности).

В принципе допускается включить между разъемом адаптера и BNC Т-коннектором отрезок кабеля и расположить весь соединительный узел (Т-коннектор и два BNC разъема) подальше от адаптера и компьютера. Но стандарт определяет, что длина такого вставленного отрезка кабеля не должна превышать 4 см. Вряд ли кабель такой небольшой длины что-нибудь даст, поэтому лучше все-таки выполнять соединение именно так, как показано на рис. 8.6.

Пример соединения компьютеров в сеть с помощью тонкого кабеля показан на рис. 11.7. Здесь, как и в случае толстого кабеля (10BASE5), реализуется стандартная топология *шина*. На концах кабеля (на разъемы крайних адаптеров) включаются 50-омные терминаторы, один (и только один) из которых необходимо заземлить.

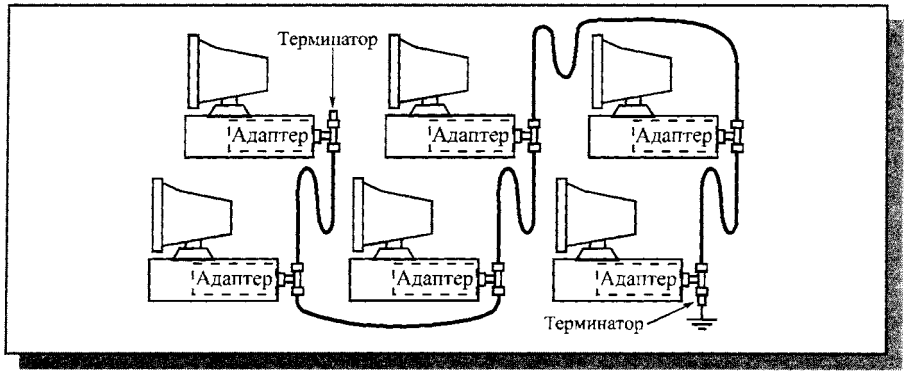



**Рис. 11.7.** Соединение компьютеров сети тонким кабелем

Следует отметить, что разъемы отечественного производства типа СР-50 подходят для соединения с импортными разъемами BNC. Однако совсем небольшое отличие в размерах этих разъемов приводит к тому, что их соединение требует значительных физических усилий, опасных для целости адаптера, так что лучше все-таки придерживаться одного типа разъемов.

При необходимости увеличения длины сети можно использовать репитеры (рис. 11.8). Если вся сеть выполняется на тонком кабеле, то, согласно стандарту, количество сегментов не должно превышать пяти (таким образом, общая длина сети составит 925 метров, потребуется четыре репитера). Как и в случае 10BASE5, необходимо соблюдать правило «5-4-3», то есть только на трех сегментах могут располагаться компьютеры. К одному сегменту может подключаться до 30 абонентов, включая и репитеры.

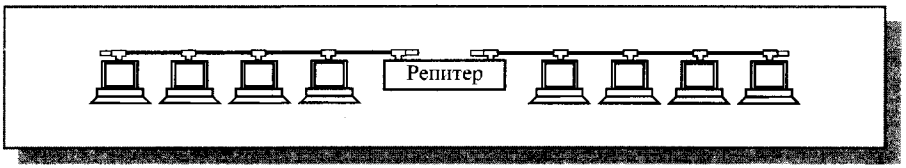



**Рис. 11.8.** Объединение сегментов 10BASE2 с помощью репитеров

Минимальный набор оборудования для односегментной сети на тонком кабеле должен включать в себя следующие элементы:

- сетевые адаптеры (по числу объединяемых в сеть компьютеров);
- отрезки кабеля с BNC-разъемами на обоих концах, общая длина которых достаточна для объединения всех компьютеров;
- BNC T-коннекторы (по числу сетевых адаптеров);
- один BNC–терминатор без заземления;
- один BNC–терминатор с заземлением.

Если сеть создается из нескольких сегментов с использованием репитеров и концентраторов, то надо учитывать, что некоторые концентраторы имеют встроенные 50-омные терминаторы (иногда – отключаемые), что упрощает проблемы согласования. Если же таких встроенных терминаторов нет, то надо использовать внешние терминаторы на каждом конце сегмента, и тогда перечисленная аппаратура будет требоваться для каждого сегмента.

В принципе реализация какого-то сегмента сети на базе отрезков кабелей разного типа (толстого и тонкого) возможна. В этом случае для расчета допустимой длины сегмента кабеля рекомендуется пользоваться следующим соотношением:

$$(3{,}28 \times L_{тн}) + L_{тл} < 500 \text{ м},$$

где $L_{тн}$ и $L_{тл}$ – соответственно длина тонкого и толстого кабеля. Но лучше все-таки использовать точный расчет работоспособности сети, который описан в главе 10.

До недавнего времени аппаратура 10BASE2 была самой популярной. Кабели, разъемы, адаптеры для нее выпускались наибольшим количеством производителей, что приводило к регулярному снижению цен. Но сейчас ее все больше вытесняет 10BASE-T, порой совершенно неоправданно, ведь для небольших сетей Ethernet сегмент 10BASE2 обычно представляет собой более дешевое и удобное решение. Правда, 10BASE2 не имеет таких возможностей модернизации, как 10BASE-T.

## Аппаратура 10BASE-T

Стандарт 10BASE-T определяет сегмент Ethernet на основе неэкранированных витых пар (UTP) категории 3 и выше с топологией пассивная звезда (Twisted-Pair Ethernet). Это самый поздний стандарт Ethernet на ос-

нове электрического кабеля (развивается с 1990 года). Он считается перспективным, и практически вытеснил сегменты 10BASE5 и 10BASE2.

Данный тип сегмента Ethernet имеет все преимущества и недостатки пассивной звезды.

С одной стороны, он заметно дороже шинного сегмента 10BASE2, так как требует обязательного применения концентратора (хаба). Суммарное количество кабеля, необходимого для объединения такого же количества компьютеров, оказывается гораздо больше, чем в случае шины. С другой стороны, обрыв кабеля не приводит к отказу всей сети, монтаж, а также диагностика неисправности сети проще. Кроме того, важно и то, что к каждому компьютеру подводится один кабель, а не два, как в случае 10BASE2, не нужно применять также внешние терминаторы и заземлять сеть.

Однако главное преимущество 10BASE-T в том, что только данный стандарт благодаря использованию передачи «точка-точка» позволяет выполнить плавный перевод сети Ethernet в сеть Fast Ethernet. Подробнее об этом – в конце данной главы.

В сегменте 10BASE-T передача сигналов осуществляется по двум витым парам проводов, каждая из которых передает только в одну сторону (одна пара – передающая, другая – принимающая). Кабелем, содержащим такие двойные витые пары, каждый из абонентов сети присоединяется к концентратору (хабу), использование которого в данном случае в отличие от рассмотренных ранее обязательно. Концентратор производит смешение сигналов от абонентов для реализации метода доступа CSMA/CD, то есть в данном случае реализуется топология пассивная «звезда» (рис. 11.9), которая, как уже отмечалось, равноценна топологии «шина».

Использование двух встречно направленных витых пар упрощает задачу детектирования коллизий. Коллизия детектируется тогда, когда име-

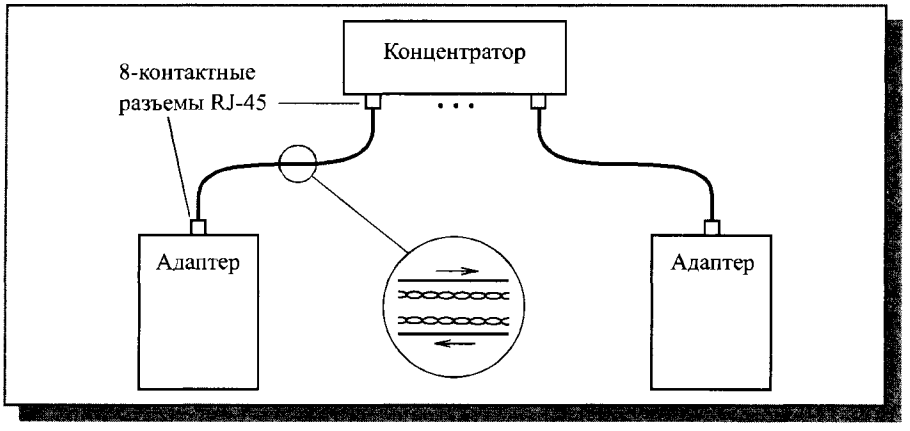



**Рис. 11.9.** Подключения абонентов 10BASE-T с помощью витой пары

ется входной сигнал во время передачи.

Возможно соединение нескольких концентраторов между собой для получения древовидной структуры. Каждый концентратор помимо обычных портов для присоединения абонентов содержит порт расширения «UpLink», который служит для присоединения к концентратору более высокого уровня. Но концентраторы могут соединяться между собой и через обычные порты (рис. 11.10). Общее правило выбора конфигурации в данном случае выглядит так: между двумя абонентами не может быть больше четырех концентраторов.

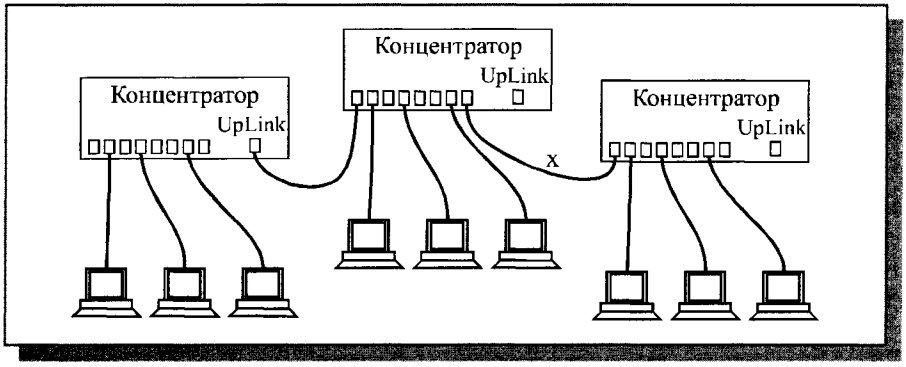



**Рис. 11.10.** Соединение абонентов 10BASE-T с помощью концентраторов

Гальваническая развязка осуществляется аппаратурой адаптеров и имеет типовое напряжение изоляции 100 В, что соответствует параметрам 10BASE2.

Длина соединительного кабеля между адаптером и концентратором не должна превышать 100 метров (минимальная длина – 2,5 м), что часто накладывает существенные ограничения на размещение компьютеров. Кабель применяется гибкий, диаметром около 6 мм. Из четырех витых пар, входящих в кабель, используются только две. Наиболее распространенный тип кабеля – это кабель EIA/TIA категории 3. Но в настоящее время рекомендуется использовать более качественный кабель категории 5 (или даже выше), который позволяет без проблем переходить на Fast Ethernet. Популярен кабель марки AWG 22-26.

Кабели присоединяются к адаптеру и к концентратору 8-контактными разъемами типа RJ-45 (рис. 11.11), внешне похожими на обычные телефонные разъемы, в которых используются только четыре контакта. Назначение контактов разъема приведено в табл. 11.2. Провода передающей пары обозначены TX+ и TX-, а приемной пары – RX+ и RX-.

Монтаж и обслуживание неэкранированных кабелей с витыми парами (UTP-кабелей) гораздо проще, чем коаксиальных кабелей, так как они

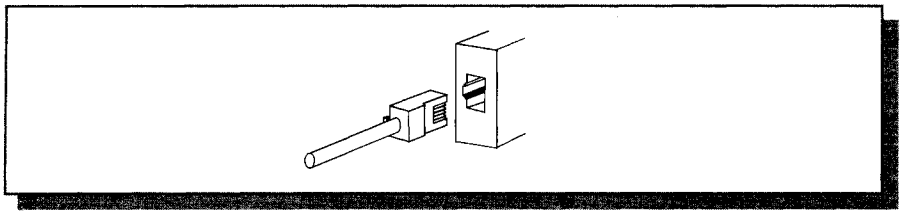


**Рис. 11.11.** Разъем RJ-45

не имеют металлической оплетки. UTP-кабели стоят примерно вдвое дешевле, чем тонкий коаксиальный кабель, но при этом надо учитывать, что в случае топологии пассивная «звезда» кабеля обычно требуется гораздо больше, чем при топологии «шина».

Передача по витым парам ведется дифференциальными сигналами с целью увеличения помехоустойчивости сети, то есть ни один из проводов этих витых пар не заземляется. В отличие от сегментов с коаксиальным кабелем пользователю не надо ни использовать внешние терминаторы, ни заземлять кабель – достаточно всего лишь обеспечить заземление компьютеров сети.

В сети 10BASE-T применяются два вида соединения проводов кабеля (рис. 11.12). Если надо объединить в сеть всего два компьютера, то можно обойтись вообще без концентратора, применив так называемый *перекрестный кабель* (crossover cable), который соединяет передающие контакты одного разъема RJ-45 с приемными контактами другого разъема RJ-45 и наоборот. А для связи компьютеров с концентратором обычно используется *прямой кабель* (direct cable), в котором соединяются между собой одинаковые контакты обоих разъемов. На такой прямой кабель рассчитано большинство концентраторов. Надо, правда, учитывать, что иногда перекрестное соединение имеется внутри порта концентратора

**Таблица 11.2.** Назначение контактов разъема RJ-45 сегмента 10BASE-T

| Контакт | Назначение | Цвет провода |
|---|---|---|
| 1 | TX+ | Белый/оранжевый |
| 2 | TX- | Оранжевый/белый |
| 3 | RX+ | Белый/зеленый |
| 4 | Не используется | |
| 5 | Не используется | |
| 6 | RX- | Зеленый/белый |
| 7 | Не используется | |
| 8 | Не используется | |

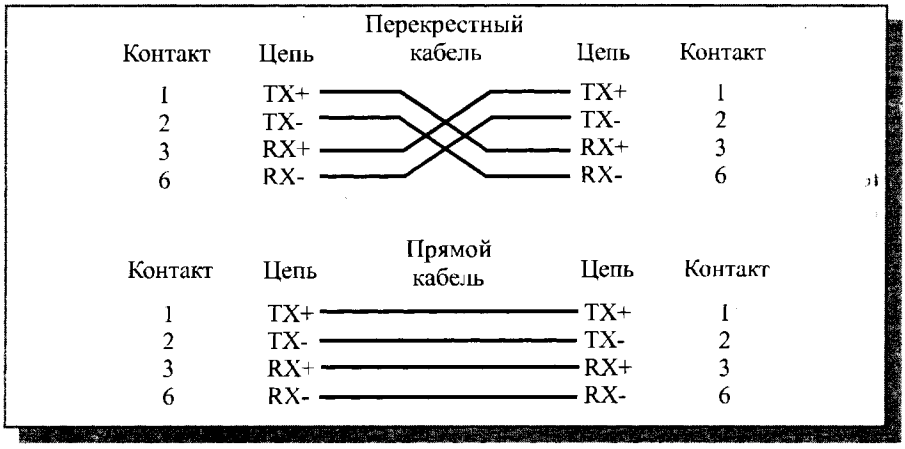



**Рис. 11.12.** Соединение проводов прямого и перекрестного кабелей сегмента 10BASE-T

(стандарт рекомендует помечать такой порт буквой «X»), поэтому, выполняя соединения в сети, следует быть очень аккуратным.

Необходимо также принимать во внимание и то, что кабель, соединяющий между собой два концентратора через обычные порты, должен быть перекрестным (на рис. 11.10 он помечен буквой «x»). А вот кабель, соединяющий специальный расширительный порт одного концентратора (UpLink) с нормальным портом другого концентратора, должен быть прямым.

Стоит отметить, такую особенность адаптеров и концентраторов, рассчитанных на работу с витой парой, как наличие в них встроенного контроля правильности соединения сети. В отсутствии передачи информации они периодически (раз в 16,8 мс) передают тестовые импульсы (NLP – Normal Link Pulse), по наличию которых на приемном конце определяется целостность кабеля. Для визуального контроля правильности соединений предусмотрены специальные светодиоды «Link», которые горят при правильном соединении аппаратуры. Это очень удобно и выгодно отличает сегмент 10BASE-T от 10BASE2 и 10BASE5, где подобная функция из-за шинной структуры в принципе не может быть предусмотрена, так как в них все абоненты соединены параллельно.

Минимальный набор оборудования для сети на витой паре включает в себя следующие элементы:

- сетевые адаптеры (по числу объединяемых в сеть компьютеров), имеющие UTP-разъемы RJ-45;
- отрезки кабеля с разъемами RJ-45 на обоих концах (по числу объединяемых компьютеров);
- один концентратор, имеющий столько UTP-портов с разъемами RJ-45, сколько необходимо объединить компьютеров.

## Аппаратура 10BASE-FL

Широко использовать оптоволоконный кабель в Ethernet начали сравнительно недавно. Его применение позволило сразу же значительно увеличить допустимую длину сегмента и помехоустойчивость передачи. Немаловажна также и полная гальваническая развязка компьютеров сети, которая достигается здесь без всякой дополнительной аппаратуры, в силу специфики среды передачи. Еще одно преимущество оптоволоконных кабелей состоит в возможности постепенного перехода на Fast Ethernet без замены кабелей, так как пропускная способность оптоволокна позволяет достигнуть не только 100 Мбит/с, но и более высоких скоростей передачи.

Передача информации в данном случае идет по двум оптоволоконным кабелям, передающим сигналы в разные стороны (как и в 10BASE-T). Иногда используются двухпроводные оптоволоконные кабели, содержащие два кабеля в общей внешней оболочке, но чаще – два одиночных кабеля. Вопреки распространенному мнению, стоимость оптоволоконного кабеля не слишком высока (она близка к стоимости тонкого коаксиального кабеля). Правда, в целом аппаратура в данном случае оказывается заметно дороже, так как требует использования дорогих оптоволоконных трансиверов.

Аппаратура 10BASE-FL имеет сходство как с аппаратурой 10BASE5 (здесь тоже могут применяться внешние трансиверы, соединенные с адаптером трансиверным кабелем), так и с аппаратурой 10BASE-T (здесь также применяются топология пассивная «звезда» и два разнонаправленных кабеля). Схема соединения сетевого адаптера и концентратора показана на рис. 11.13.

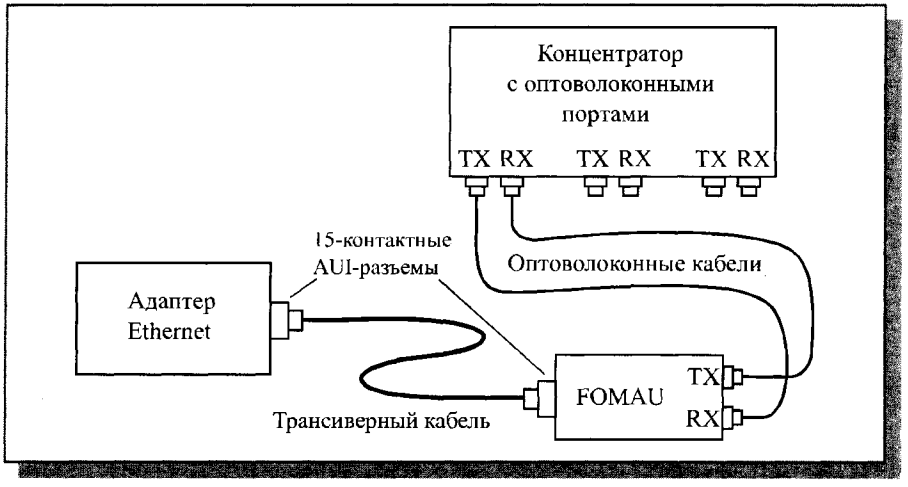



**Рис. 11.13.** Соединение адаптера и концентратора в 10BASE-FL

Оптоволоконный трансивер называется FOMAU (Fiber Optic MAU). Он выполняет все функции обычного трансивера (MAU), но, кроме того, преобразует электрический сигнал в оптический при передаче и обратно при приеме. FOMAU также формирует и контролирует сигнал целостности линии связи, передаваемый в паузах между пакетами. Целостность линии связи, как и в случае 10BASE-T, индицируется светодиодами «Link» и определяется по наличию между передаваемыми пакетами сигнала «Idle» частотой 1 МГц. Для присоединения трансивера к адаптеру применяется стандартный AUI-кабель, такой же, как и в случае 10BASE5, но длина его не должна превышать 25 метров.

Имеются также сетевые адаптеры со встроенными трансиверами FOMAU, которые имеют только внешние оптоволоконные разъемы и не нуждаются в трансиверных кабелях.

Длина оптоволоконных кабелей, соединяющих трансивер и концентратор, может достигать 2 километров без применения каких бы то ни было ретрансляторов. Таким образом, возможно объединение в локальную сеть компьютеров, находящихся в разных зданиях, разнесенных территориально.

Первоначально оптоволоконная связь применялась преимущественно для связи между репитерами. Первый стандарт FOIRL (Fiber Optic Inter-Repeater Link), разработанный в начале 80-х годов XX века, предполагал как раз связь между двумя репитерами на расстояние до 1000 метров. Затем были разработаны оптоволоконные трансиверы для подключения к репитеру отдельных компьютеров и стандарт 10BASE-F, включающий в себя следующие три типа сегментов:

- 10BASE-FL (Fiber Link) – заменил старый стандарт FOIRL и наиболее распространен в настоящее время. Он обеспечивает связь между двумя компьютерами, между двумя репитерами или между компьютером и репитером. Максимальное расстояние – до 2000 метров.
- 10BASE-FB (Fiber Backbone) – стандарт предназначен для синхронного обмена между несколькими репитерами с целью образования базовой распределенной репитерной системы. Максимальное расстояние – до 2000 метров. Совместим со стандартом 10BASE-FL, однако широкого распространения не получил.
- 10BASE-FP (Fiber Passive) – предназначен для объединения в топологию пассивная «звезда» без использования репитеров до 33 компьютеров (для этого применяются специальные пассивные оптические разветвители). Максимальное расстояние от компьютера до разветвителя – до 500 метров. Такое значительное сокращение допустимого расстояния объясняется сильным затуханием в пассивном оптическом разветвителе. Стандарт несовместим с 10BASE-FL. Широкого распространения этот тип сегмента также не получил.

Таким образом, сейчас реально используется только стандарт 10BASE-FL.

В 10BASE-FL применяется мультимодовый кабель и свет с длиной волны 850 нанометров, однако имеется аппаратура и для использования одномодового кабеля (с предельной длиной до 5 км).

Суммарные оптические потери в сегменте (как в кабеле, так и в разъемах) не должны превышать 12,5 дБ. При этом потери в кабеле составляют около 5 дБ на километр длины кабеля, а потери в разъеме – от 0,5 до 2,0 дБ (эта величина сильно зависит от качества установки разъема). Только при таких величинах потерь можно гарантировать устойчивую связь на предельной длине кабеля. На практике лучше не рисковать и брать длину кабеля процентов на десять меньше предельной (что и рекомендуется стандартом).

Стандартный оптоволоконный кабель 10BASE-FL должен иметь на обоих концах оптоволоконные байонетные ST-разъемы, показанные на рис. 11.14 (стандарт BFOC/2.5). Присоединение этого разъема к трансиверу или концентратору не сложнее, чем BNC-разъема в сети 10BASE2 (см. рис.11.5).

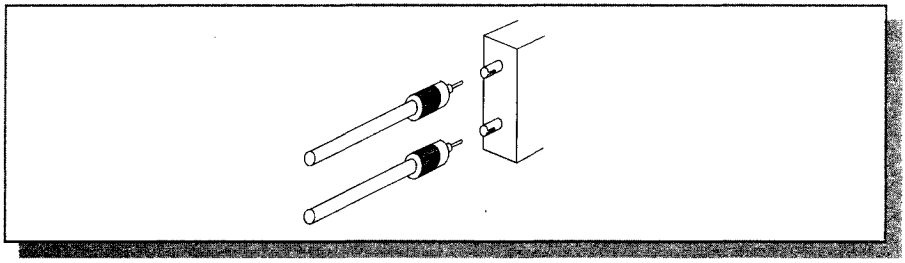


**Рис. 11.14.** ST-разъем для оптоволоконного кабеля

Используются также оптоволоконные разъемы типа SC, присоединяемые подобно RJ-45 путем простого вставления в гнездо. Разъемы SC обычно жестко соединены по два для двух кабелей (рис. 11.15).

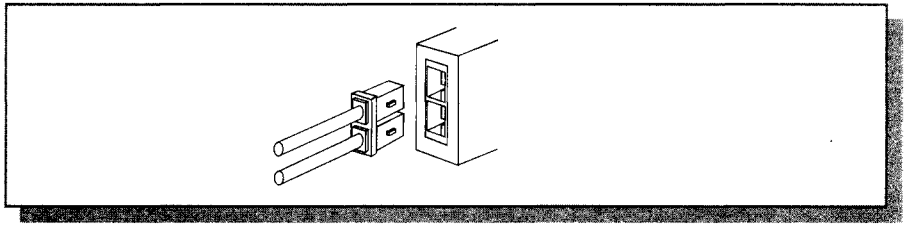


**Рис. 11.15.** SC-разъем для оптоволоконного кабеля

Существуют также разъемы типа MIC FDDI, аналогичные разъемам SC, вставляемым в гнездо. Правда, они используются реже. При покупке

оборудования 10BASE-FL надо следить за соответствием разъемов, установленных на кабеле, и ответных разъемов трансиверов или концентраторов.

Пример соединения компьютеров с помощью оптоволоконного кабеля в топологию пассивная «звезда» показан на рис. 11.16.

Как и в случае 10BASE-T, несколько концентраторов могут объединяться между собой для получения древовидной топологии. Вообще, наиболее часто сегмент 10BASE-FL как раз и используется для соединения двух концентраторов. А к концентраторам подключаются компьютеры по стандарту 10BASE-T. Таким образом, удается совместить достоинства обоих сегментов – низкую стоимость 10BASE-T и большие расстояния 10BASE-FL.

Минимальный набор оборудования для соединения оптоволоконным кабелем двух компьютеров включает в себя следующие элементы:

- два сетевых адаптера с трансиверными разъемами;
- два оптоволоконных трансивера (FOMAU);
- два трансиверных кабеля;
- два оптоволоконных кабеля с ST-разъемами (или с SC– или с MIC–разъемами) на концах.

Если требуется соединить больше двух компьютеров, то надо использовать концентратор, имеющий оптоволоконные порты. Каждый компьютер снабжается своим трансивером и трансиверным кабелем, а также двумя оптоволоконными кабелями с соответствующими разъемами для подключения к концентратору.

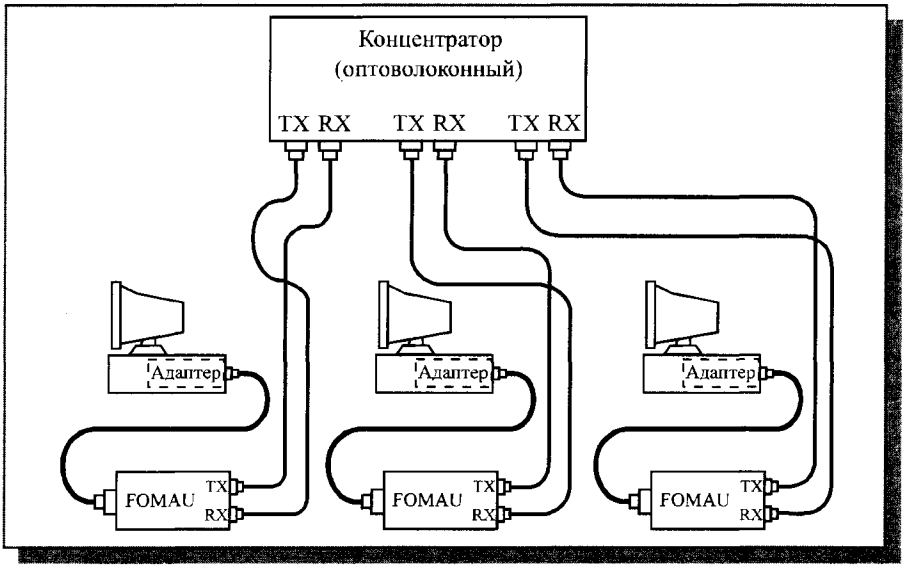



**Рис. 11.16.** Объединение компьютеров в сеть по стандарту 10BASE-FL

# Лекция 12. Стандартные сегменты Fast Ethernet

**В этой лекции говорится о стандартных сегментах сети Fast Ethernet, их топологиях, аппаратуре, кабелях, разъемах, достоинствах и недостатках, а также о методе автоматического согласования скоростей передачи.**

**Ключевые слова:** 100BASE-TX, 100BASE-T4, 100BASE-FX, 8B/6T, Auto-Negotiation, FLP, NLP, LCW.

## Аппаратура 100BASE-TX

Стандарт Fast Ethernet IEEE 802.3u появился значительно позже стандарта Ethernet – в 1995 году. Его разработка в первую очередь была связана с требованием повышения скорости передачи информации. Однако переход с Ethernet на Fast Ethernet позволяет не только повысить скорость передачи, но и существенно отодвинуть границу перегрузки сети (что обычно гораздо важнее). Поэтому популярность Fast Ethernet постоянно растет.

Вместе с тем надо учитывать, что стандартные сегменты Fast Ethernet имеют свои особенности и недостатки, которые далеко не очевидны, но которые обязательно надо учитывать. Создатели Fast Ethernet сделали все возможное для облегчения перехода на новую скорость, однако, в каком-то смысле Fast Ethernet – это уже другая, новая сеть.

Если сравнивать набор стандартных сегментов Ethernet и Fast Ethernet, то главное отличие – полный отказ в Fast Ethernet от шинных сегментов и коаксиального кабеля. Остаются только сегменты на витой паре и оптоволоконные сегменты.

Стандарт 100BASE-TX определяет сеть с топологией пассивная *звезда* и использованием сдвоенной витой пары.

Схема объединения компьютеров в сеть 100BASE-TX практически ничем не отличается от схемы по стандарту 10BASE-T (рис. 12.1). Однако, в этом случае необходимо применение кабелей с неэкранированными витыми парами (UTP) категории 5 или выше, что связано с требуемой пропускной способностью кабеля. В настоящее время это самый популярный тип сети Fast Ethernet.

Для присоединения кабелей так же, как и в случае 10BASE-T используются 8-контактные разъемы типа RJ-45. Длина кабеля так же не может превышать 100 метров (стандарт, правда, рекомендует ограничиваться длиной сегмента в 90 метров, чтобы иметь 10-процентный запас). Так же используется топология пассивная *звезда* с концентратором в центре. Только сетевые адаптеры должны быть Fast Ethernet, и концентратор должен быть рассчитан на подключение сегментов 100BASE-TX. Именно

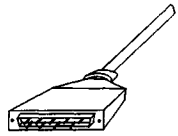


**Рис. 12.2.** Разъем DB-9

– 150 Ом). В этом случае должен применяться 9-контактный экранирован ный разъем DB-9, он же разъем STP IBM типа 1 (рис. 12.2), такой же, как сети Token-Ring. Назначение контактов этого разъема приведено в табл. 12.

**Таблица 12.2.** Назначение контактов разъема DB9

| Контакт | Назначение | Цвет провода |
|---|---|---|
| 1 | RX+ | Оранжевый |
| 2 | Не используется | |
| 3 | Не используется | |
| 4 | Не используется | |
| 5 | TX+ | Красный |
| 6 | RX– | Черный |
| 7 | Не используется | |
| 8 | Не используется | |
| 9 | TX– | Зеленый |

Как и в случае 10BASE-T, в сети 100BASE-TX могут использоватьс два типа кабеля: прямой и перекрестный (рис. 12.3). Для соединения дву компьютеров без применения концентраторов используется стандартны перекрестный (crossover) кабель. А для связи компьютера с концентрато ром применяется прямой (direct) кабель с соединенными между собо одинаковыми контактами разъемов. Если перекрестное соединение пре дусмотрено внутри концентратора, то соответствующий порт его долже быть помечен буквой «X».Здесь все точно так же, как и в случае 10BASE-

Для контроля целостности сети в 100BASE-TX предусмотрена пере дача в интервалах между сетевыми пакетами специальных сигналов (FL – Fast Link Pulse). Но в отличие от 10BASE-T выполняют также функци автоматического согласования скорости передачи аппаратных средст (Auto-Negotiation). Об этом автоматическом согласовании будет расска зано в разделе «Автоматическое определение типа сети».

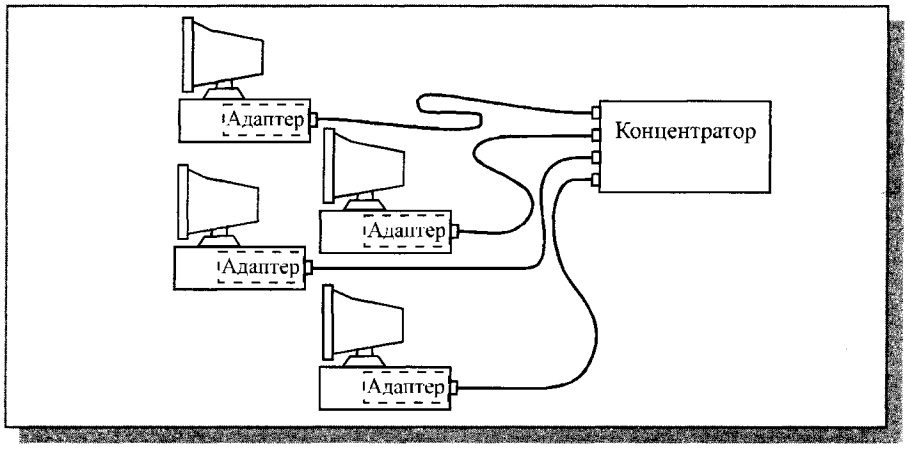



**Рис. 12.1.** Схема объединения компьютеров по стандарту 100BASE-TX

поэтому рекомендуется даже при установке сети 10BASE-T прокладывать кабель категории 5.

Из восьми контактов разъема RJ-45 используется только 4 контакта (табл. 12.1): два для передачи информации (TX+ и TX-) и два для приема информации (RX+ и RX-). Передача производится дифференциальными сигналами. Для передачи используется код 4B/5B, такой же, как в сети FDDI, что позволяет снизить частоту изменения сигналов по сравнению с манчестерским кодом. Это уже серьезный шаг в сторону от первоначального стандарта IEEE 802.3.

Стандарт предусматривает также возможность применения экранированного кабеля с двумя витыми парами проводов (волновое сопротивление

**Таблица 12.1.** Назначение контактов разъема типа RJ-45

| Контакт | Назначение | Цвет провода |
|---|---|---|
| 1 | TX+ | Белый/оранжевый |
| 2 | TX- | Оранжевый/белый |
| 3 | RX+ | Белый/зеленый |
| 4 | Не используется | |
| 5 | Не используется | |
| 6 | RX- | Зеленый/белый |
| 7 | Не используется | |
| 8 | Не используется | |

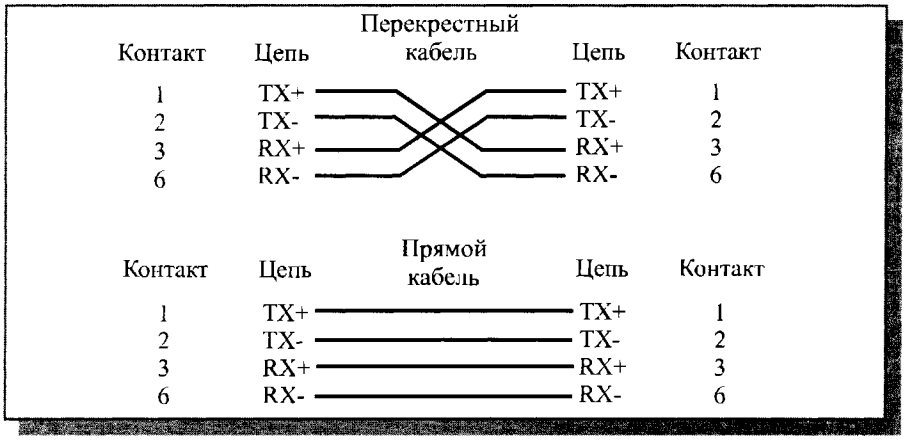



**Рис. 12.3.** Прямой и перекрестный кабели, применяемые в сегменте 100BASE-TX

## Аппаратура 100BASE-T4

Основное отличие аппаратуры 100BASE-T4 от 100BASE-TX состоит в том, что передача производится не по двум, а по четырем неэкранированным витым парам (UTP). При этом кабель может быть менее качественным, чем в случае 100BASE-TX (категории 3, 4 или 5). Принятая в 100BASE-T4 система кодирования сигналов обеспечивает ту же самую скорость 100 Мбит/с на любом из этих кабелей, хотя стандарт рекомендует, если есть такая возможность, все-таки использовать кабель категории 5.

Схема объединения компьютеров в сеть ничем не отличается от 100BASE-TX (рис. 12.1). Компьютеры присоединяются к концентратору по схеме пассивной звезды. Длина кабелей точно так же не может превышать 100 метров (стандарт и в этом случае рекомендует ограничиваться 90 метрами для 10-процентного запаса).

Как и в случае 100BASE-TX, для подключения сетевого кабеля к адаптеру (трансиверу) и к концентратору используются 8-контактные разъемы типа RJ-45. Но в данном случае задействованы уже все 8 контактов разъема. Назначение контактов разъемов представлено в таблице 12.3.

Обмен данными идет по одной передающей витой паре, по одной приемной витой паре и по двум двунаправленным витым парам с использованием трехуровневых дифференциальных сигналов.

Для связи двух компьютеров без применения концентраторов используется перекрестный кабель. В обычном же прямом кабеле, применяемом для связи компьютера с концентратором, соединены одноименные контакты обоих разъемов. Схемы кабелей приведены на рис 12.4. Если перекрестное соединение предусмотрено внутри концентратора, то

**Таблица 12.3.** Назначение контактов разъема типа RJ-45 для сегмента 100BASE-T4

| Контакт | Назначение | Цвет провода |
|---|---|---|
| 1 | TX_D1+ | Белый/оранжевый |
| 2 | TX_D1– | Оранжевый/белый |
| 3 | RX_D2+ | Белый/зеленый |
| 4 | BI_D3+ | Голубой/белый |
| 5 | BI_D3– | Белый/голубой |
| 6 | RX_D2– | Зеленый/белый |
| 7 | BI_D4+ | Белый/коричневый |
| 8 | BI_D4– | Коричневый/белый |

TX – передача данных, RX – прием данных,
BI – двунаправленная передача

соответствующий порт должен помечаться буквой «X». Здесь все точно так же, как в случае 100BASE-TX и 10BASE-T.

Для реализации передачи информации со скоростью 100 Мбит/с по кабелю с малой полосой пропускания (категории 3) в сегменте 100BASE-

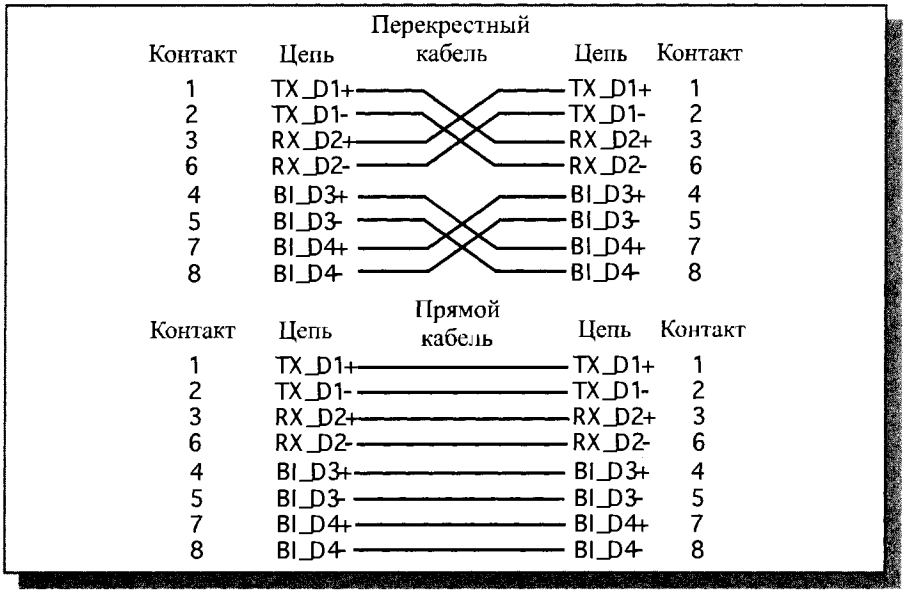



**Рис. 12.4.** Прямой и перекрестный кабель сети 100BASE-T4

T4 используется оригинальный принцип кодирования информации, называющийся 8B/6T. Его идея состоит в том, что 8 бит, которые надо передать, преобразуются в 6 тернарных (трехуровневых с уровнями -3,5 В, +3,5 В и 0 В) сигналов, которые затем передаются за два такта по трем витым парам. При шестиразрядном трехзначном коде общее число возможных состояний равно $3^6 = 729$, что больше, чем $2^8 = 256$, то есть никаких проблем из-за уменьшения количества разрядов не возникает. В результате по каждой витой паре передается информация со скоростью 25 Мбит/с, то есть требуется полоса пропускания всего 12,5 МГц (рис. 12.5). Дополнительно сигналы, передаваемые в кабель, кодируются по методу MLT-3.

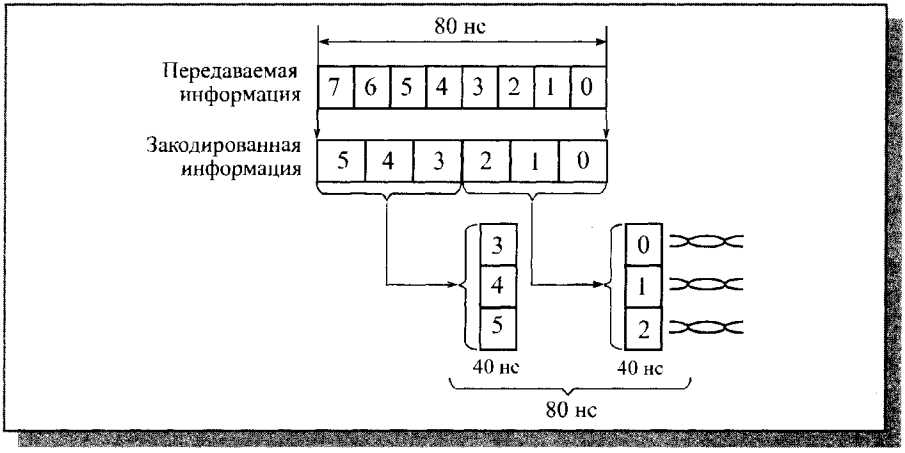



**Рис. 12.5.** Кодирование информации 8B/6T в сегменте 100BASE-T4

Для передачи информации одновременно используются две двунаправленные витые пары (BI_D3 и BI_D4) и одна однонаправленная (TX_D1 или RX_D2). Четвертая витая пара, не участвующая в передаче информации (TX_D1 или RX_D2), применяется для обнаружения коллизий (рис. 12.6).

Для контроля целостности сети в 100BASE-T4 также предусмотрена передача специального сигнала FLP между сетевыми пакетами. Наличие связи индицируется светодиодами «Link». Сигналы FLP также используются для автоматического согласования скоростей передачи (см. раздел «Автоматическое определение типа сети»).

## Аппаратура 100BASE-FX

Применение оптоволоконного кабеля в сегменте 100BASE-FX позволяет существенно увеличить протяженность сети, а также избавиться от электрических наводок и повысить секретность передаваемой информации.

Аппаратура 100BASE-FX очень близка к аппаратуре 10BASE-FL. Точно так же здесь используется топология пассивная «звезда» с подклю-

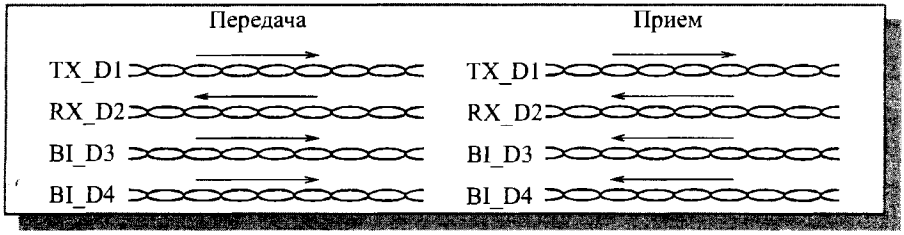



**Рис. 12.6.** Использование линий связи при передаче и приеме

чением компьютеров к концентратору с помощью двух разнонаправленных оптоволоконных кабелей (рис. 12.7).

Между сетевыми адаптерами и кабелями возможно включение выносных трансиверов. Как и в случае сегмента 10BASE-FL, оптоволоконные кабели подключаются к адаптеру (трансиверу) и к концентратору с помощью разъемов типа SC, ST или FDDI. Для присоединения разъемов SC и FDDI достаточно просто вставить их в гнездо, а разъемы ST имеют байонетный механизм.

Максимальная длина кабеля между компьютером и концентратором составляет 412 метров, причем это ограничение определяется не качеством кабеля, а установленными временными соотношениями. Согласно стандарту, применяется мультимодовый или одномодовый кабель с длиной волны света 1,35 мкм. В последнем случае потери мощности сигнала в сегменте (в кабеле и разъемах) не должны превышать 11 дБ. При этом надо учитывать,

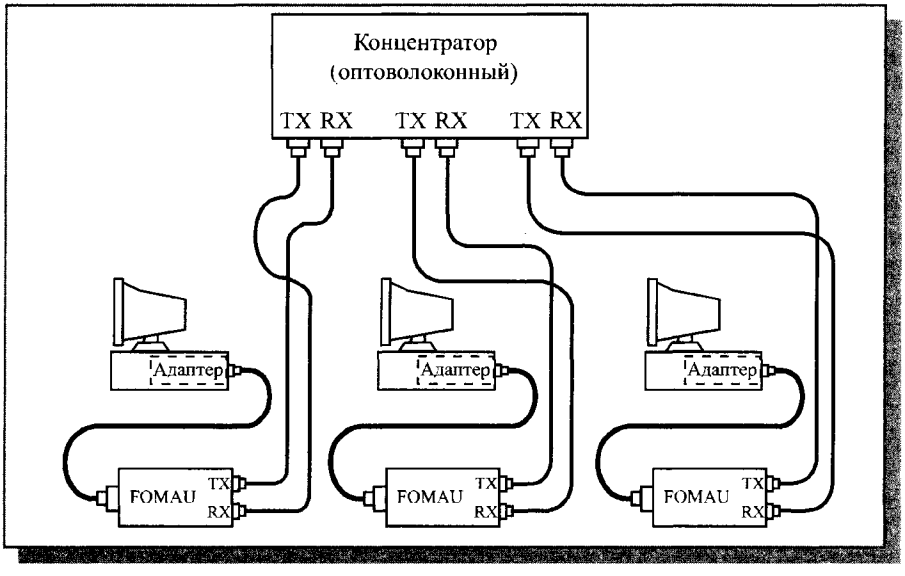



**Рис. 12.7.** Подключение компьютеров к сети 100BASE-FX

что потери в кабеле составляют 1–2 дБ на километр длины, а потери в разъеме – от 0,5 до 2 дБ (при условии, что разъем установлен качественно).

Как и в других сегментах Fast Ethernet, в 100BASE-FX предусмотрен контроль целостности сети, для чего в промежутках между сетевыми пакетами по кабелю передается специальный сигнал. Целостность сети индицируется светодиодами «Link».

Используемый метод кодирования – 4B/5B (как и в сегменте 100BASE-TX), что позволяет довольно просто осуществлять сопряжение этих двух сегментов (иногда они даже объединяются в единый стандарт 100BASE-X). Дополнительное кодирование – NRZI.

## Автоматическое определение типа сети (Auto-Negotiation)

Функция автоматического определения типа сети (или скорости передачи), предусмотренная стандартом Ethernet, не является обязательной. Однако ее реализация в сетевых адаптерах и концентраторах позволяет существенно облегчить жизнь пользователям сети. Особенно это важно на современном этапе, когда широко применяются как ранняя версия Ethernet со скоростью обмена 10 Мбит/с, так и более поздняя версия Fast Ethernet со скоростью 100 Мбит/с.

Функция автодиалога или автосогласования (так можно перевести Auto-Negotiation) позволяет адаптерам, в которых предусмотрено переключение скорости передачи, автоматически подстраиваться под скорость обмена в сети, а концентраторам, в которых предусмотрен автодиалог, самим определять скорость передачи адаптеров, подключенных к их портам. При этом пользователь сети не должен следить за тем, на какую скорость обмена настроена его аппаратура: система сама выберет максимально возможную скорость.

Сразу следует отметить, что режим автодиалога применяется только в сетях на основе сегментов, использующих витые пары: 10BASE-T, 100BASE-TX и 100BASE-T4. Для сегментов на базе коаксиального кабеля и оптоволоконного кабеля автодиалог не предусмотрен. Шинные сегменты на коаксиальном кабеле не дают возможности двухточечной связи, поэтому в них невозможно попарное согласование абонентов. А в оптоволоконных сегментах применяется другая система служебных сигналов, передаваемых между пакетами.

Автодиалог основан на использовании сигналов, передаваемых в Fast Ethernet, которые называются FLP (Fast Link Pulse) по аналогии с сигналами NLP (Normal Link Pulse), применяемыми в сегментах 10BASE-T. Так же, как и NLP, сигналы FLP начинают вырабатываться с включением питания соответствующей аппаратуры (адаптера или концентратора) и формируют-

ся в паузах между передаваемыми сетевыми пакетами, поэтому они никак не влияют на загрузку сети. Именно сигналы FLP и передают информацию о возможностях подключенной к данному сегменту аппаратуры.

Так как аппаратура 10BASE-T разрабатывалась до создания механизма автодиалога, для автоматического определения типа сети необходимо обрабатывать не только сигналы FLP, но и NLP. Это также предусмотрено в аппаратуре, поддерживающей автодиалог. Естественно, в такой аппаратуре, как правило, заложена возможность отключения режима автодиалога, чтобы пользователь сам мог задать режим работы своей сети.

Помимо уже упоминавшихся сегментов 10BASE-T, 100BASE-TX и 100BASE-T4 автодиалог обеспечивает обслуживание так называемых полнодуплексных (full duplex) сегментов сети Ethernet (10BASE-T Full Duplex) и сети Fast Ethernet (100BASE-TX Full Duplex).

Рассмотрим особенности полнодуплексного режима передачи.

Как уже упоминалось, связь между абонентами бывает трех основных видов:

- симплексная (всегда только в одну сторону);
- полудуплексная (по очереди то в одну сторону, то в другую);
- полнодуплексная (одновременно в две стороны).

Классический Ethernet использует полудуплексную связь: по его единственному кабелю в разное время может проходить разнонаправленная информация. Это позволяет легко реализовать обмен между большим количеством абонентов, но требует сложных методов доступа к сети (CSMA/CD).

Полнодуплексная версия Ethernet гораздо проще. Она предназначена для обмена только между двумя абонентами по двум разнонаправленным кабелям, причем передавать могут оба абонента сразу, одновременно. Два преимущества такого подхода понятны сразу:

- не требуется никакого механизма доступа к сети,
- в идеале пропускная способность полнодуплексной линии связи оказывается вдвое выше, чем при полудуплексной передаче.

Режим полного дуплекса гораздо сложнее реализовать технически, поэтому полнодуплексные версии Ethernet и Fast Ethernet находятся все еще на стадии стандартизации, единых правил обмена пока не выработано, и аппаратура разных производителей может основываться на разных принципах обмена. Тем не менее, автодиалог уже ориентирован на их распознавание и использование.

При проведении автодиалога применяется таблица приоритетов (табл. 12.4), в которой полнодуплексные версии имеют более высокие приоритеты, чем классические полудуплексные, так как они более быстрые. Выбирается версия с максимально возможным для обоих абонентов приоритетом.

**Таблица 12.4.** Приоритеты автодиалога

| Приоритет | Тип сети |
|---|---|
| 1 | 100BASE-TX Full Duplex |
| 2 | 100BASE-T4 |
| 3 | 100BASE-TX |
| 4 | 10BASE-T Full Duplex |
| 5 | 10BASE-T |

1 – высший приоритет, 5 – низший приоритет

Из таблицы следует, что если, например, аппаратура на обоих концах сегмента поддерживает обмен с двумя скоростями, например, в режимах 10BASE-T и 100BASE-TX, то в результате автодиалога будет выбран режим 100BASE-TX, как имеющий больший приоритет (обеспечивающий большую скорость).

Автодиалог предусматривает также разрешение ситуаций, когда на одном конце кабеля подключена двухскоростная аппаратура, а на другом – односкоростная. Например, если двухскоростной адаптер присоединен к концентратору 10BASE-T, в котором не предусмотрена возможность автодиалога, то он не будет получать сигналы FLP, а только NLP. В результате действия механизма автодиалога адаптер будет переключен в режим концентратора 10BASE-T. Точно так же, если двухскоростной концентратор присоединен к односкоростному адаптеру 100BASE-TX, не рассчитанному на автодиалог, то концентратор перейдет в режим адаптера 100BASE-TX. Этот механизм одностороннего определения типа сети называется параллельным детектированием (Parallel Detection).

В любом случае, автодиалог не может обеспечить большей скорости, чем самый медленный из компонентов сети. Таким образом, если к репитерному концентратору, в котором имеется функция автодиалога, подключены два адаптера: односкоростной 10BASE-T и двухскоростной (10BASE-T и 100BASE-TX), то вся сеть будет настроена на работу по стандарту 10BASE-T, так как никакого накопления информации и никакой ее обработки в репитерном концентраторе не предусмотрено. Присоединение к такому концентратору двух неперестраиваемых (односкоростных) адаптеров с разными скоростями делает сеть неработоспособной. Иногда в конструкции репитеров предусматривается автоматическое отключение портов, к которым присоединены неперестраиваемые низкоскоростные (10BASE-T) адаптеры. Некоторые концентраторы (самые сложные) могут автоматически перекоммутировать порты таким

образом, чтобы сегменты со скоростью 10 Мбит/с обменивались информацией только между собой, а сегменты со скоростью 100 Мбит/с – между собой.

Помимо собственно определения типа сети и выбора максимально возможной скорости обмена автодиалог обеспечивает и некоторые дополнительные возможности. В частности, он позволяет определять, почему нарушилась связь в процессе работы, а также обмениваться информацией об ошибках. Для передачи этой дополнительной информации используется тот же самый механизм, что и для основного автодиалога, но только после того, как установлен тип сети и скорость передачи. Данная функция называется «функцией следующей страницы» (next page function).

Обмен информацией при автодиалоге производится посылками (пакетами) FLP-импульсов, которыми кодируется 16-битное слово. Каждая посылка содержит от 17 до 33 импульсов, идентичных импульсам NLP, которые используются в 10BASE-T. Посылки имеют длительность около 2 мс и передаются с периодом 16,8 мс (рис.12.8).

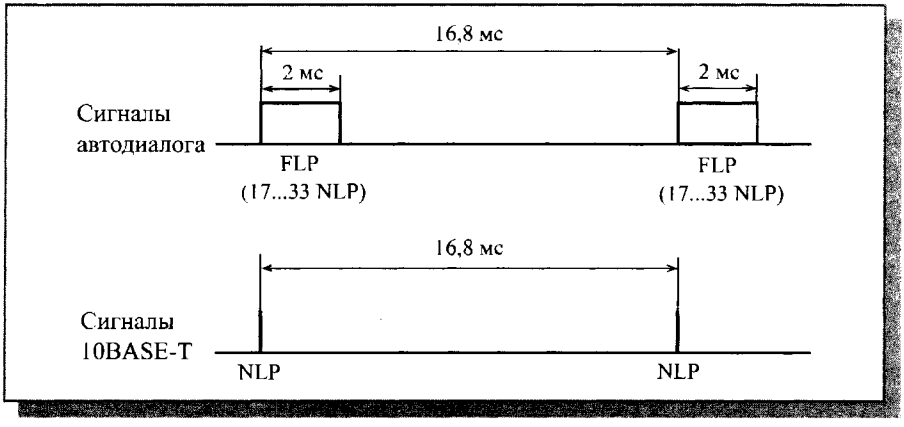



**Рис. 12.8.** Временная диаграмма автодиалога и 10BASE-T

Для кодирования битов в FLP применяется следующий код. В начале каждого битового интервала передается импульс. В середине бита, соответствующего логической единице, передается еще один импульс. В середине бита, соответствующего логическому нулю, импульса нет. Этот код иллюстрируется рис. 12.9. В начале посылки передается стартовый нулевой бит, именно поэтому общее количество импульсов в посылке FLP может изменяться в пределах от 17 до 33.

Обмен информацией при автодиалоге осуществляется 16-битными словами, называемыми LCW (Link Code Word), с форматом, представленным на рис. 12.10.

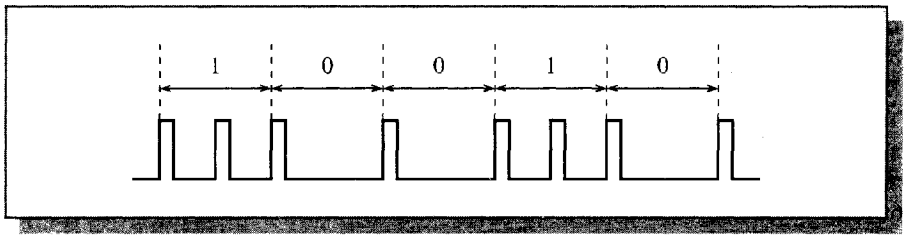



**Рис. 12.9.** Код, применяемый при автодиалоге

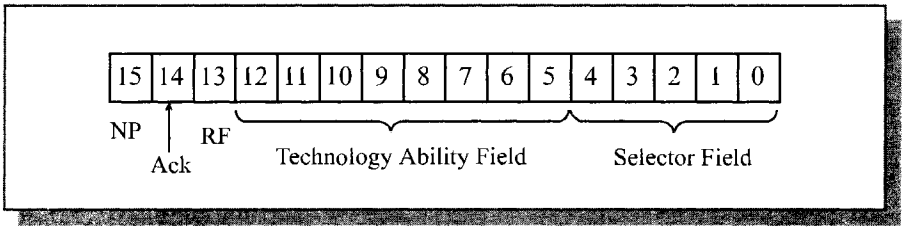



**Рис. 12.10.** Формат слова LCW, применяемого в автодиалоге

Пятиразрядное поле селектора (Selector Field) определяет один из 32 возможных типов стандарта сети. В настоящее время для него используется только два кода: код 00001 соответствует стандарту IEEE 802.3, а код 00010 – IEEE 802.9.

Восьмиразрядное поле технологических особенностей (Technology Ability Field) определяет тип сети в пределах стандарта, заданного битами поля селектора. Для стандарта IEEE 802.3 пока что определены пять типов, которые представлены в таблице 12.4.

Бит удаленной ошибки RF (Remote Fault) позволяет передавать информацию о наличии ошибок. Бит подтверждения Ack (Acknowledge) используется для подтверждения получения посылки. Наконец, бит следующей страницы NP (Next Page) говорит о поддержке функции следующей страницы, о том, что абонент собирается передавать еще и дополнительную информацию в следующем слове.

В автодиалоге используется специально разработанный протокол с многократным подтверждением принятия посылок. В случае если автодиалог происходит между абонентами 1 и 2, последовательность действий абонентов будет такой:

1. Абонент 1 передает свою посылку (LCW) с неустановленным (равным нулю) битом Ack.
2. Абонент 2 в ответ начинает передавать последовательные ответные посылки (LCW).
3. Когда абонент 1 получает три последовательные посылки от абонента 2 (бит Ack при этом игнорируется), он передает посылку с уста-

новленным (равным единице) битом Ack (подтверждает правильный прием LCW от абонента 2).

4. Абонент 2 продолжает передавать свои LCW с установленным битом Ack.
5. Когда абонент 1 получает три последовательные посылки от абонента 2 с установленным битом Ack, он понимает, что абонент 2 правильно принял его LCW.
6. Абонент 1 передает свое LCW с установленным битом Ack 6–8 раз для гарантии, что диалог завершен полностью.
7. В результате оба абонента получают информацию о своем партнере и могут выбрать тот режим работы, который обеспечит наилучшие характеристики обмена.

В соответствии с этим алгоритмом действуют оба абонента, участвующие в автодиалоге. Как видно, здесь реализуется механизм многократного взаимного подтверждения, что существенно повышает надежность передачи данных об аппаратуре абонентов. При этом также легко детектируются ошибочные ситуации, например, неисправности аппаратуры абонентов, нарушения целостности кабеля, несовместимость аппаратуры абонентов и т.д.

Для реализации функции следующей страницы используется бит NP (см. рис. 12.10). Если оба абонента устанавливают его в своих LCW, то есть оба они поддерживают эту функцию, то между ними может быть произведен дополнительный обмен информацией такими же 16-разрядными словами, но с другим форматом. В этих словах 11 битов отводится на информацию, а пять битов используются как служебные. В частности, это позволяет производить более полную диагностику аппаратуры, а также выявлять повышенный уровень помех в линии связи.

Вероятно, в дальнейшем принцип автодиалога будет совершенствоваться, включая в себя другие стандарты и типы сети, давая возможность разрешения все новых задач. Но его реализация в принципе невозможна при стандартной топологии «шина», поэтому, скорее всего, доля шинных сегментов (10BASE2 и 10BASE5) будет все больше сокращаться. И в новых сетях (Fast Ethernet, Gigabit Ethernet) шинные сегменты вряд ли появятся.

# Глава 9. Оборудование Ethernet и Fast Ethernet

## Лекция 13. Оборудование Ethernet и Fast Ethernet

**В этой лекции представлен материал об аппаратуре сети Ethernet/Fast Ethernet: адаптерах, концентраторах, коммутаторах, мостах и маршрутизаторах, их функциях, типах, характеристиках, достоинствах и недостатках.**

**Ключевые слова:** NIC, Hub, Switch, Bridge, Router, FCE, ECE, Jabber, Cut-Trough, SAF, Spanning Tree, маршрутизируемая сеть.

В настоящее время сеть Ethernet/Fast Ethernet распространена наиболее широко, ее аппаратура выпускается наибольшим числом производителей, и ее перспективы представляются самыми благоприятными. В связи с этим следует более подробно рассмотреть некоторые особенности ее аппаратных средств. Впрочем, многое из сказанного в данном разделе относится не только к Ethernet, но и к аппаратуре других, менее популярных сетей.

### Адаптеры Ethernet и Fast Ethernet

#### Характеристики адаптеров

Сетевые адаптеры (NIC, Network Interface Card) Ethernet и Fast Ethernet могут сопрягаться с компьютером через один из стандартных интерфейсов:

- шина ISA (Industry Standard Architecture);
- шина PCI (Peripheral Component Interconnect);
- шина PC Card (она же PCMCIA).

Адаптеры, рассчитанные на системную шину (магистраль) ISA, еще не так давно были основным типом адаптеров. Количество компаний, выпускавших такие адаптеры, было велико, именно поэтому устройства данного типа были самыми дешевыми. Адаптеры для ISA выпускаются 8- и 16-разрядными. 8-разрядные адаптеры дешевле, а 16-разрядные – быстрее. Правда, обмен информацией по шине ISA не может быть слишком быстрым (в пределе – 16 Мбайт/с, реально – не более 8 Мбайт/с, а для 8-разрядных адаптеров – до 2 Мбайт). Поэтому адаптеры Fast Ethernet, требующие

для эффективной работы больших скоростей обмена, для этой системной шины практически не выпускаются. Шина ISA уходит в прошлое.

Шина PCI сейчас практически вытеснила шину ISA и становится основной шиной расширения для компьютеров. Она обеспечивает обмен 32- и 64-разрядными данными и отличается высокой пропускной способностью (теоретически до 264 Мбайт/с), что вполне удовлетворяет требованиям не только Fast Ethernet, но и более быстрой Gigabit Ethernet. Важно еще и то, что шина PCI применяется не только в компьютерах IBM PC, но и в компьютерах PowerMac. Кроме того, она поддерживает режим автоматического конфигурирования оборудования Plug-and-Play. Видимо, в ближайшем будущем на шину PCI будет ориентировано большинство сетевых адаптеров. Недостаток PCI по сравнению с шиной ISA в том, что количество ее слотов расширения в компьютере, как правило, невелико (обычно 3 слота). Но именно сетевые адаптеры подключаются к PCI в первую очередь.

Шина PC Card (старое название PCMCIA) применяется пока только в портативных компьютерах класса Notebook. В этих компьютерах внутренняя шина PCI обычно не выводится наружу. Интерфейс PC Card предусматривает простое подключение к компьютеру миниатюрных плат расширения, причем скорость обмена с этими платами достаточна высока. Однако все больше портативных компьютеров оснащается встроенными сетевыми адаптерами, так как возможность доступа к сети становится неотъемлемой частью стандартного набора функций. Эти встроенные адаптеры опять же подключены к внутренней шине PCI компьютера.

При выборе сетевого адаптера, ориентированного на ту или иную шину, необходимо прежде всего убедиться, что свободные слоты расширения данной шины есть в компьютере, включаемом в сеть. Следует также оценить трудоемкость установки приобретаемого адаптера и перспективы выпуска плат данного типа. Последнее может понадобиться в случае выхода адаптера из строя.

Наконец, встречаются еще сетевые адаптеры, подключающиеся к компьютеру через параллельный (принтерный) порт LPT. Главное достоинство такого подхода состоит в том, что для подключения адаптеров не нужно вскрывать корпус компьютера. Кроме того, в данном случае адаптеры не занимают системных ресурсов компьютера, таких как каналы прерываний и ПДП, а также адреса памяти и устройств ввода/вывода. Однако скорость обмена информацией между ними и компьютером в этом случае значительно ниже, чем при использовании системной шины. К тому же они требуют больше процессорного времени на обмен с сетью, замедляя тем самым работу компьютера.

В последнее время все больше встречается компьютеров, в которых сетевые адаптеры встроены в системную плату. Достоинства такого под-

хода очевидны: пользователь не должен покупать сетевой адаптер и устанавливать его в компьютер. Достаточно только подключить сетевой кабель к внешнему разъему компьютера. Однако недостаток состоит в том, что пользователь не может выбрать адаптер с лучшими характеристиками.

К другим важнейшим характеристикам сетевых адаптеров можно отнести:

- способ конфигурирования адаптера;
- размер установленной на плате буферной памяти и режимы обмена с ней;
- возможность установки на плату микросхемы постоянной памяти для удаленной загрузки (BootROM).
- возможность подключения адаптера к разным типам среды передачи (витая пара, тонкий и толстый коаксиальный кабель, оптоволоконный кабель);
- используемая адаптером скорость передачи по сети и наличие функции ее переключения;
- возможность применения адаптером полнодуплексного режима обмена;
- совместимость адаптера (точнее, драйвера адаптера) с используемыми сетевыми программными средствами.

Конфигурирование адаптера пользователем применялось в основном для адаптеров, рассчитанных на шину ISA. Конфигурирование подразумевает настройку на использование системных ресурсов компьютера (адресов ввода/вывода, каналов прерываний и прямого доступа к памяти, адресов буферной памяти и памяти удаленной загрузки). Конфигурирование может осуществляться путем установки в нужное положение переключателей (джамперов) или с помощью прилагаемой к адаптеру DOS-программы конфигурирования (Jumperless, Software configuration). При запуске такой программы пользователю предлагается установить конфигурацию аппаратуры при помощи простого меню: выбрать параметры адаптера. Эта же программа позволяет произвести самотестирование адаптера. Выбранные параметры хранятся в энергонезависимой памяти адаптера. В любом случае при выборе параметров необходимо избегать конфликтов с системными устройствами компьютера и с другими платами расширения.

Конфигурирование адаптера может выполняться и автоматически в режиме Plug-and-Play при включении питания компьютера. Современные адаптеры обычно поддерживают именно этот режим, поэтому их легко может установить пользователь.

В простейших адаптерах обмен с внутренней буферной памятью адаптера (Adapter RAM) осуществляется через адресное пространство устройств ввода/вывода. В этом случае никакого дополнительного конфигурирования адресов памяти не требуется. Базовый адрес буферной памяти,

работающей в режиме разделяемой памяти, необходимо задавать. Он приписывается к области верхней памяти компьютера (UMA, Upper Memory Address) в диапазоне адресов A0000h—FFFFFh. В эту же зону адресов помещается и ПЗУ удаленной загрузки (Boot ROM), если предполагается его использование для создания бездисковой рабочей станции. Если используется конфигурирование вручную, то надо следить, чтобы не было конфликтов адресов адаптера с другими устройствами компьютера.

Все операции по конфигурированию сетевого адаптера необходимо проводить в строгом соответствии с документацией, поставляемой вместе с ним, так как каждый из многочисленных производителей адаптеров обычно вносит в них что-то свое, оригинальное. Поэтому никакие более подробные универсальные рекомендации попросту невозможны. Впрочем, это относится к любым электронным устройствам.

От размера буферной памяти адаптера зависит как скорость работы адаптера, так и его способность держать высокие информационные нагрузки. Размер памяти обычно составляет от 8 Кбайт до нескольких мегабайт. Чем больше память, тем больше передаваемых и принимаемых пакетов может в ней храниться. Для адаптеров, работающих на выделенном сервере, большой объем буферной памяти просто необходим, ведь через него пойдут все информационные потоки сети. Впрочем, самая большая буферная память не поможет, если компьютер работает медленно, и не успевает перекачивать приходящую по сети информацию.

Для скорости работы адаптера важен режим обмена компьютера с буферной памятью адаптера. Если адаптер поддерживает режим прямого доступа к памяти (DMA – Direct Memory Access), режим прямого управления шиной (Bus Mastering) или режим разделения памяти, то он обычно работает более производительно, чем адаптеры, не поддерживающие этих режимов. Более того, адаптеры, рассчитанные на быструю шину PCI и работающие в режимах прямого доступа к памяти или прямого управления шиной, могут и не нуждаться в большом объеме буферной памяти, так как информация может передаваться адаптером напрямую в память компьютера и обратно.

Некоторые адаптеры поддерживают функцию удаленной загрузки по сети. Для этого на плате адаптера устанавливается микросхема постоянной памяти (Boot ROM), в которой находится программа начальной загрузки. Такое решение позволяет использовать бездисковые рабочие станции. Но сейчас данная возможность применяется не слишком часто, так как практически все компьютеры оснащены дисководами.

Все функции по обслуживанию обмена по сети в сетевом адаптере, как правило, выполняет одна специализированная микросхема или небольшой комплект микросхем (2–3 штуки). Этим и объясняется достаточно низкая цена адаптеров. Поставщиков подобных комплектов микросхем не так много, поэтому очень многие адаптеры выполнены по сход-

ным схемам. Однако организация обмена шины компьютера с адаптером может быть различной, поэтому показатели производительности адаптеров от разных изготовителей и показатели надежности их работы, особенно в экстремальных условиях, сильно различаются.

Адаптер может быть рассчитан только на один тип среды передачи, к примеру, на витую пару, но может также поддерживать возможность подключения нескольких разных сред передачи, например, тонкий и толстый коаксиальные кабели. Для этого на плате устанавливаются соответствующие разъемы (см. Лекцию 5 «Аппаратура локальных сетей»). Наиболее универсальны так называемые адаптеры «Combo», которые имеют полный набор разъемов (BNC, RJ-45 и AUI для Ethernet). Для выбора конкретного типа среды иногда используются переключатели (джамперы). Как правило, их несколько и переключать их надо обязательно все вместе. Иногда выбор среды передачи осуществляется программно.

Адаптеры Fast Ethernet выпускаются как односкоростными (100 Мбит/с), так и двухскоростными (10 Мбит/с и 100 Мбит/с). Двухскоростные платы (их обычно помечают «10/100») несколько дороже односкоростных, но зато они могут работать в любой сети Ethernet/Fast Ethernet без всяких проблем.

Поддержка адаптером полнодуплексного режима обмена по сети пока что встречается нечасто. Это связано с тем, что полнодуплексный режим требует и применения полнодуплексных коммутаторов. Это оказывается очень дорого. Однако для мощных серверов больших сетей поддержка полнодуплексного режима очень желательна.

Все сетевые адаптеры должны быть сертифицированы. Сертификат FCC класса A позволяет использовать адаптер в бизнесе, сертификат FCC класса B – в домашних условиях. Стандарт предусматривает безопасный уровень электромагнитного излучения сетевого адаптера.

При выборе адаптера очень важно обращать внимание на совместимость его драйвера с сетевым программным обеспечением. Все поставщики сетевых программных средств (Novell, Microsoft и др.) проводят работу по сертификации драйверов. Если такой сертификат имеется, то можно быть уверенным, что проблем по совместимости не будет. С другой стороны, все сетевые программные продукты поставляются с набором протестированных драйверов, совместимых с ними. Если драйвер приобретенной платы входит в этот набор, то проблем тоже, скорее всего, не будет. Солидные производители сетевых адаптеров регулярно распространяют обновленные, более быстрые и универсальные версии драйверов для своих плат. Низкая цена некоторых адаптеров может объясняться как раз отсутствием сертификата, плохой совместимостью с программными средствами. Вообще же цены на адаптеры разных фирм и разных типов могут различаться в десятки раз.

Несколько слов о производительности адаптера.

Реальная скорость обмена информацией по сети представляет собой интегральный параметр, зависящий не только от адаптера, но и от компьютера (быстродействия процессора и дисковода, объема системной памяти), среды передачи (уровня помех), программных средств, величины загрузки сети и т.д. Поэтому выбор самого быстрого (и дорогого) адаптера далеко не всегда гарантирует заметный выигрыш в скорости обмена. Например, переход с 8-разрядного ISA–адаптера на 16-разрядный или с ISA–адаптера на 32-разрядный PCI–адаптер может практически не сказаться на скорости. Тем не менее, нередки ситуации, когда именно адаптер становится самым узким местом в системе и его замена может резко увеличить производительность сети.

Косвенные показатели производительности адаптера уже были перечислены: производительнее всего работают те, которые рассчитаны на PCI, поддерживают режим разделения буферной памяти, у которых буферная память большего объема. Быстрее будут те адаптеры, которые максимальное количество функций выполняют без участия процессора, опираясь на встроенный интеллект.

Но получить реальные количественные показатели производительности можно только в результате тестирования сети в целом. Для этого существует целый ряд тестовых программ. Наиболее известные — Perform3 компании Novell и Netbench 3.0 фирмы Ziff-Davis. Любые тестовые программы слабо отражают реальную ситуацию в сети, но позволяют сравнивать между собой различные сетевые адаптеры в условиях, близких к реальным и в реальной конфигурации аппаратных средств.

### Адаптеры с внешними трансиверами

Адаптеры Fast Ethernet могут выпускаться с внешним, выносным модулем трансивера для подключения к среде передачи (PHY). В этом случае для присоединения внешнего модуля трансивера к адаптеру используется интерфейс MII (Media-Independent Interface), предусматривающий использование 40-контактного разъема, подобного разъему компьютерного интерфейса SCSI.

Сменный модуль трансивера может устанавливаться непосредственно на плате адаптера (в специальный вырез платы), а может связываться с платой адаптера внешним кабелем длиной до 0,5 метра (рис. 13.1 и 13.2). При вычислении полного времени задержки в сети необходимо учитывать и задержку в этом трансиверном MII–кабеле.

На плате трансивера располагается микросхема приемопередатчика и разъем, зависящий от типа среды (MDI – Medium Dependent Interface), например, RJ-45 для витой пары. Таким образом, один и тот же адаптер

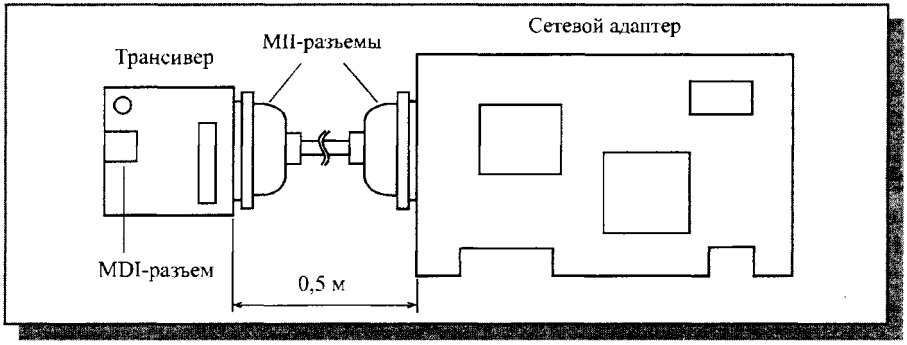



**Рис. 13.1.** Сетевой адаптер с внешним трансивером на MII-кабеле

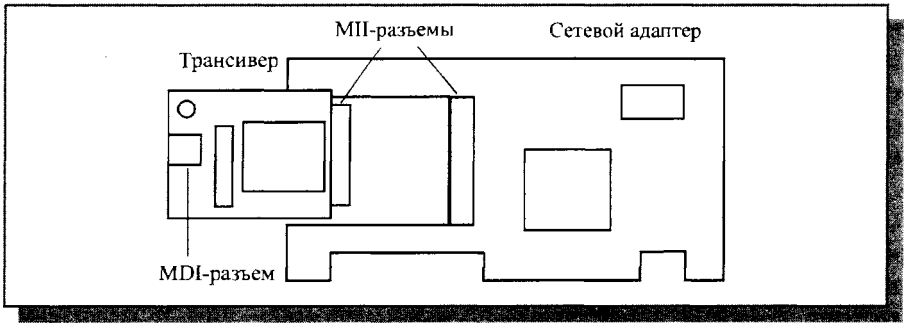



**Рис. 13.2.** Сетевой адаптер с внешним трансивером, устанавливаемым на плату адаптера

может поддерживать обмен с любым типом среды за счет простой замены сравнительно дешевого трансивера. В целом подобные составные адаптеры оказываются дороже обычных адаптеров со встроенными приемопередатчиками, но иногда их применение оправдано, если предполагается постепенная замена среды передачи, например, на оптоволоконные кабели.

## Репитеры и концентраторы Ethernet и Fast Ethernet

Использование репитеров и концентраторов (хабов) в сети Ethernet не является обязательным. Небольшие сети на основе сегментов 10BASE2 или 10BASE5 вполне могут обойтись без них. Для сетей из нескольких таких сегментов необходимы простейшие репитеры. А при выборе в качестве среды передачи витой пары (10BASE-T) или оптоволоконного кабеля (10BASE-FL) уже необходимы концентраторы (если, конечно, в сеть объединяются не два компьютера, а хотя бы три). В сети Fast Ethernet применение концентраторов обязательно.

## Функции репитеров и концентраторов

Репитеры (повторители), как уже отмечалось, ретранслируют приходящие на них (на их порты) сигналы, восстанавливают их амплитуду и форму, что позволяет увеличивать длину сети. То же самое делают и простейшие репитерные концентраторы. Но помимо этой основной функции концентраторы Ethernet и Fast Ethernet обычно выполняют еще ряд функций по обнаружению и исправлению некоторых простейших ошибок сети. К этим ошибкам относятся следующие:

- ложная несущая (FCE – False Carrier Event);
- множественные коллизии (ECE – Excessive Collision Error);
- затянувшаяся передача (Jabber).

Все эти ошибки могут быть вызваны неисправностями оборудования абонентов, высоким уровнем шумов и помех в кабеле, плохими контактами в разъемах и т.д.

Под *ложной несущей* понимается ситуация, когда концентратор получает от одного из своих портов (от единичного абонента или из сегмента) данные, не содержащие ограничителя начала потока данных, то есть преамбула пакета началась, но в ней нет признака начала кадра.

Если после старта передачи кадр не начался в течение заданного временного интервала (5 мкс для Fast Ethernet, 50 мкс для Ethernet), то концентратор посылает сигнал «Пробка» всем остальным портам, чтобы они обнаружили коллизию. Длительность этого сигнала также составляет 5 или 50 мкс. Затем выявленный порт переводится в состояние «Связь неустойчива» (Link Unstable) и отключается. Обратное включение порта концентратором может произойти только при поступлении от него правильного пакета, без ложной несущей.

Ситуация *множественных коллизий* фиксируется при выявлении в данном порту более 60 коллизий подряд. Концентратор считает количество коллизий в каждом порту и сбрасывает счетчик, если получает пакет без коллизии. Порт, в котором возникают множественные коллизии, отключается. Если в течение заданного времени (5 мкс для Fast Ethernet, 50 мкс для Ethernet) в этом порту не будет зафиксировано коллизий, то он снова включается.

Ситуация *затянувшейся передачи* фиксируется в случае, когда время передачи превышает более чем в три раза максимально возможную длительность пакета, то есть 400 мкс для Fast Ethernet или 4000 мкс для Ethernet. При обнаружении такой затянувшейся передачи соответствующий порт отключается. После окончания затянувшейся передачи данный порт снова включается.

Кроме перечисленных функций концентратор также активно способствует обнаружению любых коллизий в сети. При одновременном по-

ступлении на его порты двух и более пакетов он, как и любой абонент, усиливает столкновение путем передачи во все порты сигнала «ПРОБКА» в течение 32 битовых интервалов. В результате все передающие абоненты всех сегментов обязательно обнаруживают факт коллизии и прекращают свою передачу.

Таким образом, даже самый простой концентратор представляет собой довольно сложное устройство, позволяющее автоматически устранять некоторые неисправности и временные сбои. Таким образом, концентратор не только объединяет точки включения кабелей сети, но и активно улучшает условия обмена, повышает производительность сети, отключая время от времени неисправные или неустойчиво работающие сегменты. Впрочем, главный признак концентратора остается – он не производит никакой обработки информации, воспринимает пакеты как единое целое, не анализируя их содержимое.

Как и сетевые адаптеры, концентраторы могут быть односкоростными и двухскоростными. Для большей свободы в проектировании сети лучше выбирать именно двухскоростные (10/100 Мбит/с) концентраторы.

Чаще всего репитеры и концентраторы выполняются в виде отдельных автономных блоков, имеющих внутренний или внешний источник питания.

Некоторые концентраторы рассчитаны на подключение жестко заданного количества сегментов определенного типа (например, на четыре сегмента 10BASE2 или же на восемь сегментов 10BASE-T). Для этого на них устанавливаются соответствующие типу сегмента разъемы: BNC, RJ-45, AUI или оптоволоконные разъемы.

Другие, более дорогие концентраторы, называемые наращиваемыми, стековыми (Stackable), имеют модульную структуру и позволяют гибко приспосабливать их к заданной конфигурации сети. В этом случае в каркас (стек) концентратора может быть установлено различное число (обычно до 8) сменных модулей, каждый из которых ориентирован на один или несколько сегментов какого-нибудь типа и имеет соответствующие разъемы для подключения кабеля сети (например, BNC, AUI, RJ-45, ST-разъемы). Как правило, количество подключаемых сегментов (портов концентратора) выбирается кратным четырем: 4, 8, 12, 16, 24. Наращиваемый концентратор может поддерживать, к примеру, 192 порта (восемь модулей, каждый из которых рассчитан на 24 сегмента). Структура такого наращиваемого концентратора показана на рис. 13.3.

Самые сложные концентраторы на базе единого шасси (рис. 13.4) позволяют путем перекоммутации связей на контактной задней панели строить сложные конфигурации сетей. Например, они могут одновременно поддерживать несколько типов сетей (Token-Ring, Ethernet и FDDI), а также допускают включение не только модулей репитерных концентрато-

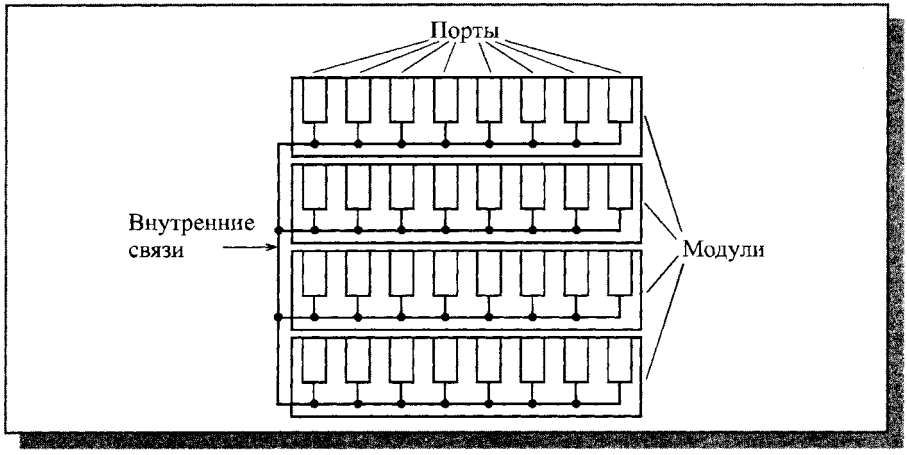



**Рис. 13.3.** Структура наращиваемого концентратора

ров, но и модулей маршрутизаторов и коммутаторов. На основе такого концентратора можно также организовывать одновременно несколько независимых однотипных сетей (например, Ethernet) для разделения информационных потоков между ними и снижения нагрузки на сеть.

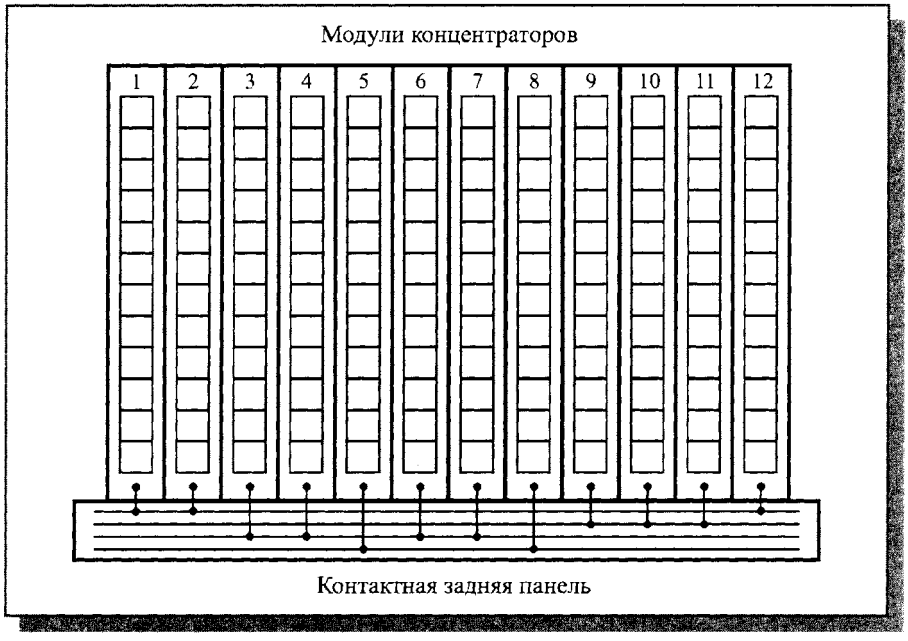



**Рис. 13.4.** Концентратор на основе шасси

Как правило, концентраторы на базе шасси предусматривают возможность довольно сложного управления обменом. Количество портов таких концентраторов может доходить до 288. Правда, этот тип концентратора оказывается обычно самым дорогим в расчете на один порт. Считается, что их применение становится экономически оправданным только в случае необходимости поддержки большого количества портов (около 100).

Встречаются также совсем простые и самые дешевые репитеры и концентраторы, выполненные в виде платы, вставляемой в разъем системной шины компьютера (из компьютера они берут при этом только питание). Недостаток такого решения состоит в том, что для работы сети необходимо, чтобы компьютер, в который включена плата репитера (концентратора), был постоянно включен (в идеале – круглосуточно). При выключении питания этого компьютера связь по сети становится невозможной.

## Концентраторы класса I и класса II

Стандарт IEEE 802.3 определяет два класса репитерных концентраторов Ethernet/Fast Ethernet, отличающихся друг от друга своими функциональными возможностями и областями применения. Каждый концентратор должен иметь маркировку своего класса в виде римской цифры I или II, заключенной в кружок.

**Концентраторы класса II** —классические концентраторы, использовавшиеся с самого начала в сетях Ethernet. Именно поэтому их применение было разрешено и в сетях Fast Ethernet. Эти концентраторы отличаются тем, что они непосредственно повторяют приходящие на них из сегмента сигналы и передают их в другие сегменты без какого бы то ни было преобразования. Они не способны преобразовывать методы кодирования сетевых сигналов. Поэтому к ним можно подключать только сегменты, использующие одну систему сигналов. Например, к концентратору могут подключаться только одинаковые сегменты 10BASE-T или только одинаковые сегменты 100BASE-TX. Допустимо, правда, подключение и разных сегментов, но они должны использовать один код передачи, например, 10BASE-T и 10BASE-FL или 100BASE-TX и 100BASE-FX. Данные концентраторы принципиально не могут объединять сегменты с разными системами кодирования, в частности, 100BASE-TX и 100BASE-T4.

Задержка сигналов в концентраторах класса II меньше, чем в концентраторах класса I. Согласно стандарту, она должна составлять от 46 битовых интервалов (для 100BASE-TX/FX) до 67 битовых интервалов (для 100BASE-T4). Отсюда следуют ограничения на наращиваемость таких концентраторов и на количество их портов (как правило, оно не пре-

вышает 24). Зато меньшая задержка концентратора позволяет использовать кабели большей длины, так как на работоспособность сети влияет суммарная задержка сигнала в сети, включающая в себя задержки как концентраторов, так и в кабелях.

Для соединения концентраторов класса II между собой используется специальный порт расширения (UpLink port). Каждый концентратор подключается этим портом к одному из обычных портов другого концентратора (рис. 13.5).

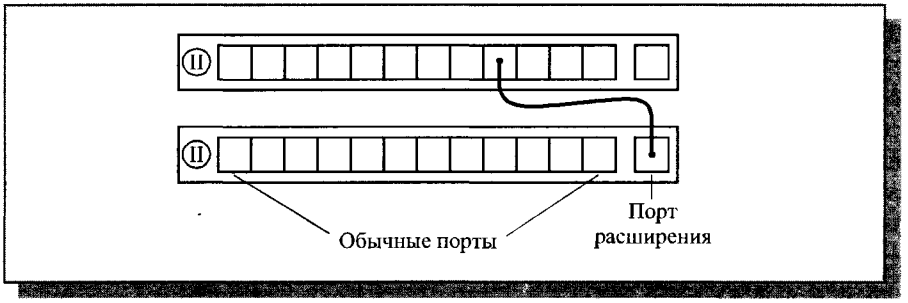



**Рис. 13.5.** Соединение двух концентраторов класса II

Концентраторы класса II сложнее в производстве, чем концентраторы класса I, так как временные требования, предъявляемые к ним, жестче. Но при этом возможности их меньше, поэтому в настоящее время их вытесняют концентраторы класса I.

**Концентраторы класса I** характеризуются тем, что они преобразуют приходящие по сегментам сигналы в цифровую форму, прежде чем передавать их во все другие сегменты. Они содержат декодирующие и кодирующие узлы.

В отличие от концентраторов класса II они способны преобразовывать коды, применяемые в разных сегментах. Поэтому к ним можно одновременно подсоединять сегменты разных типов, например, 100BASE-TX, 100BASE-T4 и 100BASE-FX. Но этот процесс двойного преобразования кодов требует времени, поэтому данные концентраторы оказываются медленнее (по стандарту, их задержка составляет не более 140 битовых интервалов).

Концентраторы класса I — более гибкие, они имеют расширенные возможности по наращиваемости. Именно из них строятся сложные концентраторы на базе шасси. К тому же благодаря внутренним цифровым шинам сигналов они допускают управление с удаленных рабочих станций, позволяющих контролировать нагрузку сети, состояние портов, интенсивность ошибок в сети, а также автоматически отключать неисправные сегменты.

При этом для обмена с управляющей станцией применяется специально разработанный протокол обмена SNMP (Simple Network Management Protocol – простой протокол управления сетью). Такой концентратор, допускающий удаленное управление, называется интеллектуальным (Intelligent Hub).

Протокол SNMP был предложен в 1988 году комиссией IAB (Internet Activities Board). Он описывается документами RFC 1067, RFC 1098, RFC 1157. Комиссия IAB определила также и метод описания данных для этого протокола под названием ASN.1 (Abstract Syntax Notation). Протокол SNMP относится к прикладному уровню, он работает с протоколами IP и IPX, а также позволяет не только собирать информацию о сети, но и управлять устройствами сети.

Протокол SNMP подразумевает хранение информации об устройствах сети в формате ASN.1 в виде текстовых файлов, так называемых MIB (Management Information Base – база управляющей информации). Например, в случае интеллектуального концентратора с него можно считать информацию о количестве пакетов, переданных и полученных каждым из портов, можно также включить и выключить каждый порт.

Для управления устройством сети, контроллер этого устройства должен выполнять программу агента SNMP. Программа агента собирает данные о системе, в которой он запущен и управляет объектами данных системы.

Рабочая станция, управляющая сетью (NMS – Network Management Station) – это один из компьютеров, подключенных к сети, на котором запущен специальный пакет прикладных программ, в удобном графическом виде отображающий состояние сетевых устройств и позволяющий управлять ими.

Протокол SNMP поддерживает три типа команд:

- Команда GET читает значения объектов данных устройства (из MIB) в произвольном порядке.
- Команда GET NEXT читает следующее по порядку значение объекта данных устройства.
- Команда SET применяется для изменений (записи) значений объектов данных устройства.

Команды и реакции протокола SNMP передаются посредством модулей данных в составе дейтаграмм (PDU – Protocol Data Unit). Протокол предусматривает также передачу информации о типе кодирования MIB, поэтому в разных устройствах MIB может иметь различный формат. Существует ряд фирменных и стандартных форматов MIB для сетевых адаптеров (MIB-II), концентраторов, мостов и сети в целом (RMON MIB), поддерживаемых SNMP.

# Коммутаторы Ethernet и Fast Ethernet

Коммутирующие концентраторы (Switched Hubs) или, как их еще называют, коммутаторы (Switches), переключатели и свичи, могут рассматриваться, как простейший и очень быстрый мост. Они позволяют разделить единую сеть на несколько сегментов для увеличения допустимого размера сети или с целью снижения нагрузки (трафика) в отдельных частях сети.

Как уже отмечалось, в отличие от мостов, коммутирующие концентраторы не принимают приходящие пакеты, а только переправляют из одной части сети в другую те пакеты, которые в этом нуждаются. Они в реальном темпе поступления битов пакета распознают адрес приемника пакета и принимают решение о том, надо ли это пакет переправлять, и, если надо, то кому. Никакой обработки пакетов не производится, хотя их заголовок контролируется . Коммутаторы практически не замедляют обмена по сети. Но они не могут преобразовывать форматы пакетов и протоколов обмена по сети. Поскольку коммутаторы работают с информацией, находящейся внутри кадра, часто говорят, что они ретранслируют кадры, а не пакеты, как репитерные концентраторы.

Коллизии коммутатором не ретранслируются, что выгодно отличает его от более простого репитерного концентратора. Можно сказать, что коммутаторы производят более глубокое разделение сети, чем концентраторы. Они разделяют на части зону коллизий (Collision Domain) сети, то есть область сети, на которую распространяются коллизии.

Логическая структура коммутатора довольно проста (рис.13.6).

Она включает в себя так называемую перекрестную (коммутационную) матрицу (Crossbar Matrix), во всех точках пересечения которой могут устанавливаться связи на время передачи пакета. В результате пакет, поступающий из любого сегмента, может быть передан в любой другой сегмент (рис. 13.6). В случае широковещательного пакета, адресованного всем абонентам, он передается во все сегменты одновременно, кроме того сегмента, по которому он пришел (рис. 13.7).

Помимо перекрестной матрицы коммутатор включает в себя память, в которой он формирует таблицу MAC-адресов всех компьютеров, подключенных к каждому из его портов. Эта таблица создается на этапе инициализации сети и затем периодически обновляется для учета изменений конфигурации сети. Именно на основании анализа этой таблицы делается вывод о том, какие связи надо замыкать, и куда отправлять пришедший пакет. Коммутатор читает MAC-адреса отправителя и получателя в пришедшем пакете и передает пакет в тот сегмент, в который он адресован. Если пакет адресован абоненту из того же сегмента, к которому принадлежит отправитель, то он не ретранслируется вообще. Широковещательный пакет не передается в тот сегмент, к которому присоединен абонент

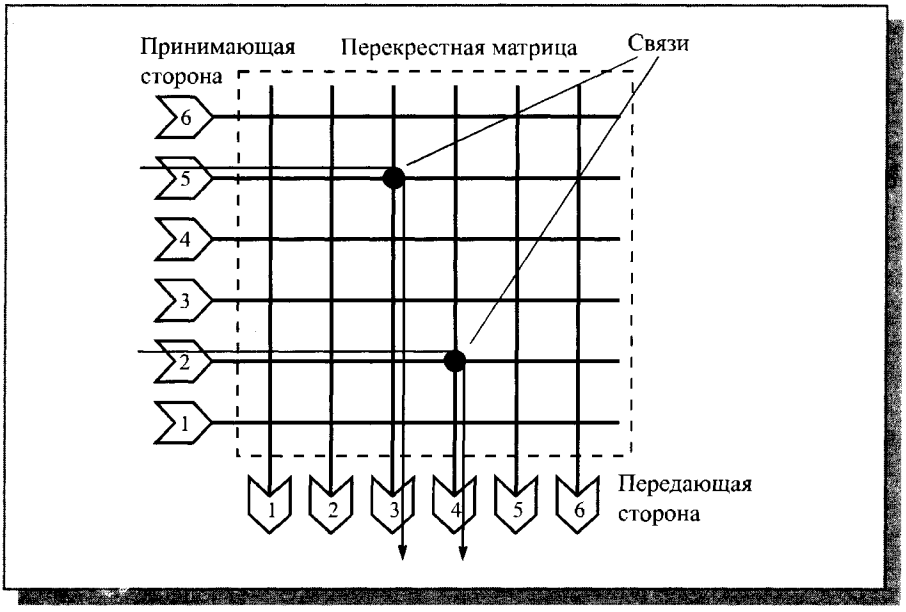



**Рис. 13.6.** Логическая схема коммутатора

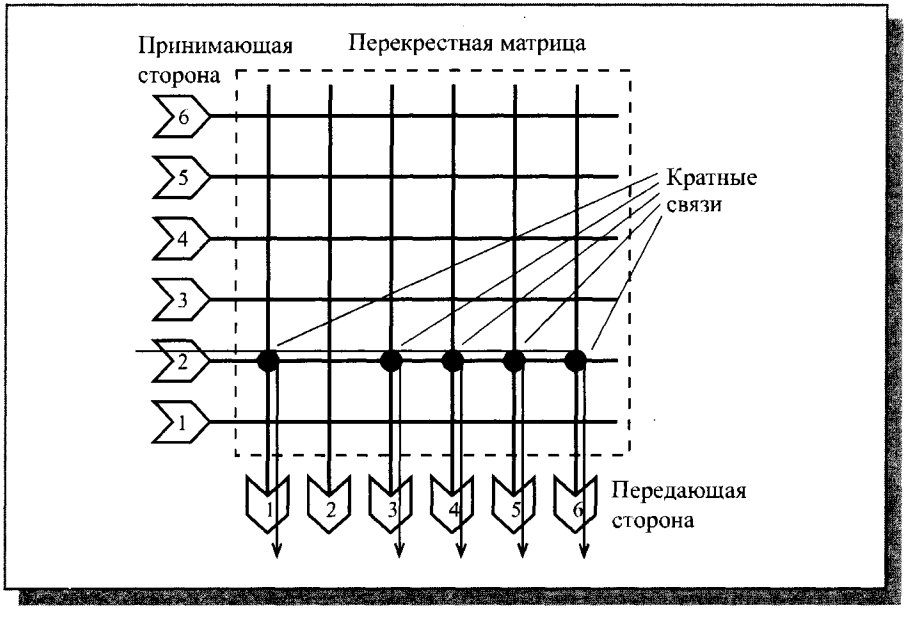



**Рис. 13.7.** Ретрансляция широковещательного пакета

— отправитель пакета. Адрес отправителя пакета заносится в таблицу адресов (если его там еще нет).

Коммутаторы выпускаются на различное число портов. Чаще всего встречаются коммутаторы с 6, 8, 12, 16 и 24 портами. Следует отметить, что мосты, как правило, редко поддерживают более 4 портов. Различаются коммутаторы и допустимым количеством адресов на один порт. Этот показатель определяет предельную сложность подключаемых к порту сегментов (количество компьютеров в каждом сегменте). Некоторые коммутаторы позволяют разбивать порты на группы, работающие независимо друг от друга, то есть один коммутатор может работать как два или три.

Так же, как и концентраторы, коммутаторы выпускаются трех видов в зависимости от сложности, возможности наращивания количества портов и стоимости:

- коммутаторы с фиксированным числом портов (обычно до 30);
- модульные коммутаторы (с числом портов до 100);
- стековые коммутаторы.

Коммутаторы характеризуются двумя показателями производительности:

- Максимальная скорость ретрансляции пакетов измеряется при передаче пакетов из одного порта в другой, когда все остальные порты отключены.
- Совокупная скорость ретрансляции пакетов измеряется при активной работе всех имеющихся портов. Совокупная скорость больше максимальной, но максимальная скорость, как правило, не может быть обеспечена на всех портах одновременно, хотя коммутаторы и способны одновременно обрабатывать несколько пакетов (в отличие от моста).

Главное правило, которого надо придерживаться при разбиении сети на части (сегменты) с помощью коммутатора, называется «правило 80/20». Только при его выполнении коммутатор работает эффективно. Согласно этому правилу, необходимо, чтобы не менее 80 процентов всех передач происходило в пределах одной части (одного сегмента) сети. И только 20 процентов всех передач должно происходить между разными частями (сегментами) сети, проходить через коммутатор. На практике это обычно сводится к тому, чтобы сервер и активно работающие с ним рабочие станции (клиенты) располагались на одном сегменте. Это же правило 80/20 применимо и к мостам.

Существует два класса коммутаторов, отличающихся уровнем интеллекта и способами коммутации:

- коммутаторы со сквозным вырезанием (Cut-Through);
- коммутаторы с накоплением и ретрансляцией (Store-and-Forward, SAF).

## Коммутаторы Cut-Through

Коммутаторы Cut-Through – самые простые и быстрые, они не производят никакого буферирования пакетов и никакой их селекции. Про них часто говорят, что они производят коммутацию «на лету» (on-the-fly).

Эти коммутаторы буферируют только головную часть пакета, чтобы прочитать 6-байтовый адрес приемника пакета и принять решение о коммутации, на которое у некоторых коммутаторов уходит около 10 битовых интервалов. В результате время ожидания ретрансляции (задержка на коммутаторе), включающее как время буферирования, так и время коммутации, может составлять около 150 битовых интервалов. Конечно, это больше задержки репитерного концентратора, но гораздо меньше задержки ретрансляции любого моста.

Недостаток данного типа коммутатора состоит в том, что он ретранслирует любые пакеты с нормальной головной частью, в том числе и заведомо ошибочные пакеты (например, с неправильной контрольной суммой) и карликовые пакеты (длиной менее 512 битовых интервалов). Ошибки одного сегмента ретранслируются в другой сегмент, что приводит к снижению пропускной способности сети в целом.

Еще одна проблема состоит в том, что коммутаторы данного типа часто перегружаются и плохо обрабатывают ситуацию перегрузки. Например, из двух или более сегментов одновременно поступают пакеты, адресованные одному и тому же сегменту. Но коммутатор не может одновременно передать несколько пакетов в один сегмент, поэтому часть пакетов пропадает. Вместе с тем коммутатор не может ретранслировать и пакеты, приходящие из того же порта, в который коммутатор передает в данный момент.

Одно из усовершенствований коммутаторов Cut-Trough получило название Interim Cut-Trough Switching (ICS). Оно направлено на то, чтобы избежать ретрансляции карликовых кадров. Для этого на принимающей стороне коммутатора все порты имеют буферную память типа FIFO на 512 бит. Если пакет заканчивается раньше, чем буфер заполнится, то содержимое буфера автоматически отбрасывается. Однако все остальные недостатки метода Cut-Through в данном случае сохраняются. Задержка ретрансляции коммутаторов данного типа (ICS) увеличивается примерно на 400 битовых интервалов по сравнению с обычным Cut-Trough.

## Коммутаторы Store-and-Forward

Коммутаторы Store-and-Forward (SAF) представляют собой наиболее дорогие, сложные и совершенные устройства данного типа. Они уже гораздо ближе к мостам и лишены перечисленных недостатков коммута-

торов Cut-Trough. Главное их отличие состоит в полном буферировани во внутренней буферной памяти FIFO всех ретранслируемых пакето Размер каждого буфера при этом должен быть не меньше максимально длины пакета. Соответственно значительно возрастает и задержка комму тации, она составляет не менее 12000 битовых интервалов. Карликовы пакеты (меньше 512 бит) и ошибочные пакеты (с неправильной кон трольной суммой) таким коммутатором отфильтровываются и не пересы лаются. Перегрузки возникают гораздо реже, так как есть возможност отложить на время передачу пакета.

Буферная память (с организацией FIFO) может размещаться н принимающей стороне всех портов (накопление перед коммутацией · рис. 13.8), на передающей стороне портов (накопление перед ретрансля цией), а также может быть общей для всех портов, причем эти методы ча сто комбинируются для достижения наибольшей гибкости и увеличени производительности. Чем больше объем памяти, тем лучше коммутато справляется с перегрузкой. Но с ростом объема памяти повышается стоимость оборудования. Растет и требование к быстродействию комму татора. Иногда в состав коммутатора включается и универсальный про цессор, но чаще коммутаторы выполняются на специализированных бы стродействующих микросхемах, жестко специализированных именно н задачах коммутации пакетов.

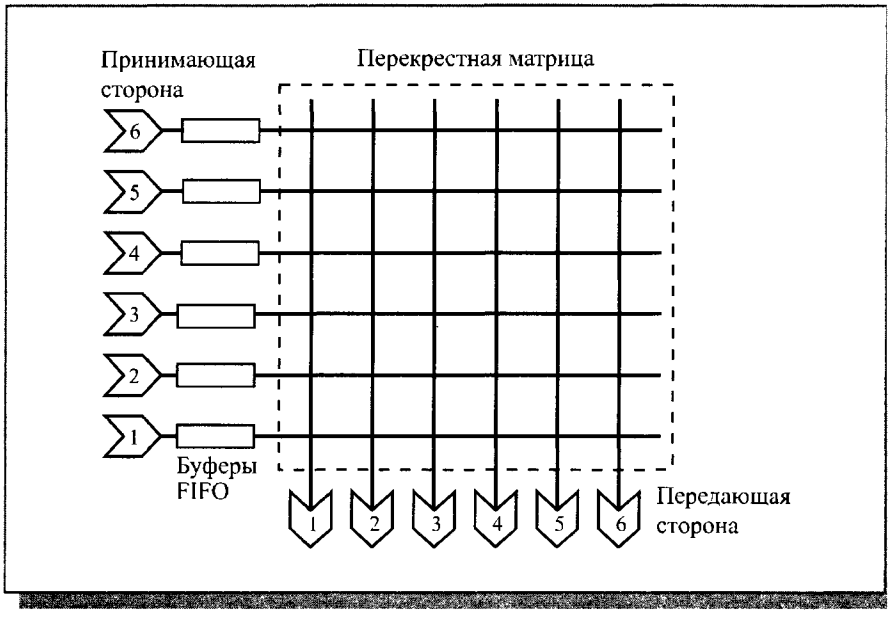



**Рис. 13.8.** Буферная память в коммутаторе

Коммутаторы SAF в отличие от других типов коммутаторов могут поддерживать одновременно разные скорости передачи (10 Мбит/с и 100 Мбит/с). Полное буферирование пакета вполне позволяет передавать его не с той скоростью, с которой он поступил. В результате часть портов коммутатора может работать с сетью Ethernet, другая – с Fast Ethernet, причем некоторые коммутаторы автоматически настраивают свои порты на скорость передачи подключенного к порту сегмента. Коммутаторы SAF облегчают переход с Ethernet на Fast Ethernet. Существуют уже и коммутаторы, поддерживающие обмен с Gigabit Ethernet на скорости 1000 Мбит/с. Но в отличие от мостов коммутаторы, как правило, не меняют формат пакетов, поэтому сети с разными форматами пакетов нельзя объединять с их помощью.

Также выпускаются так называемые гибридные (или адаптивные) коммутаторы, которые могут автоматически переключаться из режима Cut-Through в режим SAF и наоборот. При малой нагрузке и низком уровне ошибок они работают как более быстрые Cut-Through коммутаторы, а при большой нагрузке и значительном количестве ошибок переходят в более медленный, но более качественный режим SAF.

Наконец, еще одно важное достоинство коммутаторов по сравнению с репитерными концентраторами состоит в том, что они могут поддерживать режим полнодуплексной связи. Как уже отмечалось, при этом режиме упрощается обмен в сети, а скорость передачи в идеале удваивается (20 Мбит/с для Ethernet, 200 Мбит/с для Fast Ethernet).

Достоинства и недостатки полнодуплексного режима следующие.

Сегменты на витой паре и на оптоволоконном кабеле в любом случае используют две линии связи, которые передают информацию в разные стороны. (Это не относится к сегментам 100BASE-T4, содержащим двунаправленные витые пары, передающие в обе стороны по очереди). Но в стандартном полудуплексном режиме информация не передается по этим линиям связи одновременно (это означает коллизию, в результате чего передача прекращается).

Однако, если адаптер и коммутатор, связанные этими же двумя линиями, поддерживают полнодуплексный режим, то одновременная передача информации возможна. Несомненно, аппаратура адаптера и коммутатора должна при этом обеспечивать прием приходящего из сети пакета и передачу своего пакета одновременно.

Полнодуплексный режим в принципе исключает любую возможность коллизии и делает ненужным сложный алгоритм управления обменом CSMA/CD. Каждый из абонентов (адаптер и коммутатор) может передавать в данном случае в любой момент без ожидания освобождения сети. В результате сеть нормально функционирует даже при нагрузке, приближающейся к 100% (в полудуплексном режиме – не более 30–40%).

Этот режим удобен для высокоскоростных серверов и высокопроизводительных рабочих станций.

Кроме того, отказ от метода CSMA/CD автоматически снимает ограничения на размер сети, связанные с ограничениями на двойное время распространения сигнала. Особенно это важно для Fast Ethernet и Gigabit Ethernet. При полнодуплексном режиме обмена размер любой сети ограничен только затуханием сигнала в среде передачи. Поэтому, например, сети Fast Ethernet и Gigabit Ethernet могут использовать оптоволоконные сегменты длиной 2 километра или даже больше. При стандартном полудуплексном режиме и методе CSMA/CD это было бы в принципе невозможно, так как двойное время распространения сигнала для Fast Ethernet не должно превышать 5,12 мкс, а для Gigabit Ethernet – 0,512 мкс (а при переходе на минимальную длину пакета в 512 байт – 4,096 мкс).

Таким образом, полнодуплексный режим можно рассматривать как приближение к топологии классической (активной) звезды. Как и в активной звезде, здесь не может быть конфликтов, но требования к центру (как по надежности, так и по быстродействию) чрезвычайно велики. Как и при активной звезде, строить сети с большим количеством абонентов затруднительно, необходимо использовать много центров (в данном случае – коммутаторов). Как и при активной звезде, стоимость оборудования оказывается довольно высокой, так как кроме сетевых адаптеров и соединительных кабелей нужны сложные, быстрые и дорогие коммутаторы. Но, видимо, все это неизбежная плата за повышение скорости обмена. Строго говоря, полнодуплексные сети уже трудно назвать классическими Ethernet и Fast Ethernet, так как в них уже ничего не остается ни от топологии «шина», ни от метода CSMA/CD. Сохраняется только формат пакета и (не всегда) метод кодирования.

В настоящее время коммутирующие концентраторы (коммутаторы) выполняют все больше функций, традиционно относившихся к мостам. В пределах одной сети или однотипных сетей с одинаковыми форматами пакетов (Ethernet и Fast Ethernet) коммутаторы все больше вытесняют мосты, так как они более быстрые и дешевые. На долю мостов остается только соединение разнотипных сетей, что встречается не так уж и часто. Эта тенденция прослеживается и в других областях электроники: узко специализированные быстрые устройства вытесняют универсальные, более медленные.

## Мосты и маршрутизаторы Ethernet и Fast Ethernet

Мосты и маршрутизаторы, строго говоря, не совсем правильно относить к специфическому сетевому оборудованию. Изначально они представляли собой универсальные компьютеры, работающие в сети и

выполняющие специфическую функцию соединения двух или более частей сети. Правда, сейчас уже существуют мосты и маршрутизаторы, жестко специализированные на работе в сети. В частности, маршрутизаторы выпускаются рядом фирм в виде модулей, устанавливаемых в концентраторы на базе шасси. Их стоимость ниже, чем маршрутизаторов на базе компьютеров, а быстродействие выше, так как они узко специализированы.

### Функции мостов

Мосты до недавнего времени были основными устройствами, применявшимися для разбиения сети на части (то есть для сегментирования сети). Их стоимость меньше, чем у маршрутизаторов, а быстродействие выше, к тому же они, как и коммутаторы, прозрачны для протоколов второго уровня модели OSI. Абоненты сети могут не знать о наличии в сети мостов, и все их пакеты доходят до нужного адресата по сети без всяких проблем.

По функциям мост очень близок к коммутатору, но медленнее, чем коммутатор.

Мост обычно имеет от двух до четырех портов, причем каждый из них соединен с одним из сегментов сети. В случае, когда мост выполняется на базе универсального компьютера, в этот компьютер просто устанавливается нужное число сетевых адаптеров, и к каждому из адаптеров подключается сегмент сети. Коммутатор в этом смысле гораздо удобнее, он имеет значительно больше портов (не менее 8).

Как и в случае коммутаторов, конфигурация сети с мостами может быть довольно сложной (рис. 13.9), но в ней ни в коем случае не должно быть замкнутых маршрутов (петель), то есть альтернативных путей доставки пакетов (рис. 13.10). Это связано в первую очередь с тем, что мосты, как и коммутаторы, прозрачны для широковещательных пакетов. Если в сети есть петли, то в результате многократного прохождения широковещательных пакетов по замкнутому маршруту возникают перегрузки сети (так называемые широковещательные штормы) и ряд других проблем.

Для того, чтобы этого не происходило, в мостах предусматривается так называемый *алгоритм остовного дерева* (spanning tree), который позволяет отключать порты, участвующие в создании петель (например, оба порта моста 2 на рис. 13.10) в результате диалога (обмена управляющими пакетами) между всеми мостами сети. Благодаря этому, можно специально дублировать соединение сегментов посредством мостов (создавать петли) с тем, чтобы при отказе одной из линий связи автоматически восстанавливать целостность сети по альтернативному маршруту.

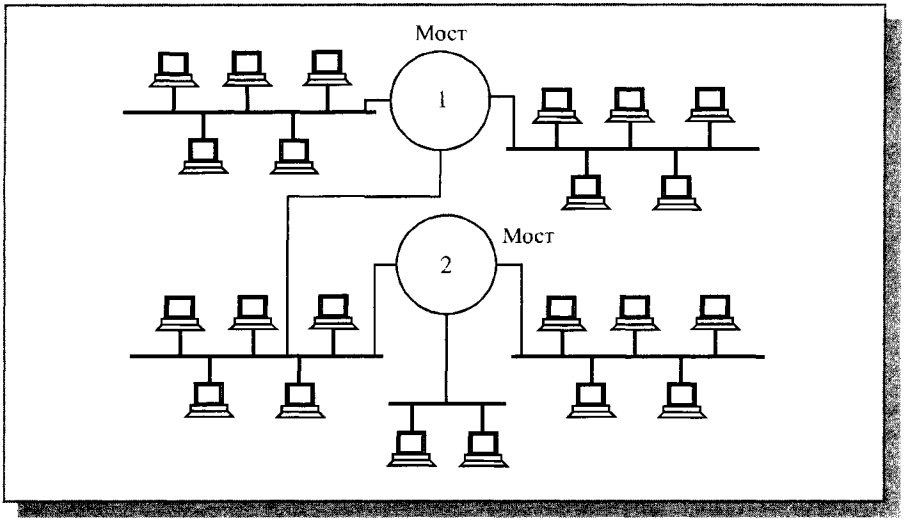



**Рис.13.9.** Сеть с мостами

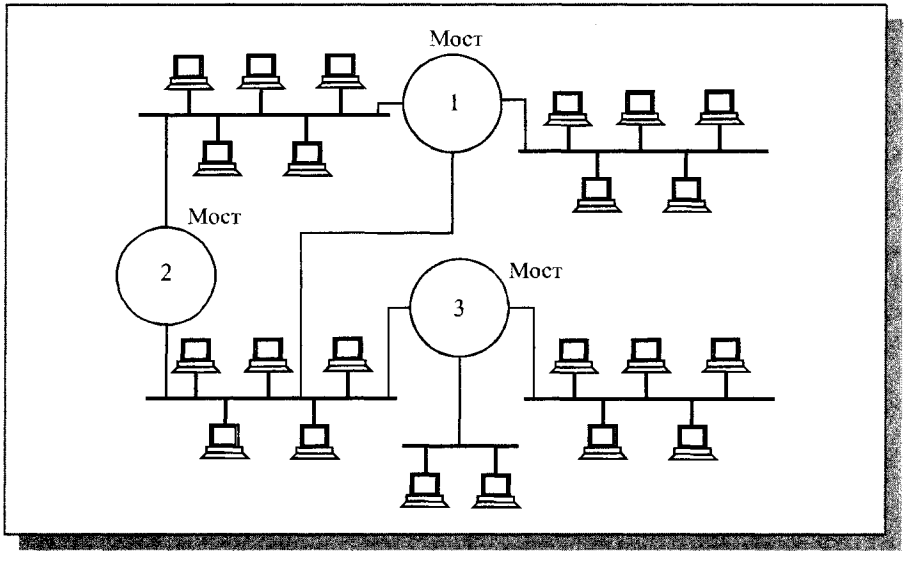



**Рис. 13.10.** Петля в сети с мостами

Коммутаторы обычно не поддерживают алгоритм остовного дерева за исключением самых сложных и дорогих. Так что в этом смысле мост более универсален, чем коммутатор.

Традиционно мосты подразделяются на внутренние и внешний.

*Внутренние мосты* выполняются на основе компьютера-сервера, в который устанавливают сетевые адаптеры (обычно до четырех), подключенные к разным сегментам сети. Строго говоря, именно эти сетевые адаптеры и соответствующие программные средства и называются внутренним мостом.

*Внешний мост* представляет собой рабочую станцию, в которую установлены два сетевых адаптера. В этом случае, в отличие от внутреннего моста, сегменты могут быть только однотипными (например, Ethernet — Ethernet).

Внешний мост может быть *выделенным* (dedicated) или *невыделенным* (non-dedicated) в зависимости от того, выполняет ли компьютер рабочей станции еще какие-нибудь функции, кроме сетевых. Термин «внешний» употребляется в этом случае по отношению к серверу как основному компьютеру сети. В любой сети может присутствовать одновременно как внешний, так и внутренний мост или несколько мостов.

Мосты, как и коммутаторы, разделяют зону конфликта (область коллизии, Collision Domain), но не разделяют широковещательную область (Broadcast Domain), то есть ту часть сети, в которой свободно проходят широковещательные пакеты. В результате разделения зоны конфликта нагрузка на каждый сегмент уменьшается, а ограничения на размер сети преодолеваются.

Одновременно мост может обрабатывать (ретранслировать) только один пакет, а не несколько, как коммутатор. Дело в том, что все функции моста выполняются последовательно одним центральным процессором. Именно поэтому мост работает значительно медленнее, чем коммутатор.

Как и в коммутаторе, любой пакет, приходящий на один из портов моста, обрабатывается следующим образом:

1. Мост выделяет MAC-адрес источника (отправителя) пакета и ищет его в таблице адресов абонентов, относящейся к данному порту. Если этого адреса в таблице нет, то он туда добавляется. Таким образом, автоматически формируется таблица адресов всех абонентов каждого сегмента из подключенных к портам моста.
2. Мост выделяет адрес приемника (получателя) пакета и ищет его в таблицах адресов, относящихся ко всем портам. Если пакет адресован в тот же сегмент, из которого он пришел, то он не ретранслируется (отфильтровывается). Если пакет широковещательный или многопунктовый (групповой), то он ретранслируется во все порты кроме принявшего. Если пакет однопунктовый (адресован одному абоненту), то он ретранслируется только в тот порт, к которому присоединен сегмент с этим абонентом. Наконец, если адрес приемника не обнаружен ни в одной из таблиц адресов, то пакет посылается во все порты, кроме принявшего (как широковещательный).

Таблицы адресов абонентов имеют ограниченный размер, поэтому они формируются так, чтобы иметь возможность автоматического обновления их содержимого. Адреса тех абонентов, которые долго не присылают пакетов, через заданное время (по стандарту IEEE 802.1D оно равно 5 минут) стираются из таблицы. Это гарантирует, что адрес абонента, отключенного от сети или перенесенного в другой сегмент, не будет занимать лишнего места в таблице.

Поскольку мост, подобно коммутатору, анализирует информацию внутри кадра (физические адреса, MAC-адреса), часто говорят, что он ретранслирует кадры, а не пакеты (в отличие от репитера или репитерного концентратора).

Как и в случае коммутаторов, для эффективной работы моста необходимо выполнять упоминавшееся «правило 80/20», то есть большинство передач (не менее 80%) должно быть внутрисегментными, а не межсегментными.

Подобно коммутаторам Store-and-Forward, мосты могут поддерживать обмен между сегментами с разной скоростью передачи (Ethernet и Fast Ethernet), а также обеспечивать сопряжение полудуплексных и полнодуплексных сегментов. Полный прием пакетов в буферную память моста и их последующая передача легко решают такие проблемы.

Как видно из вышесказанного, мосты и коммутаторы очень близки по своим характеристикам.

Однако у моста есть большое преимущество. Мосты могут не только соединять одноименные сегменты, но также сопрягать сети Ethernet и Fast Ethernet с сетями любых других типов, например, FDDI или Token-Ring, что не по силам большинству коммутаторов. Поэтому мосты, хоть и вытесняются коммутаторами, все-таки в ближайшее время не исчезнут.

### Функции маршрутизаторов

Вытесняя мосты, коммутаторы сильно потеснили и маршрутизаторы. Но маршрутизаторы работают на более высоком, третьем уровне модели OSI (мосты и коммутаторы – на втором), они имеют дело с протоколами более высоких уровней. Поэтому им, скорее всего, не грозит полное исчезновение.

Маршрутизаторы, как и мосты или коммутаторы, ретранслируют пакеты из одной части сети в другую (из одного сегмента в другой). Изначально маршрутизатор от моста отличался только тем, что на компьютере, соединяющем две или более части сети, было установлено другое программное обеспечение. Но между маршрутизатором и мостом существуют и принципиальные отличия:

- Маршрутизаторы работают не с физическими адресами пакетов (MAC-адресами), а с логическими сетевыми адресами (IP-адресами или IPX-адресами).
- Маршрутизаторы ретранслируют не всю приходящую информацию, а только ту, которая адресована им лично, и отбрасывают (не ретранслируют) широковещательные пакеты, разделяя тем самым широковещательную область сети (Broadcast Domain). Все абоненты обязательно должны знать о присутствии в сети маршрутизатора. Они не прозрачны для абонентов в отличие от мостов и коммутаторов.
- Самое главное – маршрутизаторы поддерживают сети с множеством возможных маршрутов и путей передачи информации — так называемые ячеистые сети (meshed networks). Пример такой сети показан на рис. 13.11. Мосты же требуют, чтобы в сети не было петель, чтобы путь распространения информации между двумя любыми абонентами был единственным.

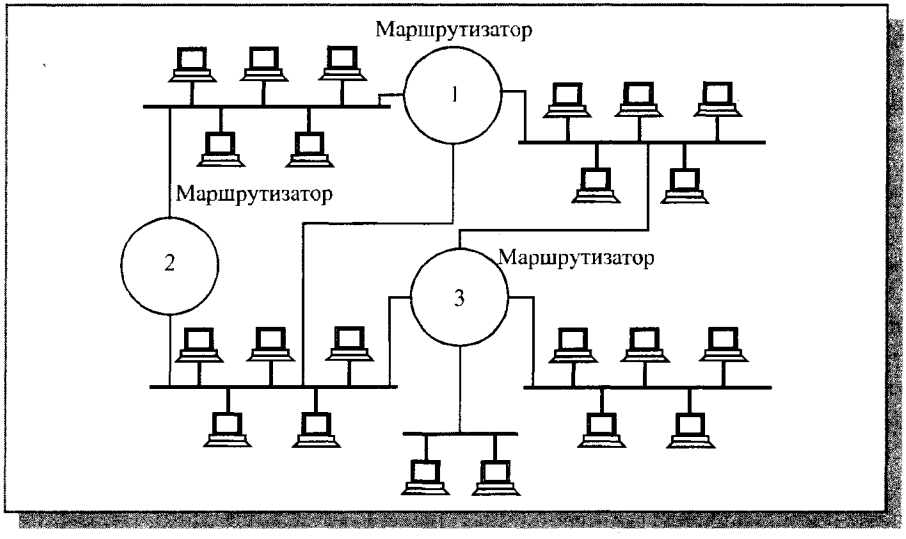



**Рис. 13.11.** Ячеистая сеть с маршрутизаторами

Маршрутизаторы сложнее мостов и коммутаторов и, следовательно, дороже (например, стоимость коммутации в Ethernet примерно в 10 раз ниже стоимости маршрутизации). Маршрутизаторами сложнее управлять, они почти всегда значительно медленнее коммутаторов. Зато они обеспечивают самое глубокое разделение сети на части.

Если репитерные концентраторы всего лишь повторяют все поступившие на них пакеты (уровень 1 модели OSI), а коммутаторы и мосты ретранслируют только межсегментные и широковещательные пакеты

(уровень 2 модели OSI), то маршрутизаторы соединяют практически самостоятельные, не зависящие друг от друга сети, сохраняя при этом возможность передачи информации между ними (уровень 3 модели OSI).

Размер сети с маршрутизаторами практически ничем не ограничен: ни допустимыми размерами зоны конфликтов, ни допустимым количеством широковещательных пакетов (которые могут просто не оставлять места для обычных, однопунктовых пакетов), ни возможными для коммутаторов и мостов разнообразными перегрузками. При этом легко обеспечиваются альтернативные, дублирующие пути распространения информации для увеличения надежности связи.

Для принятия решения о выборе маршрута каждый маршрутизатор формирует в своей памяти таблицы данных, которые содержат:

- Номера всех сетей, подключенных к данному маршрутизатору;
- Список всех соседних маршрутизаторов;
- Список MAC-адресов и IP (IPX)-адресов всех абонентов сетей, подключенных к маршрутизатору. Этот список автоматически обновляется, как и в случае мостов и коммутаторов.

Кроме того, список всех доступных маршрутизаторов должен быть у каждого абонента сети.

Именно маршрутизаторы чаще всего используются для связи локальных сетей с глобальными, в частности, с Интернетом, который может рассматриваться как полностью маршрутизируемая сеть. Преобразовать протоколы локальных сетей в протоколы глобальных сетей для маршрутизатора вполне по силам.

Маршрутизаторы часто применяются для объединения опорной (стержневой) сетью типа FDDI множества локальных сетей (рис. 13.12)

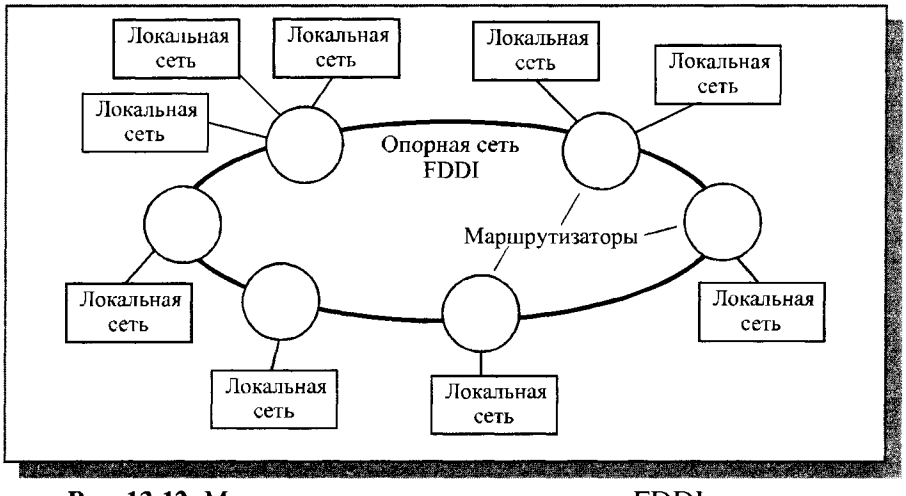



**Рис. 13.12.** Маршрутизируемая сеть на основе FDDI

или для связи локальных сетей разных типов. Преобразование формата пакетов, требуемое в данной ситуации, для маршрутизатора не представляет никакой сложности. Например, большие пакеты сети FDDI могут разбиваться (фрагментироваться) на несколько меньших пакетов Ethernet.

Маршрутизаторы также легко преобразуют скорости передачи, связывая, например, между собой сети Ethernet, Fast Ethernet и Gigabit Ethernet. Не пропуская широковещательных пакетов, они лучше справляются с этой задачей, чем мосты или коммутаторы, так как защищают медленные сегменты от перегрузок со стороны быстрых сегментов.

Маршрутизаторы иногда объединяют между собой. Множество сопряженных друг с другом маршрутизаторов могут образовывать так называемое облако (Cloud), представляющее собой, по сути, один гигантский маршрутизатор. Такое соединение обеспечивает исключительно гибкую и надежную связь между всеми подключенными к нему локальными сетями (рис. 13.13).

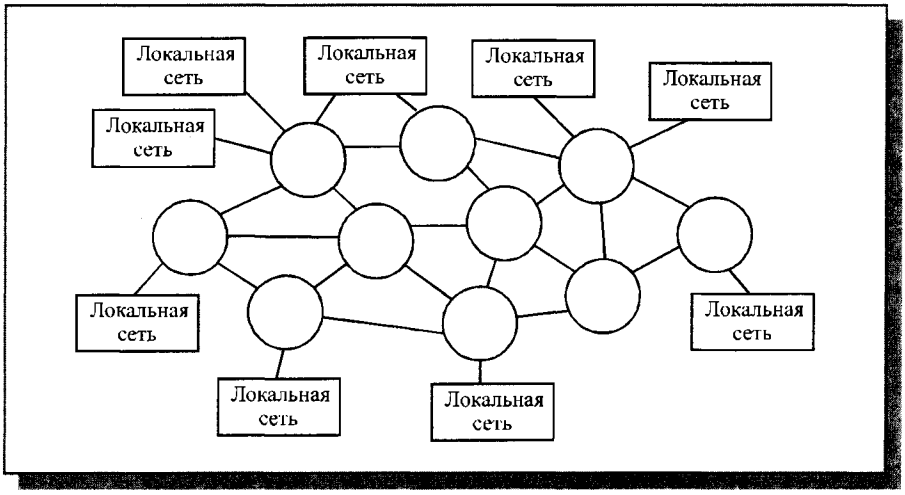



**Рис. 13.13.** Маршрутизируемое облако

Как уже отмечалось, можно считать, что репитерные концентраторы работают с пакетами, а мосты и коммутаторы – с кадрами. Маршрутизаторы обрабатывают адресную информацию, относящуюся к структуре дейтаграммы IP (IPX), которая вложена в область данных кадра, в свою очередь вложенного в пакет (рис. 13.14). Поэтому говорят, что они работают с дейтаграммами, или ретранслируют дейтаграммы. Маршрутизатор анализирует сетевой IP-адрес дейтаграммы (см. рис. 6.9) или сетевой IPX-адрес дейтаграммы (см. рис. 6.8). В оба эти адреса входят номер сети, и

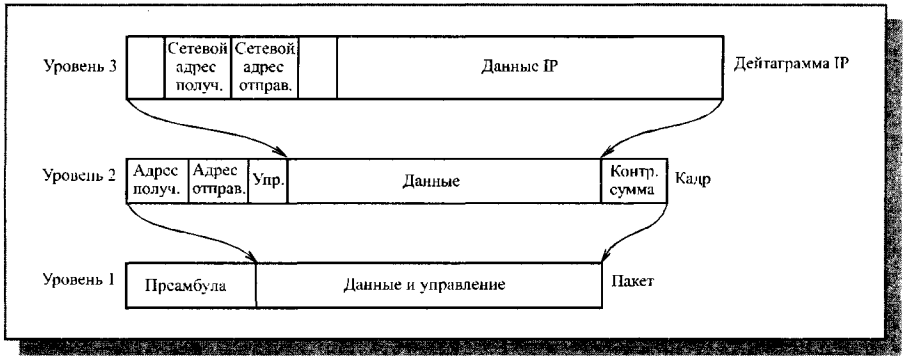



**Рис. 13.14.** Вложение дейтаграммы в кадр и пакет

именно эти сети соединяет маршрутизатор. Сетями в данном случае называются широковещательные области (Broadcast Domain).

Каждый абонент, прежде чем послать пакет, определяет, может ли он послать его непосредственно получателю или же ему надо воспользоваться услугами маршрутизатора. Если номер собственной сети передающего абонента совпадает с номером сети абонента, которому должен передаваться пакет, то пакет передается непосредственно, без маршрутизации. Если же адресат находится в другой сети, то передаваемая дейтаграмма должна быть отправлена маршрутизатору, который затем переправит ее в нужную сеть. При этом получается, что пакет в целом адресован маршрутизатору (как одному из абонентов собственной сети), а заключенная в нем дейтаграмма адресована абоненту из другой сети, которому она, собственно, и предназначена.

Маршрутизатор анализирует IP (или IPX) адреса в приходящей в составе пакета дейтаграмме и преобразует пакет, пришедший по одной из сетей, в пакет, предназначенный для другой сети. В поле адресов передаваемого пакета он ставит MAC-адрес получателя и свой MAC-адрес, как отправителя пакета. Ответный пакет точно так же должен пройти через посредника – маршрутизатора.

Хороший маршрутизатор очень дорог и сложен в настройке и эксплуатации. Поэтому использовать его следует только в тех случаях, когда это действительно необходимо, например, когда применение коммутаторов и мостов не позволяет преодолеть перегрузку сети.

# Глава 10. Выбор конфигурации сетей Ethernet и Fast Ethernet

## Лекция 14. Выбор конфигурации сетей Ethernet и Fast Ethernet

**В этой лекции дается представление о методах оценки работоспособности различных конфигураций сетей Ethernet и Fast Ethernet, моделях, применяемых для этого, а также о способах преодоления ограничений, обусловленных особенностями данной сети.**

**Ключевые слова:** зона конфликта, двойное время прохождения сигнала, сокращение межпакетного интервала, начальные, конечные и промежуточные сегменты, путь максимальной длины.

### Выбор конфигурации Ethernet

При выборе конфигурации сети Ethernet, состоящей из сегментов различных типов, возникает много вопросов, связанных прежде всего с максимально допустимым размером (диаметром) сети и максимально возможным числом различных элементов. Сеть будет работоспособной только в том случае, если задержка распространения сигнала в ней не превысит предельной величины. Это определяется выбранным методом управления обменом CSMA/CD, основанном на обнаружении и разрешении коллизий.

Прежде всего, следует отметить, что для получения сложных конфигураций Ethernet из отдельных сегментов применяются промежуточные устройства двух основных типов:

- Репитерные концентраторы (хабы) представляют собой набор репитеров и никак логически не разделяют сегменты, подключенные к ним;
- Коммутаторы передают информацию между сегментами, но не передают конфликты с сегмента на сегмент.

При использовании более сложных коммутаторов конфликты в отдельных сегментах решаются на месте, в самих сегментах, но не распространяются по сети, как в случае применения более простых репитерных концентраторов. Это имеет принципиальное значение для выбора топологии сети Ethernet, так как используемый в ней метод доступа CSMA/CD предполагает наличие конфликтов и их разрешение, причем общая длина

сети как раз и определяется размером зоны конфликта, области коллизии (collision domain). Таким образом, применение репитерного концентратора не разделяет зону конфликта, в то время как каждый коммутирующий концентратор делит зону конфликта на части. В случае применения коммутатора оценивать работоспособность надо для каждого сегмента сети *отдельно*, а при использовании репитерных концентраторов – для сети в целом.

На практике репитерные концентраторы применяются гораздо чаще, так как они и проще и дешевле. Поэтому в дальнейшем речь пойдет именно о них.

При выборе и оценке конфигурации Ethernet используются две основные модели.

### Правила модели 1

Первая модель формулирует набор правил, которые необходимо соблюдать проектировщику сети при соединении отдельных компьютеров и сегментов:

1. Репитер или концентратор, подключенный к сегменту, снижает на единицу максимально допустимое число абонентов, подключаемых к сегменту.
2. Полный путь между двумя любыми абонентами должен включать в себя не более пяти сегментов, четырех концентраторов (репитеров) и двух трансиверов (MAU).
3. Если путь между абонентами состоит из пяти сегментов и четырех концентраторов (репитеров), то количество сегментов, к которым подключены абоненты, не должно превышать трех, а остальные сегменты должны просто связывать между собой концентраторы (репитеры). Это уже упоминавшееся «правило 5-4-3».
4. Если путь между абонентами состоит из четырех сегментов и трех концентраторов (репитеров), то должны выполняться следующие условия:
   - максимальная длина оптоволоконного кабеля сегмента 10BASE-FL, соединяющего между собой концентраторы (репитеры), не должна превышать 1000 метров;
   - максимальная длина оптоволоконного кабеля сегмента 10BASE-FL, соединяющего концентраторы (репитеры) с компьютерами, не должна превышать 400 метров;
   - ко всем сегментам могут подключаться компьютеры.

При выполнении перечисленных правил можно быть уверенным, что сеть будет работоспособной. Никаких дополнительных расчетов в данном случае не требуется. Считается, что соблюдение данных правил гарантирует допустимую величину задержки сигнала в сети.

На рис. 14.1 показан пример максимальной конфигурации, удовлетворяющей этим правилам. Здесь максимально возможный путь (диаметр сети) проходит между двумя нижними по рисунку абонентами: он включает в себя пять сегментов (10BASE2, 10BASE5, 10BASE-FL, 10BASE-FL и 10BASE-T) четыре концентратора (репитера) и два трансивера MAU.

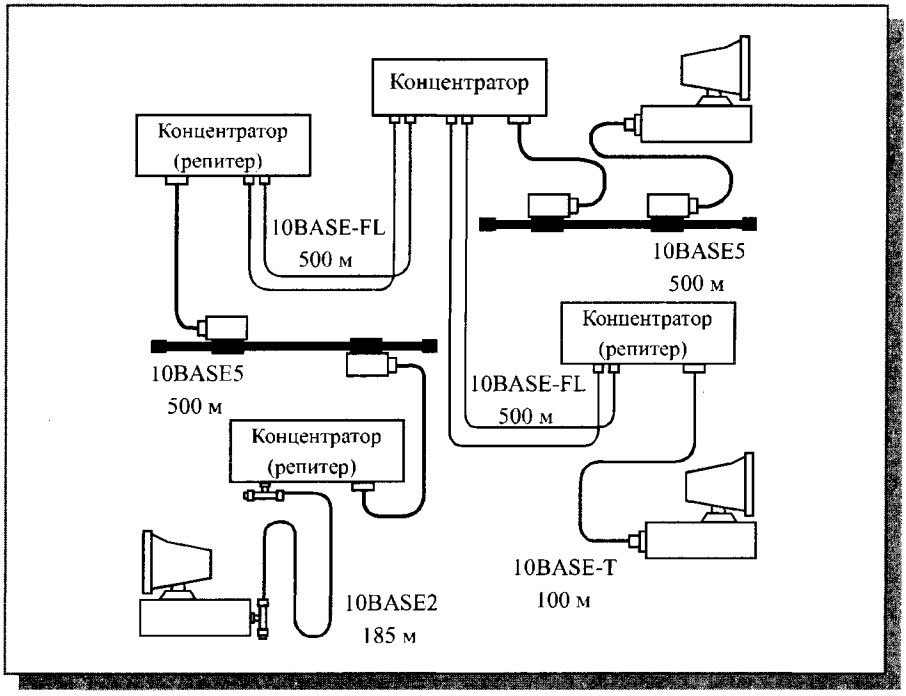



**Рис. 14.1.** Пример максимальной конфигурации в соответствии с первой моделью

## Расчет по модели 2

Вторая модель, применяемая для оценки конфигурации Ethernet, основана на точном расчете временных характеристик выбранной конфигурации сети. Эта модель иногда позволяет выйти за пределы жестких ограничений модели 1. Применение модели 2 необходимо в том случае, когда размер проектируемой сети близок к максимально допустимому.

В модели 2 используются две системы расчетов:

- первая система предполагает вычисление двойного (кругового) времени прохождения сигнала по сети и сравнение его с максимально допустимой величиной;

- вторая система проверяет допустимость величины получаемого межпакетного временного интервала, межпакетной щели (IPG – InterPacket Gap) в сети.

При этом вычисления в обеих системах расчетов ведутся для наихудшего случая, для пути максимальной длины, то есть для такого пути передаваемого по сети пакета, который требует для своего прохождения максимального времени.

При первой системе расчетов выделяются три типа сегментов:

- начальный сегмент, соответствующий началу пути максимальной длины;
- конечный сегмент, расположенный в конце пути максимальной длины;
- промежуточный сегмент, входящий в путь максимальной длины, но не являющийся ни начальным, ни конечным.

Промежуточных сегментов в выбранном пути может быть несколько, а начальный и конечный сегменты при разных расчетах могут меняться местами друг с другом. Выделение этих трех типов сегментов позволяет автоматически учитывать задержки сигнала на всех концентраторах, входящих в путь максимальной длины, а также в приемопередающих узлах адаптеров.

Для расчетов используются величины задержек, представленные в таблице 14.1.

**Таблица 14.1.** Величины задержек для расчета двойного времени прохождения сигнала (задержки даны в битовых интервалах)

| Тип сегмента Ethernet | Макс. длина м | Начальный сегмент | | Промежуточный сегмент | | Конечный сегмент | | Задержка на метр длины |
|---|---|---|---|---|---|---|---|---|
| | | $t_0$ | $t_m$ | $t_0$ | $t_m$ | $t_0$ | $t_m$ | $t_l$ |
| 10BASE5 | 500 | 11,8 | 55,0 | 46,5 | 89,8 | 169,5 | 212,8 | 0,087 |
| 10BASE2 | 185 | 11,8 | 30,8 | 46,5 | 65,5 | 169,5 | 188,5 | 0,103 |
| 10BASE-T | 100 | 15,3 | 26,6 | 42,0 | 53,3 | 165,0 | 176,3 | 0,113 |
| 10BASE-FL | 2000 | 12,3 | 212,3 | 33,5 | 233,5 | 156,5 | 356,5 | 0,100 |
| FOIRL | 1000 | 7,8 | 107,8 | 29,0 | 129,0 | 152,0 | 252,0 | 0,100 |
| AUI | 50 | 0 | 5,1 | 0 | 5,1 | 0 | 5,1 | 0,103 |

Методика расчета сводится к следующему:

1. В сети выделяется путь максимальной длины. Все дальнейшие расчеты ведутся для него. Если этот путь не очевиден, то рассчитываются все возможные пути, затем на основании этого выбирается путь максимальной длины.

2. Если длина сегмента, входящего в выбранный путь, не максимальна, то рассчитывается двойное (круговое) время прохождения в каждом сегменте выделенного пути по формуле: $t_s = L_{t1} + t_o$, где L — это длина сегмента в метрах (при этом надо учитывать тип сегмента: начальный, промежуточный или конечный).
3. Если длина сегмента равна максимально допустимой, то из таблицы для него берется величина максимальной задержки $t_m$.
4. Суммарная величина задержек всех сегментов выделенного пути не должна превышать предельной величины 512 битовых интервалов (51,2 мкс).
5. Затем необходимо проделать те же действия для обратного направления выбранного пути (то есть в данном случае конечный сегмент считается начальным и наоборот). Из-за разных задержек передающих и принимающих узлов концентраторов величины задержек в разных направлениях могут отличаться (но незначительно).
6. Если задержки в обоих случаях не превышают величины 512 битовых интервалов, то сеть считается работоспособной.

В частности, для конфигурации, показанной на рис. 14.1, путь наибольшей длины – это путь между двумя нижними по рисунку компьютерами. В данном случае это довольно очевидно. Этот путь включает в себя пять сегментов (слева направо): 10BASE2, 10BASE5, 10BASE-FL (два сегмента) и 10BASE-T.

К примеру, можно произвести расчет, считая начальным сегментом 10BASE2, а конечным 10BASE-T:

1. Начальный сегмент 10BASE2 имеет максимально допустимую длину (185 метров), для него следует взять из таблицы величину задержки 30,8.
2. Промежуточный сегмент 10BASE5 также имеет максимально допустимую длину (500 метров), поэтому для него нужно взять из таблицы величину задержки 89,8.
3. Оба промежуточных сегмента 10BASE-FL имеют длину 500 метров, следовательно, задержка каждого из них будет вычисляться по формуле:

   $500 \times 0{,}100 + 33{,}5 = 83{,}5.$
4. Конечный сегмент 10BASE-T имеет максимально допустимую длину (100 метров), поэтому величина задержки для него в таблице равняется 176,3.
5. В путь наибольшей длины входят также шесть AUI-кабелей: два из них (в сегменте 10BASE5) показаны на рисунке, а четыре (в двух сегментах 10BASE-FL) не показаны, но в реальности вполне могут присутствовать. Можно считать, что суммарная длина всех этих кабелей

равна 200 метрам, то есть четырем максимальным длинам. Тогда задержка на всех AUI-кабелях будет равна:

$4 \times 5{,}1 = 20{,}4$.

6. В результате суммарная задержка для всех пяти сегментов составит:

$30{,}8 + 89{,}8 + 83{,}5 + 83{,}5 + 176{,}3 + 20{,}4 = 484{,}3$,

что меньше, чем предельно допустимая величина 512, то есть сеть работоспособна.

Теперь можно рассчитать суммарную задержку для того же пути, но в обратном направлении. При этом начальным сегментом будет 10BASE-T, а конечным – 10BASE2. В результате в конечной сумме изменятся только два слагаемых (промежуточные сегменты остаются промежуточными). Для начального сегмента 10BASE-T максимальной длины задержка составит 26,6 битовых интервалов, а для конечного сегмента 10BASE2 максимальной длины задержка составит 188,5 битовых интервалов. Суммарная задержка будет равняться:

$26{,}6 + 83{,}5 + 83{,}5 + 89{,}8 + 188{,}5 + 20{,}4 = 492{,}3$,

что опять же меньше 512. Работоспособность сети подтверждена.

Однако для того, чтобы сделать окончательный вывод о работоспособности сети, расчета двойного времени прохождения, в соответствии со стандартом, еще не достаточно.

Второй расчет, применяемый в модели 2, проверяет соответствие стандарту величины межпакетного интервала (IPG). Эта величина изначально не должна быть меньше, чем 96 битовых интервалов (9,6 мкс), то есть только через 9,6 мкс после освобождения сети абоненты могут начать свою передачу (см. Лекция 10 «Метод управления обменом CSMA/CD»). Однако при прохождении пакетов (кадров) через репитеры и концентраторы межпакетный интервал может сокращаться, вследствие чего два пакета могут в конце концов восприниматься абонентами как один. Допустимое сокращение IPG определено стандартом в 49 битовых интервалов (4,9 мкс).

Для вычислений здесь так же, как и в предыдущем случае, используются понятия начального и промежуточного сегментов. Конечный сегмент не вносит вклада в сокращение межпакетного интервала, так как пакет доходит по нему до принимающего компьютера без прохождения репитеров и концентраторов.

Вычисления здесь очень простые. Для них используется данные таблицы 14.2.

Для получения полной величины сокращения IPG надо просуммировать величины из таблицы для сегментов, входящих в путь максимальной длины, и сравнить сумму с предельной величиной 49 битовых интервалов. Если сумма меньше 49, можно сделать вывод о работоспособности сети. Для гарантии расчет производится в обоих направлениях выбранного пути.

**Таблица 14.2.** Величины сокращения межпакетного интервала (IPG) для разных сегментов Ethernet

| Сегмент | Начальный | Промежуточный |
|---|---|---|
| 10BASE2 | 16 | 11 |
| 10BASE5 | 16 | 11 |
| 10BASE-T | 16 | 11 |
| 10BASE-FL | 11 | 8 |

Для примера стоит обратиться все к той же конфигурации, показанной на рис. 14.1. Максимальный путь здесь – между двумя нижними по рисунку компьютерами. Можно взять в качестве начального сегмента 10BASE2. Для него сокращение межпакетного интервала равно 16. Далее следуют промежуточные сегменты: 10BASE5 (величина сокращения равна 11) и два сегмента 10BASE-FL (каждый из них внесет свой вклад по 8 битовых интервалов). В результате суммарное сокращение межпакетного интервала составит:

$$16 + 11 + 8 + 8 = 43,$$

что меньше предельной величины 49. Следовательно, данная конфигурация и по этому показателю будет работоспособна.

Вычисления для обратного направления по этому же пути дадут тот же результат, так как начальный сегмент 10BASE-T даст ту же величину, что и начальный сегмент 10BASE2 (16 битовых интервалов). А все промежуточные сегменты останутся промежуточными.

Теперь можно попробовать с помощью второй модели расчетов оценить максимальный размер сети Ethernet. Теоретически возможный размер сети составляет 6,5 километров. Но это в предположении, что вся сеть выполнена на одном сегменте. Однако на практике это неосуществимо. Ведь предельная длина сегмента не превышает 2 километров (для 10BASE-FL). Присутствие репитеров или концентраторов в сети максимального размера обязательно, а они внесут свой вклад в задержку прохождения сигнала по сети.

Простейшая конфигурация сети из двух сегментов 10BASE-FL, соединенных концентратором (рис. 14.2).

Из таблицы 14.1 видно, что при выборе максимальной длины обоих сегментов по 2000 метров (один из них будет начальным, а другой – конечным) суммарная двойная задержка распространения составит:

$$212,3 + 356,5 = 568,8,$$

что значительно больше допустимой величины 512. Таким образом, реальная длина сети будет даже меньше, чем 4 километра. Элементарный

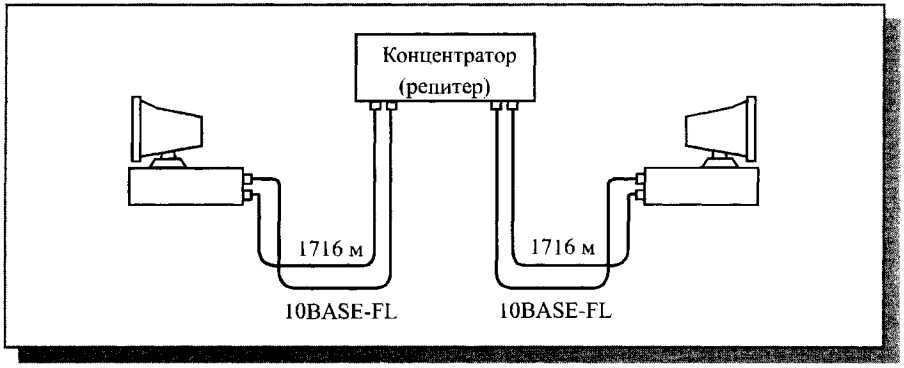



**Рис. 14.2.** Сеть Ethernet максимально возможной длины

расчет показывает, что при двух одинаковых сегментах 10BASE-FL длина каждого из них не должна превышать 1716 метров. Двойная задержка распространения при этом будет вычисляться так (табл. 14.1):

$$12{,}3 + 1716\ 0{,}1 + 156{,}5 + 1716\ 0{,}1 = 512.$$

Общая длина сети при этом составит 3432 метра, что значительно меньше теоретически возможной длины в 6500 метров.

Следует отметить, что сегменты в конфигурации на рис. 14.2 могут быть и разной длины, но их общая длина не должна превышать 3432 метров. При этом стоит еще учитывать, что в расчет не включены задержки трансиверных кабелей. Если используются внешние трансиверы, то необходимо еще уменьшить длину оптоволоконных кабелей.

Теперь можно попробовать оценить максимально возможный размер сети при использовании только электрического кабеля, например, наиболее популярной сейчас витой пары.

Допустим, имеется конфигурация из пяти сегментов 10BASE-T предельно допустимой длины (100 метров), соединенных между собой четырьмя концентраторами. Задержка начального сегмента составит (из табл. 14.1) 26,6 битовых интервалов. Задержка конечного сегмента будет равна 176,3 битовых интервалов. Задержка трех промежуточных сегментов будет составлять 53,3 битовых интервала на каждый сегмент.

Итого суммарная задержка равняется:

$$26{,}6 + 176{,}3 + 3 \times 53{,}3 = 362{,}8,$$

что меньше предельной величины 512.

Можно добавить еще два промежуточных 100-метровых сегмента, которые дадут еще 106,6, увеличив количество сегментов до 7, а число концентраторов — до 6. И еще останется запас в 42,6 битовых интервалов. Получается, что всего сегментов может быть даже 8 при семи концентраторах, а общая длина всех кабелей может достигать 705,3 метра. Это значительно превышает ограничения модели 1.

Можно подсчитать величину сокращения межпакетного интервала при такой конфигурации.

Один начальный сегмент даст 16 битовых интервалов (см. табл. 14.2). Шесть промежуточных сегментов дадут 77 битовых интервалов. В сумме получится 93 битовых интервала, что значительно превышает разрешенные 49 битовых интервалов. Поэтому в данном случае предельная длина сети будет ограничена всего лишь пятью сегментами, которые сократят межпакетный интервал на величину $16 + 11 \times 3 = 49$ битовых интервалов.

В результате сеть максимального размера на витой паре будет состоять из пяти сегментов по 100 метров (рис. 14.3), что совпадает с требованиями модели 1. Полная длина сети в этом случае равна 500 метрам. Предельная длина сети на одном сегменте 10BASE5 составляет те же самые 500 метров, но там не требуется применения концентраторов.

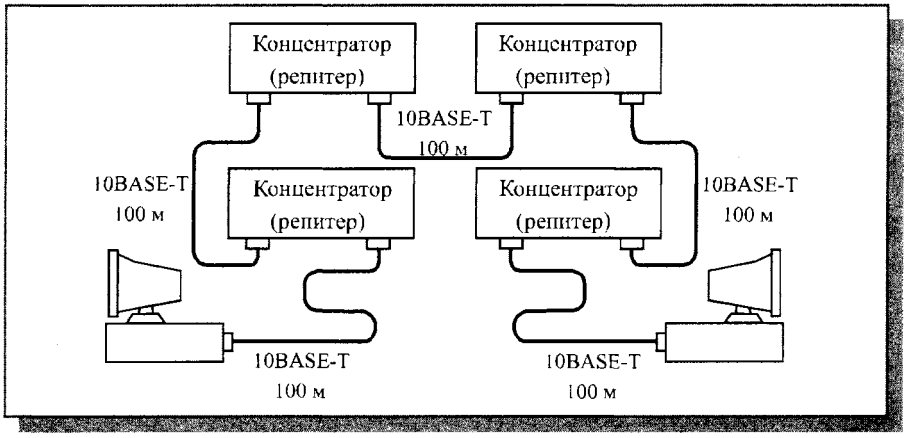



**Рис. 14.3.** Сеть Ethernet максимального размера на витой паре

Интересно, что пути максимальной длины для расчета круговой задержки и для расчета IPG могут быть различными. Вполне возможна ситуация, когда максимальную задержку прохождения дает один путь в сети, а максимальное сокращение IPG дает другой путь. Например, если один путь состоит из пяти коротких сегментов (электрических и оптоволоконных) и четырех концентраторов, а другой путь имеет всего два оптоволоконных сегмента, но зато с суммарной длиной, близкой к максимально возможной, то первый даст максимальное сокращение IPG, а второй – максимальную задержку прохождения сигнала.

Значит, в идеале необходимо рассчитывать как круговую задержку, так и сокращение IPG для каждого из возможных путей в данной топологии сети. А условие работоспособности сети будет состоять в том, что задержки всех путей должны быть меньше 512 битовых интервалов, а вели-

чины сокращения IPG для всех путей должны быть меньше 49 битовых интервалов. Правда, неоднозначность пути максимальной длины надо учитывать только в том случае, когда в сети присутствует больше четырех концентраторов, так как четыре концентратора (пять сегментов) в принципе не могут уменьшить APG больше, чем на 49 битовых интервалов при выборе любых возможных сегментов (см. табл. 14.2).

Таким образом, для оценки работоспособности той или иной конфигурации можно использовать обе модели (модель 1 и модель 2), хотя для сложных топологий и предельно длинных сегментов предпочтительнее вторая (числовая) модель, позволяющая количественно оценить временные характеристики сети. В случае же более простых топологий вполне достаточно проверить выполнение элементарных правил первой модели, что не требует никаких расчетов.

Если расчеты показывают, что сеть неработоспособна, то для преодоления этих ограничений предлагаются следующие методы:

1. Уменьшение длины кабелей с целью снижения задержки прохождения сигнала по сети (если возможно).
2. Уменьшение количества концентраторов для снижения задержек и сокращения IPG (если возможно).
3. Выбор кабеля с наименьшей задержкой. Кабели различных марок имеют разные задержки, то есть разные скорости распространения сигнала (см. табл. 2.3). Различия могут достигать 10%. Все данные в табл. 14.1 приведены для усредненного случая.
4. Разбиение сети на две части или более с помощью коммутатора – более радикальный метод. Коммутатор снижает требования к сети во столько раз, на сколько сегментов (зон конфликта) он разбивает сеть. Для каждой новой части сети требуется произвести расчет работоспособности еще раз. Сегмент, который присоединяет коммутатор, также входит в зону конфликта, и его надо учитывать при расчетах.
5. Использование полнодуплексного обмена. Полнодуплексный обмен снимает ограничения на размер сети из-за времени распространения сигнала, но требует больших затрат на замену полудуплексного оборудования.
6. Переход на другую локальную сеть (самый радикальный метод). Наиболее часто в таких случаях применяют сеть FDDI, которая позволяет строить максимальные по размеру сети. Правда, оборудование ее очень дорого, и для связи с сетью Ethernet нужны мосты.

## Выбор конфигурации Fast Ethernet

Точно так же, как и в случае Ethernet, для определения работоспособности сети Fast Ethernet стандарт IEEE 802.3 предлагает две модели,

называемые Transmission System Model 1 и Transmission System Model 2. Первая модель основана на нескольких несложных правилах. Она исходит из того, что все компоненты сети (в частности, кабели) имеют наихудшие из возможных временные характеристики, поэтому всегда дает результат со значительным запасом. Вторая модель использует систему точных расчетов с реальными временными характеристиками кабелей. В связи с этим ее применение позволяет иногда преодолеть жесткие ограничения модели 1.

## Правила модели 1

В соответствии с первой моделью, при выборе конфигурации надо руководствоваться следующими принципами:

- Сегменты, выполненные на электрических кабелях (витых парах) не должны быть длиннее 100 метров. Это относится к кабелям всех категорий – 3, 4 и 5, к сегментам 100BASE-T4 и 100BASE-TX.
- Сегменты, выполненные на оптоволоконных кабелях, не должны быть длиннее 412 метров.
- Если используются адаптеры с внешними (выносными) трансиверами, то трансиверные кабели (MII) не должны быть длиннее 50 сантиметров.

Модель 1 выделяет три возможные конфигурации сети Fast Ethernet:

1. Соединение двух абонентов (узлов) сети напрямую, без репитера или концентратора (рис.14.4). Абонентами при этом могут выступать не только компьютеры, но и сетевой принтер, порт коммутатора, моста или маршрутизатора. Такое сопряжение называется соединением DTE—DTE или двухточечным.
2. Соединение двух абонентов сети с помощью одного репитерного концентратора класса I или класса II (рис. 14.5).
3. Соединение двух абонентов сети с помощью двух репитерных концентраторов класса II (рис. 14.6). При этом предполагается, что для связи концентраторов всегда используется электрический кабель длиной не более 5 метров. Концентраторы класса II имеют меньшую задержку, поэтому их может быть два. Использование трех концентраторов в соответствии с моделью 1 не допускается.

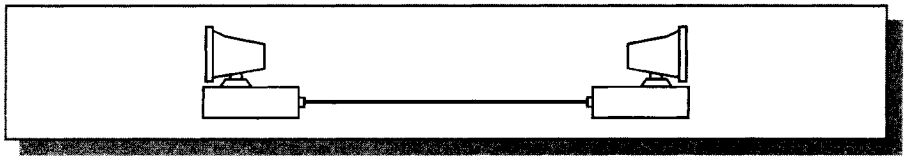


**Рис. 14.4.** Двухточечное соединение компьютеров без концентратора

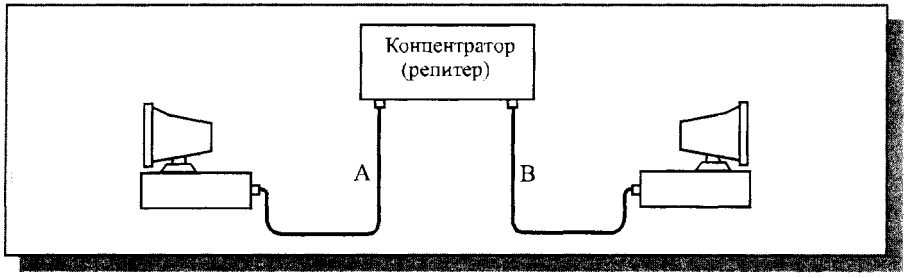



**Рис. 14.5.** Соединение с одним концентратором

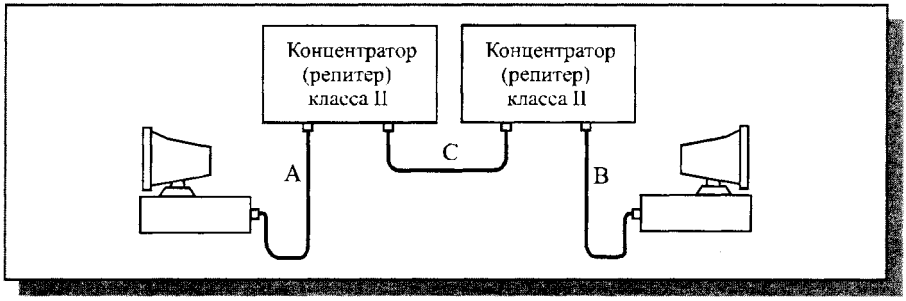



**Рис. 14.6.** Соединение с двумя концентраторами

В случае выбора первой конфигурации (двухточечной) правила модели 1 предельно просты: электрический кабель не должен быть длиннее 100 метров, полудуплексный оптоволоконный – более 412 метров, полнодуплексный оптоволоконный – 2000 метров (при этом задержка сигнала в кабеле не имеет значения, так как метод CSMA/CD не работает).

В случае применения второй конфигурации (с одним концентратором) надо ограничивать длину кабелей A и B сети в соответствии с таблицей 14.3.

В случае выбора третьей конфигурации сети (с двумя концентраторами) надо ограничивать длину кабелей A и B в соответствии с таблицей 14.4. При этом по умолчанию предполагается, что кабель C имеет длину 5 метров.

В обеих конфигурациях с концентраторами при использовании одновременно электрического и оптоволоконного кабелей можно за счет уменьшения длины электрического кабеля увеличить длину оптоволоконного. Причем уменьшению длины электрического кабеля на 1 метр соответствует увеличение длины оптоволоконного кабеля на 1,19 метра. Например, уменьшив кабель TX на 10 метров, можно увеличить кабель FX на 11,9 метра, и его предельная длина составит при двух концентраторах 128,1 метра. Немного увеличится и предельный размер сети (в нашем примере на 1,9 метра).

В случае использования двух оптоволоконных кабелей можно уменьшать один из кабелей за счет увеличения другого. При уменьшении

**Таблица 14.3.** Максимальная длина кабелей в конфигурации с одним концентратором

| Вид кабеля А | Вид кабеля В | Класс концентратора | Макс. длина кабеля А, м | Макс. длина кабеля В, м | Макс. размер сети, м |
|---|---|---|---|---|---|
| TX, T4 | TX, T4 | I или II | 100 | 100 | 200 |
| TX | FX | I | 100 | 160,8 | 260,8 |
| T4 | FX | I | 100 | 131 | 231 |
| FX | FX | I | 136 | 136 | 272 |
| TX | FX | II | 100 | 208,8 | 308,8 |
| T4 | FX | II | 100 | 204 | 304 |
| FX | FX | II | 160 | 160 | 320 |

**Таблица 14.4.** Максимальная длина кабелей в конфигурации с двумя концентраторами

| Вид кабеля А | Вид кабеля В | Макс. длина кабеля А, м | Макс. длина кабеля В, м | Макс. размер сети, м |
|---|---|---|---|---|
| TX, T4 | TX, T4 | 100 | 100 | 205 |
| TX | FX | 100 | 116,2 | 221,2 |
| T4 | FX | 100 | 136,3 | 241,3 |
| FX | FX | 114 | 114 | 233 |

одного кабеля на 10 метров можно увеличить другой тоже на 10 метров. Если же используется два электрических кабеля, то увеличивать один из них за счет уменьшения другого нельзя, так как их длина в принципе не может превышать 100 метров из-за затухания сигнала в кабеле.

Концентратор класса II в принципе не может одновременно поддерживать сегменты с разными методами кодирования TX/FX и T4. Поэтому варианты, соответствующие вторым снизу строкам обеих таблиц 14.3 и 14.4 никогда не реализуются на практике, но стандарт все же дает цифры и для них.

Во всех перечисленных случаях под размером сети понимается размер зоны конфликта (области коллизии, collision domain). При этом надо учитывать, что включение в сеть одного коммутатора позволяет увеличить полный размер сети вдвое.

Пример сети максимальной конфигурации в соответствии с первой моделью для витой пары показан на рис. 14.7. Здесь максимальный размер зоны конфликта складывается из сегментов A, B и C, то есть составляет:

100 + 5 + 100 = 205 метров,

что удовлетворяет условию работоспособности сети (табл. 14.4, верхняя строчка).

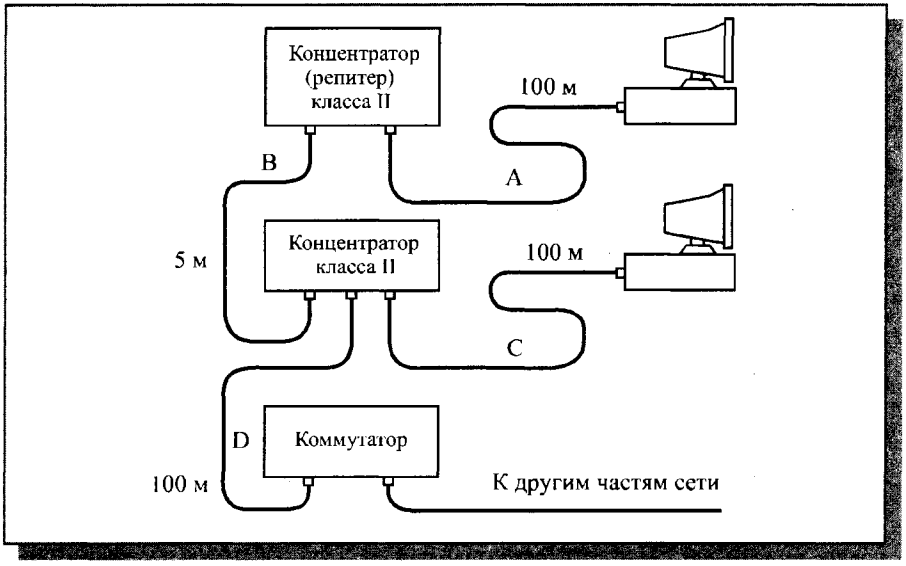



**Рис. 14.7.** Пример максимальной конфигурации сети Fast Ethernet

Сегмент D также входит в зону конфликта, так как коммутатор является полноправным передатчиком пакетов сети. Длина сегмента D не может превышать 100 метров, чтобы суммарная длина сегментов A, B и D не была больше все тех же 205 метров. Сегменты, отделенные от рассматриваемой зоны конфликта коммутатором, никак не влияют на ее работоспособность.

### Расчет по модели 2

Вторая модель для сети Fast Ethernet, как и в случае Ethernet, основана на вычислении суммарного двойного времени прохождения сигнала по сети. В отличие от второй модели, используемой для оценки конфигурации Ethernet, здесь не проводится расчетов величины сокращения межпакетного интервала (межпакетной щели, IPG). Это связано с тем, что даже максимальное количество репитеров и концентраторов, допустимых в Fast Ethernet (два), в принципе не может вызвать недопустимого сокращения межпакетного интервала.

Для расчетов в соответствии со второй моделью сначала надо выделить в сети путь с максимальным двойным временем прохождения и максимальным числом репитеров (концентраторов) между компьютерами, то есть путь максимальной длины. Если таких путей несколько, то расчет должен производиться для каждого из них.

Расчет в данном случае ведется на основании таблицы 14.5.

**Таблица 14.5.** Двойные задержки компонентов сети Fast Ethernet (величины задержек даны в битовых интервалах)

| Тип сегмента | Задержка на метр | Макс. задержка |
|---|---|---|
| Два абонента TX/FX | – | 100 |
| Два абонента T4 | – | 138 |
| Один абонент T4 и один TX/FX | – | 127 |
| Сегмент на кабеле категории 3 | 1,14 | 114 (100 м) |
| Сегмент на кабеле категории 4 | 1,14 | 114 (100 м) |
| Сегмент на кабеле категории 5 | 1,112 | 111,2 (100 м) |
| Экранированная витая пара | 1,112 | 111,2 (100 м) |
| Оптоволоконный кабель | 1,0 | 412 (412 м) |
| Репитер (концентратор) класса I | – | 140 |
| Репитер (концентратор) класса II с портами TX/FX | – | 92 |
| Репитер (концентратор) класса II с портами T4 | – | 67 |

Для вычисления полного двойного (кругового) времени прохождения для сегмента сети необходимо умножить длину сегмента на величину задержки на метр, взятую из второго столбца таблицы. Если сегмент имеет максимальную длину, то можно сразу взять величину максимальной задержки для данного сегмента из третьего столбца таблицы.

Затем задержки сегментов, входящих в путь максимальной длины, надо просуммировать и прибавить к этой сумме величину задержки для приемопередающих узлов двух абонентов (это три верхние строчки таблицы) и величины задержек для всех репитеров (концентраторов), входящих в данный путь (это три нижние строки таблицы).

Суммарная задержка должна быть меньше, чем 512 битовых интервалов. При этом надо помнить, что стандарт IEEE 802.3u рекомендует оставлять запас в пределах 1–4 битовых интервалов для учета кабелей внут-

ри соединительных шкафов и погрешностей измерения. Лучше сравнивать суммарную задержку с величиной 508 битовых интервалов, а не 512 битовых интервалов.

Все задержки, приведенные в таблице, даны для наихудшего случая. Если известны временные характеристики конкретных кабелей, концентраторов и адаптеров, то практически всегда предпочтительнее использовать именно их. В ряде случаев это может дать заметную прибавку к допустимому размеру сети.

Приведем пример расчета по второй модели для сети, показанной на рис. 14.7. Здесь существуют два максимальных пути: между компьютерами (сегменты A, B и C) и между верхним (по рисунку) компьютером и коммутатором (сегменты A, B и D). Оба эти пути включают в себя два 100-метровых сегмента и один 5-метровый. Предположим, что все сегменты представляют собой 100BASE-TX и выполнены на кабеле категории 5. Для двух 100-метровых сегментов (максимальной длины) из таблицы следует взять величину задержки 111,2 битовых интервалов.

Для 5-метрового сегмента при расчете задержки умножается 1,112 (задержка на метр) на длину кабеля (5 метров): $1{,}112 \times 5 = 5{,}56$ битовых интервалов.

Величина задержки для двух абонентов TX из таблицы – 100 битовых интервалов.

Из таблицы величины задержек для двух репитеров класса II – по 92 битовых интервала.

Суммируются все перечисленные задержки:

$$111{,}2 + 111{,}2 + 5{,}56 + 100 + 92 + 92 = 511{,}96.$$

это меньше 512, следовательно, данная сеть будет работоспособна, хотя и на пределе, что не рекомендуется.

Для гарантии лучше несколько уменьшить длину кабелей или взять кабели, имеющие меньшую задержку (см. табл. 2.3). Например, при использовании кабеля AT&T 1061 (NVP = 0,7, $t_з = 0{,}477$) получаются следующие величины задержек для 100-метровых сегментов: $(0{,}477 \times 2) \times 100 = 95{,}4$ битовых интервалов (умножение на два необходимо, чтобы получить двойное время прохождения), а для 5-метрового сегмента – 4,77 битовых интервала. Суммарная задержка при этом составит:

$$95{,}4 + 95{,}4 + 4{,}77 + 100 + 92 + 92 = 483{,}57,$$

то есть гораздо меньше 512 и даже 508, что означает полностью работоспособную сеть.

Пользуясь моделью 2, можно обойти некоторые ограничения модели 1, так как модель 1 строится из расчета на наихудший случай. Например, в сети может присутствовать больше двух концентраторов класса II или больше одного концентратора класса I, а кабель, соединяющий концентраторы, может быть длиннее 5 метров.

На рис. 14.8 показана сеть, содержащая три концентратора класса II, соединенных между собой отрезками кабеля длиной по 10 метров. Компьютеры соединены с концентраторами сегментами 100BASE-TX длиной по 50 метров. Расчет двойного времени прохождения для этого случая:

1. Каждый из трех концентраторов класса II с портами TX даст задержку 92 битовых интервала. Суммарная задержка концентраторов составит 276 битовых интервала.
2. Для двух соединительных кабелей между концентраторами задержка равна $2 \times 1{,}112 \times 10 = 2{,}24$ битовых интервала.
3. Для двух сегментов TX по 50 метров задержка составит $2 \times 1{,}112 \times 50 = 111{,}2$ битовых интервала.
4. Для двух абонентов TX задержка будет равна 100 битовым интервалам.
5. Итого суммарная задержка: $276 + 22{,}24 + 111{,}2 + 100 = 509{,}44$ битовых интервала.

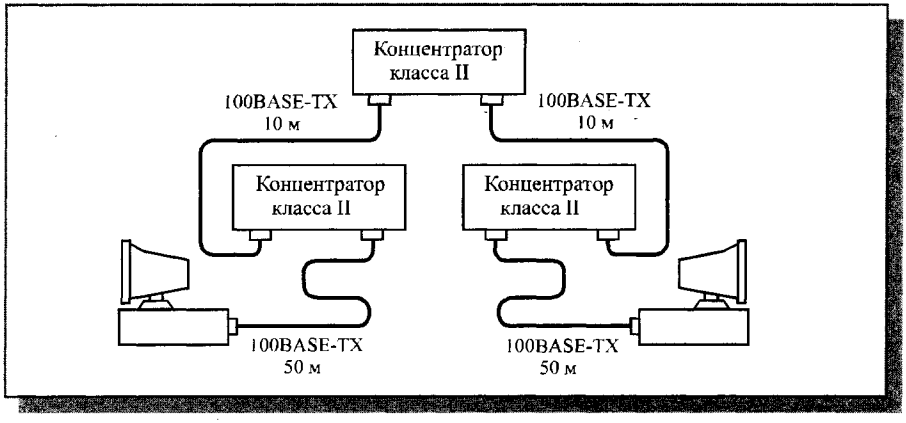



**Рис. 14.8.** Пример работоспособной конфигурации сети, нарушающей правила модели 1

Данная сеть работоспособна. Но при этом надо учитывать, что каждый дополнительный концентратор класса II уменьшает общую допустимую длину кабеля на $92/1{,}112 = 82{,}7$ метра. Сеть с четырьмя концентраторами не будет иметь смысла, так как на задержку в кабеле уже не остается почти никакого запаса (четыре концентратора дадут суммарную задержку в $92 \times 4 = 368$ битовых интервалов).

А теперь стоит посмотреть, какова будет максимальная величина сети Fast Ethernet. Для этого надо взять сеть с одним концентратором класса II и два сегмента 100BASE-FX. Элементарный расчет показывает, что при одинаковых сегментах длина каждого из них может достигать 160 ме-

тров (рис. 10.9), а общая длина сети составит 320 метров. Расчет двойного времени прохождения для этого случая будет выглядеть так:

$$92 + 100 + 2 \times 1{,}0 \times 160 = 512$$

Получается, что сеть работоспособна, хотя и на пределе. В данном случае важна только суммарная длина обоих кабелей. При уменьшении длины какого-нибудь из сегментов можно без потери работоспособности увеличить на точно такую же величину длину другого сегмента.

Если в приведенной на рис. 14.9 конфигурации используется концентратор класса I, а не концентратор класса II, то допустимая суммарная длина сегментов сокращается с 320 метров до 272 метров (расчет для этого случая очевиден). А согласно стандарту запаса лучше уменьшить суммарную длину кабеля на 1–4 метра, что даст снижение круговой задержки на 1–4 битовых интервала.

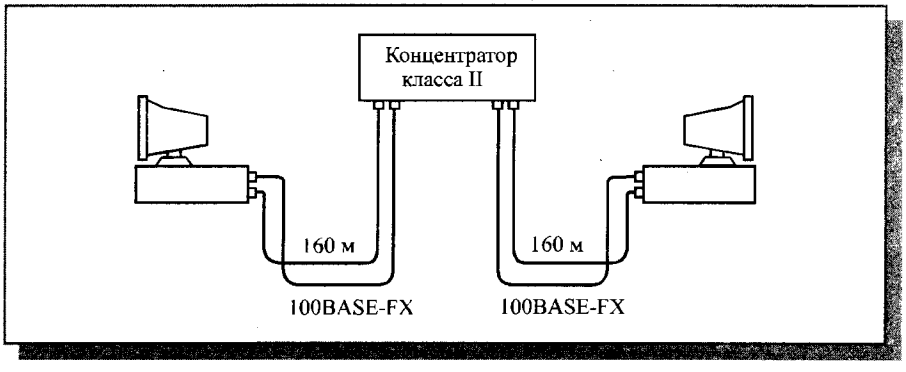



**Рис. 14.9.** Сеть Fast Ethernet максимальной длины

В заключение следует отметить, что модель 2 целесообразно применять в основном при наличии в сети оптоволоконных сегментов. На электрическом кабеле даже при большом желании довольно трудно создать сеть значительного размера.

Методы преодоления ограничений на размер сети в случае Fast Ethernet те же самые, что и в случае Ethernet: сокращение длины кабелей, уменьшение количества концентраторов, выбор марки кабеля с меньшей задержкой, использование коммутаторов, переход на полнодуплексный режим обмена, а также переход на другую сеть (например, FDDI).

# Глава 11. Проектирование локальных сетей

## Лекция 15. Методика и начальные этапы проектирования сети

**В этой лекции рассматривается общая рекомендуемая методика проектирования локальных сетей и содержание работ на начальных этапах, включая формулирование исходных данных, а также выбора вариантов структуры и размера сети, оборудования и сетевых программных средств.**

**Ключевые слова:** структура сети предприятия, одноранговые сети и сети с выделенным сервером, сетевой администратор.

Любое проектирование, как известно, представляет собой сильно упрощенное моделирование еще не наступившей действительности. Именно поэтому предусмотреть все возможные факторы, учесть все потребности, которые могут возникнуть в будущем, практически невозможно. Итак, даже самые подробные руководства по проектированию имеют не слишком большую ценность.

Однако общие подходы к проектированию локальных компьютерных сетей все-таки могут быть сформулированы, некоторые полезные принципы такого проектирования предлагаются и с успехом используются. Не стоит только воспринимать их как нечто пригодное для любых практических случаев и учитывающее все возможные ситуации.

На рис. 15.1 приведена примерная последовательность этапов и варианты выбора при проектировании локальной сети. Вообще, проблема выбора одного из многочисленных вариантов при проектировании ЛС является основной для данного раздела. Выбор затрудняет необходимость учета множества требований, иногда противоречивых (например, обеспечение высоких технических характеристик сети при доступной стоимости), а также настойчивая, порой агрессивная реклама отдельных решений. Последнее часто относится к новейшим вариантам сетевого оборудования и/или программного обеспечения, отнюдь не самым доступным по цене и не всегда имеющим значительные преимущества по техническим характеристикам перед опробованными вариантами.

Цель данного раздела состоит в том, чтобы сформулировать объективные критерии выбора конкретных решений при проектировании ЛС, опираясь на материал предыдущих разделов. Не все этапы проектирования, перечисленные на рис. 15.1, будут далее рассматриваться. Так, орга-


**Рис. 15.1.** Примерная последовательность этапов и варианты выбора при проектировании ЛС

низация силовой электрической сети (п. 5), актуальна в относительно редких случаях. Например, если сеть размещается в новом здании или производится капитальный ремонт, то возникает необходимость организации силовой электрической сети «по всем правилам». Многие из этих правил в отечественных условиях реализуются нечасто (или возможность их реализации ограничена по техническим причинам). Не вдаваясь в излишние подробности, следует упомянуть необходимость организации полноценной системы заземления оборудования (что означает использование не двух-, а трехполюсных розеток, причем один из полюсов должен быть подключен к шине физического заземления) и обеспечение мер электробезопасности. Другой этап, который также не будет далее детализироваться, это этап 6 (установка сетевых карт, активных сетевых устройств, сетевой ОС и других сетевых программных средств). С одной стороны, усилиями разработчиков компьютерного оборудования и программных средств, процедура их инсталляции максимально упрощена (режим plug-and-play, пошаговые инструкции по инсталляции). С другой же, в особо сложных случаях (например, при установке, настройке и последующей поддержке сети на основе выделенного сервера) может потребоваться либо приглашение стороннего специалиста, либо (что предпочтительнее) работа штатного системного администратора. Работы по инсталляции носят разовый характер, а специфический и не малый объем сведений и навыков, которыми должен обладать системный администратор, делают целесообразным изучение соответствующего раздела в рамках отдельного курса (как это и происходит на практике). Тем не менее, некоторые общие принципы системного администрирования рассмотрены в разделе «Выбор сетевых программных средств».

## Исходные данные

Важность этого этапа связана как с необходимостью упорядочивания требований к создаваемой ЛС и ее отдельным составляющим для обеспечения возможности принятия в будущем взвешенных конкретных решений, так и с ее обоснованием.

При создании новой сети для какого-нибудь предприятия желательно учитывать следующие факторы:

- Требуемый размер сети (в настоящее время, в ближайшем будущем и по прогнозу на перспективу).
- Структура, иерархия и основные части сети (по подразделениям предприятия, а также по комнатам, этажам и зданиям предприятия).
- Основные направления и интенсивность информационных потоков в сети (в настоящее время, в ближайшем будущем и в дальней перспективе). Характер передаваемой по сети информации (данные,

оцифрованная речь, изображения), который непосредственно сказывается на требуемой скорости передачи (до нескольких сотен Мбит/с для телевизионных изображений высокой четкости).

- Технические характеристики оборудования (компьютеров, адаптеров, кабелей, репитеров, концентраторов, коммутаторов) и его стоимость.
- Возможности прокладки кабельной системы в помещениях и между ними, а также меры обеспечения целостности кабеля.
- Обслуживание сети и контроль ее безотказности и безопасности.
- Требования к программным средствам по допустимому размеру сети, скорости, гибкости, разграничению прав доступа, стоимости, по возможностям контроля обмена информацией и т.д.
- Необходимость подключения к глобальным или к другим локальным сетям.

Вполне возможно, что после изучения всех факторов выяснится, что можно обойтись без сети, избежав тем самым довольно больших затрат на аппаратуру и программное обеспечение, установку, эксплуатацию, поддержку и ремонт сети, зарплату обслуживающему персоналу и т.д.

Сеть по сравнению с автономными компьютерами порождает множество дополнительных проблем: от простейших механических (компьютеры, подключенные к сети, труднее перемещать с места на место) до сложных информационных (необходимость контролировать совместно используемые ресурсы, предотвращать заражение сети вирусами). К тому же пользователи сети уже не так независимы, как пользователи автономных компьютеров, им надо придерживаться определенных правил, подчиняться установленным требованиям, которые им необходимо разъяснить.

Наконец, сеть остро ставит вопрос о безопасности информации, защиты от несанкционированного доступа — ведь с любого компьютера сети можно считать данные с общих сетевых дисков. Защитить один компьютер или даже несколько одиночных гораздо проще, чем целую сеть. Поэтому приступать к установке сети целесообразно только тогда, когда без сети работа становится невозможной, непроизводительной, когда отсутствие межкомпьютерной связи сдерживает развитие дела.

Требования и варианты решений при выборе размера и структуры сети, сетевого оборудования и программного обеспечения будут рассмотрены в последующих разделах. В начале проектирования сети необходимо провести полную «инвентаризацию» имеющихся компьютеров и их программного обеспечения, а также периферийных устройств (принтеров, сканеров и т.д.). Это позволит при организации сети исключить ненужное дублирование (оборудование и программное обеспечение теперь могут быть разделяемыми ресурсами), а также поставить задачи модернизации (апгрейда) как аппаратных, так и программных средств. Для корректного определения характеристик компьютеров целесообразно ис-

пользовать специальные диагностические программы или встроенные программы ОС (например, в ОС Windows Millennium это программа «Сведения о системе» из раздела служебных программ и программа «Система» из панели управления). Следует выбирать такие варианты программ, которые обеспечивают получение правильных данных («старые» диагностические программы могут неверно указать тип процессора и версию ОС), а также сохранение данных в файле (это особенно ценно при большом числе компьютеров). Кроме того, следует уделить внимание наличию встроенной сетевой карты или сетевого контроллера на системной плате, а также типу поддерживаемых ими сетевых стандартов (как правило, поддерживается сеть Ethernet на витой паре, но при этом необходимо знать ее разновидность – 10/100/1000 Мбит/с). Не все характеристики компьютеров, которые важны при их объединении в сеть, могут быть определены описанными выше способами. Из сопроводительной документации к компьютеру или после вскрытия системного блока можно и нужно определить число и тип свободных слотов (разъемов) расширения, а также максимальную мощность блока питания. Это необходимо для оценки возможности установки в компьютер новых плат.

## Выбор размера и структуры сети

Под размером сети в данном случае понимается как количество объединяемых в сеть компьютеров, так и расстояния между ними. Надо четко представлять себе, сколько компьютеров (минимально и максимально) нуждается в подключении к сети. При этом необходимо оставлять возможность для дальнейшего роста количества компьютеров в сети, хотя бы процентов на 20–50.

Кстати, совсем не обязательно раз и навсегда включать в сеть все компьютеры предприятия. Иногда имеет смысл оставить некоторые из них автономными, например, из соображений безопасности информации на их дисках. Количество подключенных к сети компьютеров сильно влияет как на производительность, так и на сложность ее обслуживания. Оно также определяет стоимость требуемых программных средств, поэтому просчеты могут иметь довольно серьезные последствия.

Требуемая длина линий связи сети также играет немалую роль в проектировании сети. Например, если расстояния очень большие, может понадобиться использование дорогого оборудования. К тому же с увеличением расстояния резко возрастает значимость защиты линий связи от внешних электромагнитных помех. От расстояния зависит и скорость передачи информации по сети (выбор между Ethernet и Fast Ethernet). Целесообразно при выборе расстояний закладывать небольшой запас (хотя бы процентов 10) для учета непредвиденных обстоятельств. Преодолеть ог-

раничения по длине иногда можно путем выбора структуры сети, разбиения ее на отдельные части.

Под структурой сети понимается способ разделения сети на части (сегменты), а также способ соединения этих сегментов между собой. Сеть предприятия может включать в себя рабочие группы компьютеров, сети подразделений, опорные сети, средства связи с другими сетями. Для объединения частей сети могут использоваться репитеры, репитерные концентраторы, коммутаторы, мосты и маршрутизаторы. Причем в ряде случаев стоимость этого объединительного оборудования может даже превысить стоимость компьютеров, сетевых адаптеров и кабеля, поэтому выбор структуры сети исключительно важен.

В идеале структура сети должна соответствовать структуре здания или комплекса зданий предприятия. Рабочие места группы сотрудников, занимающихся одной задачей (например, бухгалтерия, отдел продаж, инженерная группа), должны размещаться в одной или рядом расположенных комнатах. Тогда можно компьютеры этих сотрудников объединить в один сегмент, в единую рабочую группу и установить вблизи их комнат сервер, с которым они будут работать, а также концентратор или коммутатор, связывающий все их машины. Точно так же рабочие места сотрудников подразделения, занимающихся комплексом близких задач, лучше расположить на одном этаже здания, что существенно упростит их объединение в сегмент и дальнейшее его администрирование. На этом же этаже удобно расположить коммутаторы, маршрутизаторы и серверы, с которыми работает данное подразделение.

Как и в других случаях, при выборе структуры разумно оставлять возможности для дальнейшего развития сети. Например, лучше приобретать коммутаторы или маршрутизаторы с количеством портов, несколько большим, чем требуется в настоящий момент (хотя бы на 10–20 процентов). Это позволит при необходимости легко включить в сеть один или несколько сегментов. Ведь любое предприятие всегда стремится к росту (порой совершенно напрасно), и этот рост не должен каждый раз приводить к необходимости проектировать сеть предприятия заново.

Пусть небольшое предприятие занимает три этажа, на каждом по пять комнат, и включает в себя три подразделения, по три группы. В этом случае можно построить сеть следующим образом (рис. 15.2):

- Рабочие группы занимают по 1–3 комнаты, их компьютеры объединены между собой репитерными концентраторами. Концентратор может использоваться один на комнату, один на группу или один на весь этаж. Концентратор целесообразно расположить в помещении, в которое имеет доступ минимальное количество сотрудников.
- Подразделения занимают отдельный этаж. Все три сети рабочих групп каждого подразделения объединяются коммутатором, а для

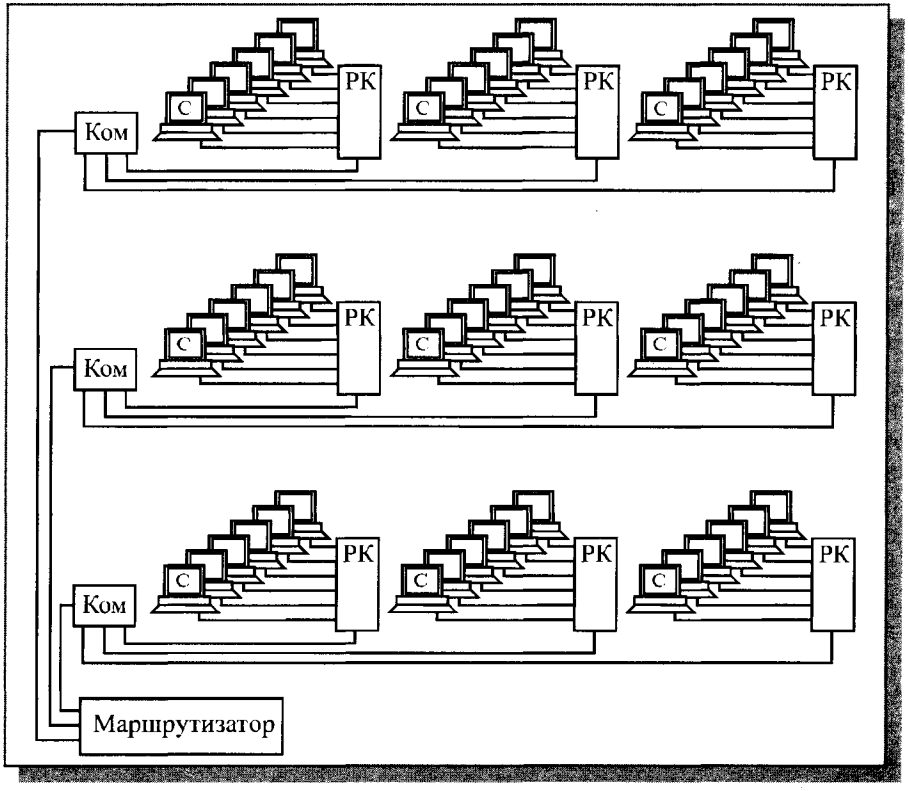



**Рис. 15.2.** Структура сети предприятия
(С – серверы рабочих групп, РК – репитерные концентраторы, Ком – коммутаторы)

связи с сетями других подразделений используется маршрутизатор. Коммутатор вместе с одним из концентраторов лучше поместить в отдельной комнате.

- Общая сеть предприятия включает три сегмента сетей подразделений, объединенных маршрутизатором. Этот же маршрутизатор может использоваться для подключения к глобальной сети.
- Серверы рабочих групп располагаются в комнатах рабочих групп, серверы подразделений – на этажах подразделений.

В рассмотренной ситуации области коллизий (зоны конфликта) сети будут включать в себя сегменты, расположенные в комнатах каждой рабочей группы, плюс сегмент, связывающий концентратор рабочей группы с коммутатором подразделения. Всего таких областей коллизий будет девять. Именно для них необходимо проводить расчеты работоспособности сети в соответствии с предыдущей главой.

Широковещательные области будут включать в себя все сегменты сети каждого подразделения плюс сегмент, связывающий коммутатор подразделения с маршрутизатором предприятия. Таких широковещательных областей будет всего три.

Если предполагаемая интенсивность обмена по проектируемой сети недостаточно велика, компьютеров не слишком много, и размеры здания позволяют, то вполне возможно обойтись без маршрутизаторов — довольно сложных и сравнительно дорогих устройств.

Тогда сети подразделений будут связаны концентраторами, а между собой они будут соединяться коммутаторами (рис. 15.3).

Области коллизий в данном случае будут включать в себя все сегменты сети каждого подразделения плюс сегмент, соединяющий концентратор подразделения и коммутатор предприятия. Таких областей коллизий всего три. Для них надо проводить расчет работоспособности сети, как описано в предыдущей главе. В единственную широковещательную область войдет вся сеть предприятия.

В ситуации, когда компьютеров на предприятии немного (до 50), имеет смысл отказаться не только от маршрутизаторов, но и от коммутаторов, оставив только репитерные концентраторы. Более того, при такой малой сети и низкой интенсивности обмена вполне может оказаться подходящей сеть Ethernet на тонком коаксиальном кабеле (сегменты 10BASE2) без концентраторов или с 1–2 простейшими репитерами. Правда, в последнем случае придется компьютеры каждого сегмента разместить на одном этаже из-за ограничений на длину кабеля сегмента 10BASE2. Следует учитывать, что во вновь создаваемых сетях использование коаксиального кабеля не рекомендуется.

Конечно, идиллическая картина, рассмотренная выше, наблюдается далеко не всегда. В реальности все бывает гораздо сложнее. Например, структура подразделений может вообще не соответствовать структуре комнат и этажей. Предприятие может занимать два разнесенных друг от друга помещения в одном здании или даже 3–4 удаленных здания. Тогда может понадобиться применение оптоволоконных сегментов (в том числе и полнодуплексных, которые обеспечивают максимальную длину кабеля). А структура сети при этом обычно чрезвычайно сложна, с множеством областей коллизий и широковещательных областей.

## Выбор оборудования

При выборе сетевого оборудования надо учитывать множество факторов, в частности:

- уровень стандартизации оборудования и его совместимость с наиболее распространенными программными средствами;

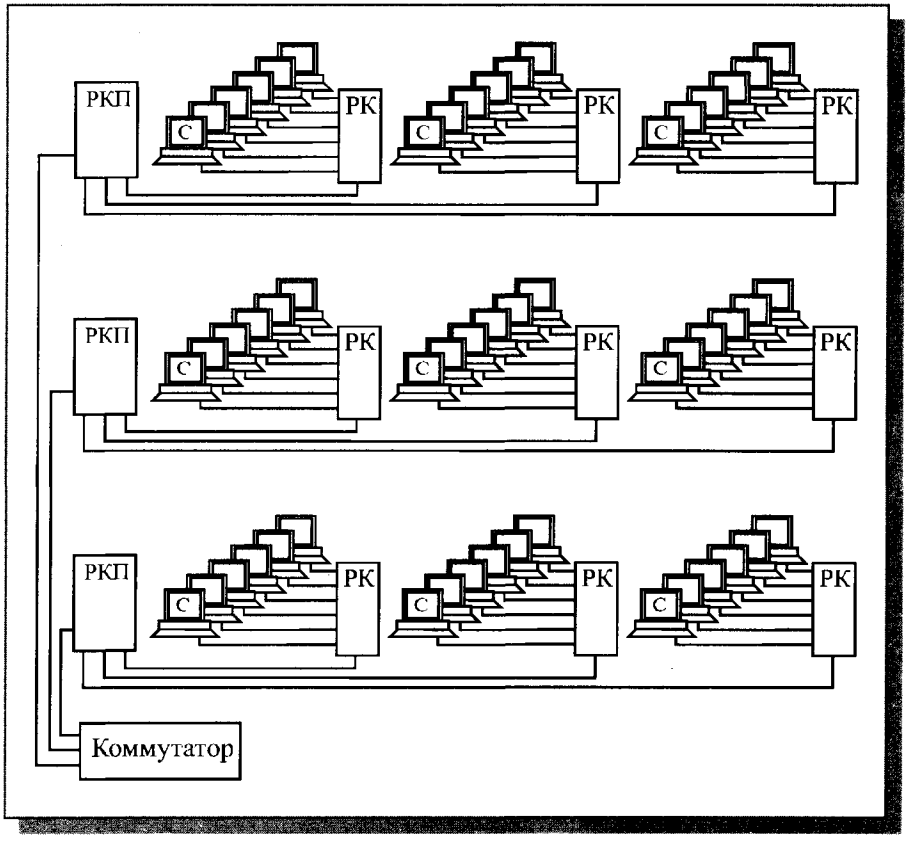



**Рис. 15.3.** Структура сети предприятия
(С – серверы рабочих групп, РК – репитерные концентраторы, РКП – концентраторы подразделений)

- скорость передачи информации и возможность ее дальнейшего увеличения;
- возможные топологии сети и их комбинации (шина, пассивная звезда, пассивное дерево);
- метод управления обменом в сети (CSMA/CD, полный дуплекс или маркерный метод);
- разрешенные типы кабеля сети, его максимальную длину, защищенность от помех;
- стоимость и технические характеристики конкретных аппаратных средств (сетевых адаптеров, трансиверов, репитеров, концентраторов, коммутаторов).

Всем этим часто пренебрегают, а напрасно: заменить программное обеспечение сравнительно просто, а вот замена аппаратуры, особенно прокладка кабеля, обходится порой очень дорого, а иногда бывает просто невозможна. В первую очередь следует проанализировать применимость для рассматриваемого случая сети Ethernet, как наиболее популярной, недорогой и допускающей развитие (Fast Ethernet и Gigabit Ethernet).

Проблема выбора типа кабеля достаточно подробно рассматривалась ранее. В предположении, что возможность выбора в данном случае существует, стоит повторить основные аргументы в пользу того или иного выбора (см. табл. 15.1).

В настоящее время для организации локальных сетей в подавляющем большинстве случаев используется неэкранированная витая пара UTP. Более дорогие варианты на основе экранированной витой пары, оптоволоконного кабеля или беспроводных соединений применяются на предприятиях, где в этом существует действительно острая необходимость. Например, оптоволокно может использоваться для связи между удаленными сегментами сети без потери скорости. Рекомендации по организации кабельной системы, в том числе, содержащиеся в стандартах на структурированные кабельные системы (СКС), рассмотрены в отдельном разделе «Проектирование кабельной системы» лекции 16.

Еще одна важная задача – это выбор компьютеров. Если для рабочих станций или невыделенных серверов обычно используют те компьютеры, которые уже имеются на предприятии, то выделенный сервер желательно приобретать специально для сети. Лучше, если это будет быстродействующий специализированный компьютер-сервер, спроектированный с учетом специфических нужд сети (такие серверы выпускаются всеми крупнейшими производителями компьютеров).

Требования к серверу:

- Максимально быстрый процессор (компания Microsoft рекомендует для своей операционной системы Windows Server 2003 процессор с тактовой частотой не менее 500 МГц). Типичная величина тактовой частоты процессора для сервера сейчас составляет 2–3 ГГц. Для больших сетей применяют и многопроцессорные серверы (иногда до 32 процессоров).
- Большой объем оперативной памяти (фирма Microsoft рекомендует для своей операционной системы Windows Server 2003 объем памяти не менее 256 мегабайт, такие же требования фирмы Novell для NetWare 6). Типичный объем оперативной памяти сервера сейчас составляет 512 Мбайт—20 Гбайт. Большой объем памяти сервера даже важнее быстродействия процессора, так как позволяет эффективно использовать кэширование дисковой информации, храня в памяти

копии тех областей диска, с которыми производится наиболее интенсивный обмен.

- Быстрые жесткие диски большого объема. Типичная величина объема диска сервера сейчас составляет 150–500 Гбайт. Дисководы должны быть совместимы с сетевой операционной системой (то есть их драйверы обязательно должны входить в набор драйверов, поставляемый с ОС). Широко применяют SCSI-дисководы, которые быстрее традиционных IDE-дисководов. В серверах часто предусматривают возможность «горячей» замены дисков (без выключения питания сервера), что очень удобно.
- Специализированные серверы уже содержат в своем составе сетевые адаптеры с оптимальными характеристиками. Если в качестве сервера используется обычный персональный компьютер, то сетевой адаптер для него надо выбирать наиболее быстродействующий.
- Видеомониторы, клавиатуры и мыши не являются обязательными принадлежностями сервера, так как сервер, как правило, никогда не работает в режиме обычного компьютера.

Если есть возможность выбора компьютеров для рабочих станций, то стоит проанализировать целесообразность применения бездисковых рабочих станций (с загрузкой операционной системы через сеть). Это сразу снизит стоимость сети в целом или позволит при тех же затратах купить более качественные компьютеры: с быстрыми процессорами, с хорошими мониторами, с большой оперативной памятью. Правда, в настоящее время использование бездисковых компьютеров считается не самым лучшим решением. Ведь в этом случае всю информацию компьютер получает через сеть и передает в сеть, что может вызвать ее чрезмерную загрузку. Бездисковые рабочие станции допустимы только при малых сетях (не более 10–20 компьютеров). В идеале значительная часть всех информационных потоков (не менее 80%) должна оставаться внутри компьютера, а к сетевым ресурсам обращения должны быть только в случае действительной необходимости. Таким образом, упоминавшееся «правило 80/20» работает и в этом случае.

При отказе от использования гибких дисков на каждом компьютере сети можно существенно повысить ее устойчивость к вирусам и несанкционированному доступу к данным. Дисковод гибкого диска вполне может быть только на одной рабочей станции сегмента или даже всей сети. Причем эта рабочая станция должна контролироваться администратором сети. Она может быть расположена в отдельной комнате вместе с концентраторами, коммутаторами, маршрутизаторами.

Для любой сети крайне критична ситуация перебоев в системе электропитания. Несмотря на то, что многие сетевые программные средства применяют специальные меры против этого, как и против других отказов

**Таблица 15.1.** Аргументы при выборе типа кабеля

| Тип кабеля | Аргументы при выборе | |
|---|---|---|
| | **за** | **против** |
| неэкранированная витая пара UTP (категория 3 или выше) | - доступность по цене;<br>- доступность инструментов для установки разъемов (RJ45);<br>- удобство прокладки кабеля (гибкий);<br>- относительная простота ремонта при повреждении;<br>- поддержка перспективных высокоскоростных сетей (Fast и Gygabit Ethernet) при использовании кабеля категории 5 или выше | - относительно низкая устойчивость к электромагнитным помехам;<br>- сравнительно малые допустимые расстояния кабельных соединений, особенно для высокоскоростных сетей;<br>- невозможность использования во внешних участках соединений (между зданиями) |
| экранированная витая пара STP (оплеточный экран)* | - повышенная устойчивость к электромагнитным помехам | - несколько более высокая цена по сравнению с кабелем типа UTP |
| экранированная витая пара FTP (экран из фольги)* | подобно предыдущему типу кабеля | |
| многомодовый оптоволоконный кабель | - практическая нечувствительность к внешним электромагнитным помехам и отсутствие собственного излучения;<br>- поддержка перспективных высокоскоростных сетей, в том числе на расстояниях, недоступных при использовании витой пары | - относительно высокая цена кабеля и сетевого оборудования;<br>- сложность установки (требуется специальный инструмент и высокая квалификация персонала);<br>- низкая ремонтопригодность;<br>- чувствительность к воздействиям факторов окружающей среды (могут вызвать помутнение оптоволокна) |
| одномодовый оптоволоконный кабель | - улучшенные технические характеристики по сравнению с многомодовым кабелем (возможность увеличения скорости передачи или длины соединений) | - более высокая цена;<br>- сложная установка и ремонт |

| | | |
|---|---|---|
| беспроводные соединения (радио и инфракрасные каналы) | - устранение необходимости организации кабельной системы;<br>- мобильность рабочих станций (простота их перемещения внутри зданий или вблизи от центрального компьютера с излучающей антенной);<br>- возможность организации глобальных сетей (с использованием радиоканалов и спутниковой связи) | - относительно дорогое оборудование;<br>- сильная зависимость надежности соединения от наличия препятствий (для радиоволн) и пыли в помещении (для инфракрасных каналов);<br>- довольно низкая скорость передачи (максимум до нескольких Мбит/с) и невозможность ее существенного увеличения |

* Существует более детальная градация витых пар в зависимости от наличия внешнего и внутренних (окружающих каждую витую пару внутри общей оболочки) экранов: F/UTP, S/UTP, S/FTP, S/STP.

аппаратуры (например, дублирование дисков), это проблема очень серьезная. Иногда отключение питания может полностью и надолго вывести сеть из строя.

В идеале защищенными от отключения питания должны быть все серверы сети (желательно и рабочие станции). Проще всего этого добиться, если сервер в сети всего один. Источник бесперебойного питания при сбое питания переходит на питание подключенного компьютера от аккумулятора и подает специальный сигнал компьютеру, который за короткое время завершает все текущие операции и сохраняет данные на диске. При выборе источника бесперебойного питания надо, прежде всего, обращать внимание на максимальную мощность, которую он обеспечивает, и на время поддержания им номинального уровня напряжения (это время составляет от нескольких минут до нескольких часов). Стоимость устройства довольно высока (до нескольких тысяч долларов). Поэтому целесообразно один источник бесперебойного питания применять для двух-трех серверов.

Наиболее устойчивы к отказам питания портативные компьютеры (ноутбуки). Встроенный аккумулятор и низкое потребление энергии обеспечивают их нормальную работу без внешнего питания в течение одного-двух часов и даже более. Если еще учесть низкий уровень излучений и высокое качество изображения мониторов этих компьютеров, то стоит всерьез рассмотреть возможность использования ноутбуков в качестве рабочих станций, а вероятно, и не слишком мощного, невыделенного сервера. Тем более что многие ноутбуки имеют встроенные сетевые адаптеры довольно неплохого качества. Особенно удобно применение ноутбуков в одноранговых сетях с множеством серверов. Применение внешних

источников бесперебойного питания в подобных случаях становится чересчур дорогим удовольствием.

Кроме перечисленных проблем проектировщику сети приходится решать задачи, связанные с выбором сетевых адаптеров, репитеров, концентраторов, коммутаторов и маршрутизаторов, но об этом уже достаточно сказано в предыдущих главах. Стоит только отметить, что производительность сети и ее надежность определяются самым низкокачественным ее компонентом. При покупке дорогих концентраторов или коммутаторов не стоит экономить, например, на сетевых адаптерах. Верно и обратное. Желательно, чтобы все компоненты оборудования максимально полно соответствовали друг другу.

## Выбор сетевых программных средств

К сожалению, в процессе проектирования сети совершенно невозможно выделить те проблемы, которые должны быть решены в начале, и те, которые можно отложить на самый конец. Выбор программных средств не стоит считать чем-то второстепенным, совершенно не влияющим ни на размер и структуру сети, ни на характеристики требуемого оборудования. Поэтому принимать решение о том, какие программные средства надо использовать или хотя бы к какому классу они должны принадлежать, необходимо в самом начале проектирования.

При выборе сетевого программного обеспечения (ПО) надо, в первую очередь, учитывать следующие факторы:

- Какую сеть поддерживает сетевое ПО: одноранговую, сеть на основе сервера или оба этих типа;
- Максимальное количество пользователей (лучше брать с запасом не менее 20%);
- Количество серверов и возможные их типы;
- Совместимость с разными операционными системами и компьютерами, а также с другими сетевыми средствами;
- Уровень производительности программных средств в различных режимах работы;
- Степень надежности работы, разрешенные режимы доступа и степень защиты данных;
- Какие сетевые службы поддерживаются;
- И, возможно, главное – стоимость программного обеспечения, его эксплуатации и модернизации.

Всегда есть соблазн использовать самый совершенный продукт — ведь он популярен и, следовательно, оптимален. Тем не менее, лучше устоять, так как с ним, возможно, сложнее обращаться, да и цена у него выше. Вполне вероятно, что для задач предприятия может подойти простая

одноранговая сеть, не требующая специального администрирования и покупки дорогого сервера.

Наконец, еще до установки сети необходимо решить вопрос об управлении сетью. Даже в случае одноранговой сети лучше выделить для этого отдельного специалиста (администратора), который будет иметь всю информацию о конфигурации сети и распределении ресурсов и следить за корректным использованием сети всеми пользователями. Если сеть большая, то одним сетевым администратором уже не обойтись — нужна группа, возглавляемая системным администратором. После установки и запуска сети решать эти вопросы, как правило, слишком поздно.

Только после всего выше перечисленного можно переходить к установке выбранного программного обеспечения, если, конечно, таковая требуется. Следует заметить, что в большинстве случаев непосредственно установкой программных средств занимаются работники специализированных компьютерных фирм. Но принимать решение о том, что нужно конкретному предприятию, должны все-таки те, кто будет с этой сетью работать в дальнейшем.

Затем необходимо провести конфигурирование сети, то есть задать ее логическую конфигурацию, настроить на работу в конкретных условиях. В обязанности системного администратора сети, который осуществляет контроль и управление, входит:

- Создание групп пользователей различного назначения;
- Определение прав доступа пользователей;
- Обучение новых пользователей и оперативная помощь в случае необходимости;
- Контроль дискового пространства всех серверов сети;
- Защита и резервное копирование данных, борьба с компьютерными вирусами;
- Модернизация программного обеспечения и сетевой аппаратуры;
- Настройка сети для получения максимальной производительности.

Системный администратор, как правило, получает максимальные права по доступу ко всем сетевым ресурсам и служебным программам. Все остальные пользователи в идеале не должны замечать сети: просто у них появляются новые диски, расположенные на файл-серверах, новые принтеры, сканеры, модемы, программы, специально ориентированные на сеть, например, электронная почта.

Создаваемые группы пользователей должны по возможности совпадать с реальными группами сотрудников предприятия, занимающимися одной или несколькими близкими проблемами. Для каждой группы системный администратор может установить свои права доступа к сетевым ресурсам. Гораздо удобнее создать группу с установленными правами, а затем включить в нее нужных пользователей, чем определять права каж-

дого пользователя в отдельности. В этом случае при необходимости изменения прав пользователя достаточно перевести его в другую группу. Желательно, чтобы каждой группой управлял свой сетевой администратор (если, конечно, группы достаточно большие). Для примера, сетевая ОС Windows Server 2000 позволяет создавать четыре типа групп:

- Локальные группы регистрируются на локальном компьютере;
- Глобальные группы регистрируются на главном контроллере домена;
- Специальные группы (обычно используются для внутрисистемных нужд);
- Встроенные группы делятся на три категории: администраторы, операторы и другие пользователи.

Свои права доступа можно установить и каждому пользователю в отдельности. В идеале пользователь должен иметь столько прав доступа, сколько ему действительно нужно. Если прав меньше, чем нужно, это мешает работе пользователя и требует постоянного вмешательства сетевого администратора. Если же прав больше, чем необходимо, то пользователь может вольно или невольно уничтожить или исказить ценную информацию.

Каждая сетевая операционная система или оболочка имеет свой набор разрешенных прав доступа к каталогам и файлам. Это характеризует ее гибкость, надежность, возможность развития сети.

Время от времени рекомендуется делать копии всех дисков сервера. Это позволит в случае аварии восстановить недавнее состояние сети, потеряв не слишком много данных. При этом системный администратор должен сохранить на диске рабочей станции информацию о пользователях и их правах доступа, чтобы при восстановлении сети не пришлось все это задавать заново. Целесообразно иметь две копии дисков серверов, одна из которых обновляется довольно редко (например, раз в месяц), а другая – чаще (раз в неделю).

Для контроля работы сети системный администратор пользуется специальными программными средствами. Современные сетевые ОС, как правило, имеют программы-утилиты, которые позволяет наблюдать в реальном времени за деятельностью процессоров, работой дисков, использованием памяти, а также сети. Анализируя параметры реального обмена в сети, администратор может установить такие режимы, которые обеспечивают наибольшую эффективность обмена. Выявив тенденции развития сети, он может вовремя принять решение о необходимости модернизации программных или аппаратных средств.

Конечно, всегда надо учитывать, что производительность любой сети зависит не только от установленной аппаратуры и программных продуктов, но и от характера решаемых задач. Одна и та же сеть может прекрасно справляться, например, с задачами доступа к базе данных, но

очень плохо работать с передачей динамических трехмерных полноцветных изображений. Так что при проектировании сети с самого начала желательно знать, какого характера информационные потоки предполагается обслуживать с ее помощью.

В последнее время наблюдается устойчивая тенденция к сокращению количества фирм, производящих сетевые программные средства. Причем даже остающиеся на этом рынке поставщики стараются минимизировать количество своих продуктов. В результате выбор у пользователя не так уж и велик. Выбирать приходится между Novell и Microsoft, причем количество основных, базовых продуктов у обеих компаний невелико (2–3). Все другие фирмы либо вообще прекратили производство новых сетевых продуктов, либо их доля в рынке несравнимо меньше, чем у этих двух гигантов.

Выбирая между продуктами компаний Microsoft и Novell, необходимо иметь в виду, что традиционно преимуществами продуктов Novell (сетевые ОС NetWare) считаются:

- Более совершенная архитектура сетевой ОС;
- Универсальность и функциональная полнота программных средств;
- Большее быстродействие при данном типе аппаратуры;
- Упрощенное администрирование сети;
- Значительно более высокая защищенность от вирусов и несанкционированного доступа;
- Поддержка различных типов пользователей на разных компьютерных платформах.

Главным преимуществом продуктов Microsoft считается лучшая совместимость с пользователями на базе ОС Microsoft Windows.

Цены на новейшие продукты компаний Microsoft и Novell примерно одинаковы. Впрочем, стоимость эксплуатации ОС NetWare оказывается обычно заметно ниже, чем стоимость эксплуатации Windows Server.

Для небольшой сети самым простым и дешевым решением обычно оказывается операционная система Microsoft Windows XP, устанавливаемая сейчас производителями на большинство новых компьютеров и поддерживающая одноранговую сеть.

Впрочем, учесть все факторы в любом случае невозможно — можно только приближаться к оптимальному соответствию возможностей и потребностей.

# Лекция 16. Выбор с учетом стоимости, проектирование кабельной системы, оптимизация и отладка сети

**В этой лекции обосновывается выбор различных аппаратных и программных средств для построения локальных сетей с учетом стоимости, рассматривается методика проектирования кабельной системы, а также методы и средства оптимизации и поиска неисправностей в работающей сети.**

**Ключевые слова:** стартовый набор, стандарты на структурированные кабельные системы (СКС), подсистемы СКС, классы приложений, кабельные сканеры, анализаторы протоколов.

## Выбор с учетом стоимости

Выше при формулировании критериев выбора сетевых аппаратных и программных средств в качестве одного из главных критериев называлась их стоимость. Очевидно, что простой констатации важности учета уровня цен недостаточно. Тем не менее, анализ текущего уровня абсолютных цен на сетевую аппаратуру и программное обеспечение, пусть даже на основе представительного обзора, имеет сам по себе малую ценность и очень быстро устаревает. Уровень абсолютных цен зависит от множества факторов, причем не всегда определяющим среди них является совокупность характеристик аппаратуры или ПО (далее для краткости называемая качеством). На него влияют также такие рыночные факторы, как конъюнктура (текущий спрос), уровень наценки, устанавливаемый дилерами или продавцами, ценовая политика самого производителя, уровень национальной валюты по отношению к евро и динамика его изменения. В этих условиях вместо абсолютных правильнее оперировать относительными ценами в координатах «цена-качество» для однородной (имеющей одинаковое или сходное назначение) продукции. Относительные цены меньше подвержены изменениям, а базовый, принимаемый за единицу отсчета уровень всегда может быть скорректирован на основании анализа свежих данных из сети Интернет или прайс-листов отдельных фирм-продавцов.

Прежде всего следует определить возможные направления финансовых затрат (к данному этапу проектирования необходимые предпосылки для решения этой задачи уже имеются):

- Дополнительные компьютеры и апгрейд существующих компьютеров. Необязательное направление затрат: при достаточном количестве и качестве существующих компьютеров их апгрейд не требуется (или требуется в минимальном объеме – например, для установки

более современных сетевых карт); в одноранговой сети не нужен (хотя и желателен) также специальный файл-сервер.

- Сетевые аппаратные средства (кабели и все, что необходимо для организации кабельной системы, сетевые принтеры, активные сетевые устройства – повторители, концентраторы, маршрутизаторы и т.д.).
- Сетевые программные средства, прежде всего, сетевая ОС на необходимое число рабочих станций (с запасом).
- Оплата работы приглашенных специалистов при организации кабельной системы, установке и настройке сетевой ОС, при проведении периодической профилактики и срочного ремонта. Необязательное направление затрат: для небольших сетей со многими из этих работ может и должен справляться штатный сетевой администратор (возможно, с помощью других сотрудников данного предприятия).

Несколько лет назад, когда вместе с появлением ОС типа Windows 95 появилась также возможность организовывать простые одноранговые сети, довольно популярным за рубежом средством упрощения проектирования (но не экономии денежных средств!) было использование так называемых стартовых наборов (starter kit). Типовой стартовый набор включал 2 сетевые карты, 2 копии сетевой ОС и коаксиальный кабель длиной 25 футов (около 7,6 м) с установленными на нем разъемами для объединения в сеть двух компьютеров. За возможность включения в сеть каждого дополнительного компьютера нужно было платить цену, равную половине цены стартового набора.

Вскоре после перехода на сети на основе витой пары, произошла трансформация подобного набора. Он стал включать концентратор (возможен выбор концентратора на разное число выходов), необходимое число сетевых карт и сетевых кабелей (витых пар) нужной длины (выбор из нескольких вариантов стандартных длин) с предустановленными на них разъемами типа RJ45, а также инструкцию по инсталляции сетевой ОС и организации сетевой печати. Подобные подходы на основе наборов типа «сеть в одной коробке» предназначены, в основном, для неискушенных пользователей. В настоящее время они мало популярны, так как установка новых сетей стала массовым явлением и происходит часто на основе передачи опыта предыдущей установки, да и полностью неискушенных пользователей становится все меньше. Следует помнить, что кроме жесткости любого готового набора сетевых средств, в котором невозможно учесть специфику данной проектируемой сети, его недостатком является и явно завышенная цена – при том же или лучшем качестве оборудования и ОС их предпочтительнее приобретать по отдельности.

На рис. 16.1 показан уровень цен для некоторых аппаратных средств, необходимых для организации локальной сети. Следует отметить, что погонная цена кабеля зависит от его типа и характеристик (кабель для внут-

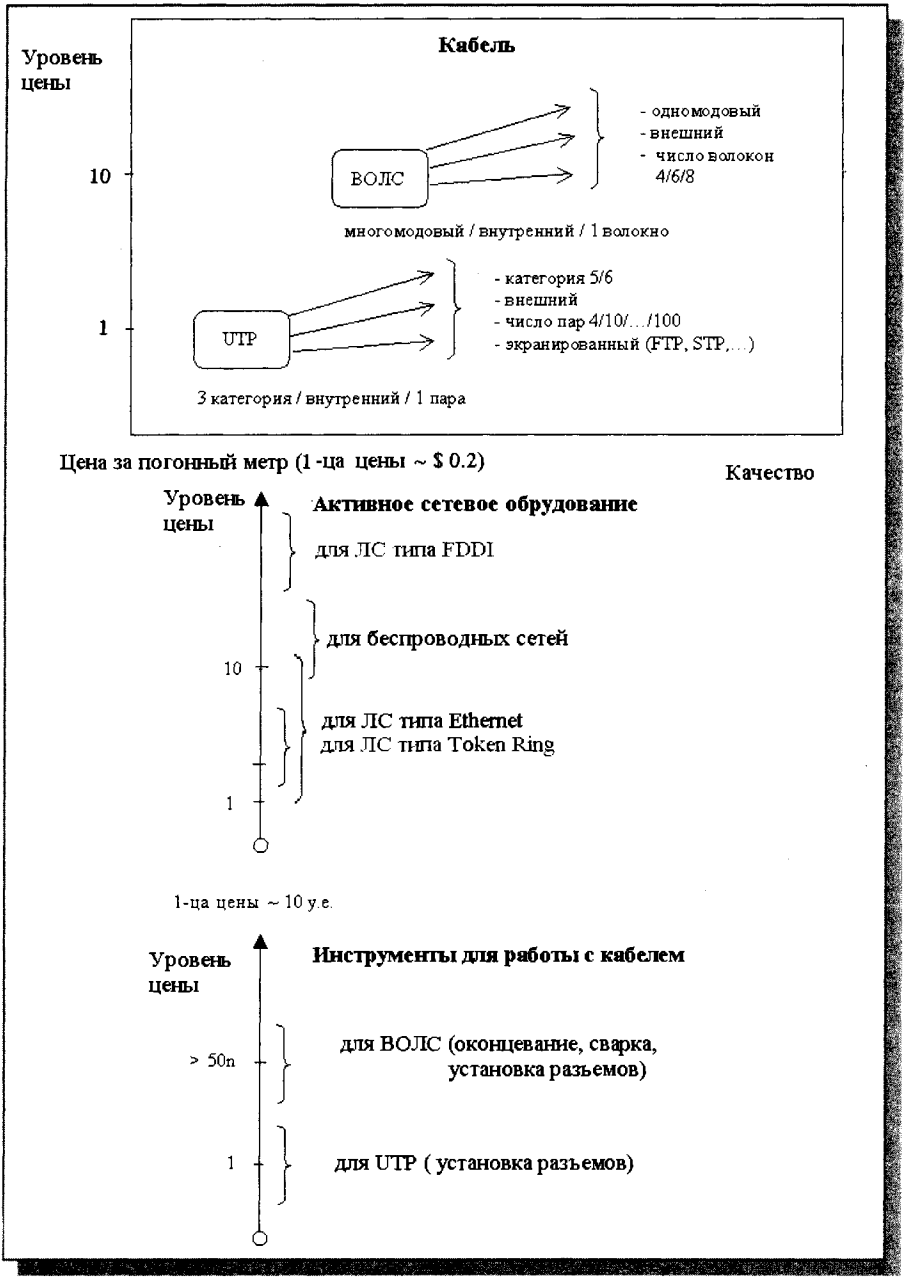



**Рис. 16.1.** Уровень цен некоторых аппаратных средств для организации локальной сети

ренней или внешней проводки, категория витой пары или тип оптического волокна ВОЛС, число витых пар или волокон в одной оболочке, наличие и разновидность экранов в витой паре). Инструменты, используемые для работы с кабелем, значительно дороже, если это оптоволокно. Активное сетевое оборудование, включая сетевые адаптеры, повторители, концентраторы, маршрутизаторы и т.д., для сетей семейства Ethernet при прочих равных условиях (прежде всего, при том же типе кабеля и скорости передачи) доступнее по цене, чем оборудование для сетей другого типа. Это одно из объяснений популярности сетей семейства Ethernet на практике у нас в стране и за рубежом. Фактически сети данного типа легли в основу стандарта структурированных кабельных систем (см. «Проектирование кабельной системы»).

На отечественном рынке сетевого оборудования преобладают средства для построения сетей Ethernet и беспроводных сетей, но последние требуют значительных финансовых затрат.

## Проектирование кабельной системы

Считается, что к данному этапу проектирования тип кабеля уже определен (сравнение различных вариантов приведено в разделах «Выбор оборудования» лекции 15 и «Выбор с учетом стоимости» данной лекции). Более того, предполагается, что тип локальной сети (Ethernet, Fast Ethernet, FDDI или др.) также выбран. В этом разделе рассматриваются рекомендации по организации кабельной системы для сетей на основе проводных соединений (витых пар и оптоволокна). При этом учитывается преобладание в настоящее время на практике сетей данного типа и их заметное отличие от сетей на основе беспроводных соединений с точки зрения особенностей организации кабельной системы. При выборе кабеля в первую очередь надо учитывать требуемую длину, а также защищенность от внешних помех и уровень собственных излучений. При большой длине сети и необходимости обеспечить секретность передаваемых данных или высоком уровне помех в помещении незаменим оптоволоконный кабель. Следует отметить, что применение оптоволоконных вместо электрических кабелей даже при достаточно комфортных условиях позволяет существенно (на 10-50%) поднять производительность сети за счет снижения доли искаженных информационных пакетов.

При проектировании кабельных систем для локальных сетей накоплен большой опыт, на основе которого могут быть сформулированы общие рекомендации по организации таких систем. Более того, существуют стандарты под общим названием «структурированные кабельные системы (СКС)», которые особенно актуальны для вновь создаваемых или реконструируемых относительно больших локальных сетей на уровне предпри-

ятия. Для сравнительно небольших локальных сетей создание сертифицированной СКС, которое предполагает работу приглашенных специалистов, резонно рассматривается как излишняя роскошь. Ниже перечислены **общие рекомендации по созданию кабельных систем**, являющиеся фактически «подмножеством» недетализированных требований стандартов СКС:

1) Составить план размещения компьютеров и других сетевых устройств в помещении (или помещениях). Этот план следует рассматривать как детализацию принятого ранее решения относительно размера и структуры сети (см. раздел «Выбор размера и структуры сети», лекция 15).

   Провести анализ возможности перемещения всех или большей части компьютеров в одно или несколько соседних помещений. Это существенно упростит организацию кабельной системы и исключит необходимость использования излишних активных сетевых устройств. Следует также принять во внимание расширение сети в будущем, для чего предусмотреть наличие точек подключения к сети даже в тех помещениях, где сетевые компьютеры пока отсутствуют. План размещения не должен быть абстрактным, не учитывающим хотя бы в эскизном варианте ограничения, накладываемые конкретным типом выбранной локальной сети. Так, например, нельзя рассчитывать в сети типа 100BASE-T4 или 100BASE-TX (Fast Ethernet на витой паре) на расстояние от абонента (сетевого компьютера или другого сетевого устройства) до концентратора, превышающее 100 м.

2) Оценить соответствие длины кабельной системы и ее отдельных частей (сегментов, соединений между данным абонентом и концентратором и т.д.) требованиям выбранной разновидности локальной сети. Для сетей семейства Ethernet необходимо учитывать ограничения на длины сегментов на разных типах кабелей и задержки сигналов в кабельной системе в соответствии с правилами модели 1 или 2 (см. гл. 10). Для сетей другого типа (Token Ring, FDDI и т.д.) действуют абсолютные ограничения на длины отдельных участков кабельной системы (см. гл. 5). В случае если рассчитанная таким образом длина кабельной системы в целом или на отдельных участках превышает предельно допустимую или близка к ней, следует выбрать одно или несколько из следующих решений (в порядке предпочтения по простоте, стоимости и эффективности реализации):
   - перейти к более качественному типу кабеля во всей сети или только на критичных участках (переход от неэкранированной витой пары к экранированной или оптоволокну);
   - использовать дополнительные репитеры или репитерные концентраторы, позволяющие восстановить амплитуду и форму сигналов, повысив тем самым длину кабельной системы;

- применять модемы для связи данной локальной сети из относительно близко расположенных абонентов с одним или несколькими удаленными абонентами, если снижение скорости передачи на данном участке (или участках) допустимо;
- перейти к другому типу сети, имеющему меньшие ограничения на длину кабельной системы (то есть от сетей на витой паре к сетям на оптоволокне).

Таким образом, выбор конфигурации кабельной системы на данном и предыдущем этапах – итерационный процесс, который может затронуть и более ранние этапы проектирования (вплоть до выбора типов локальной сети и кабеля), если выбор на этих этапах был некорректным.

3) Кабельная система должна быть устойчива к внешним электромагнитным помехам и, по возможности, не генерировать заметные собственные излучения. В противном случае снижается фактическая скорость работы сети (из-за необходимости повторной передачи искаженных помехами пакетов), а также нарушаются требования защиты информации (см. гл. 6).

Большой уровень помех может быть вызван наличием в помещении предприятия мощного электрического оборудования (например, металлообрабатывающих станков, физических установок). Он может быть также связан с близким расположением (до 100-200 метров) высоковольтных линий электропередачи и мощных радиопередатчиков (радиостанций, ретрансляционных антенн сотовой телефонии). Иногда высокий уровень помех вызван всего лишь неправильным размещением кабеля сети. Например, при прокладке кабеля вдоль силовых проводов 220 вольт или вдоль рядов светильников с лампами дневного света количество ошибок передачи резко возрастает (кстати, последнее решение кажется многим очень удобным, так как кабель никому не мешает).

4) Кабельная система должна быть защищена от механических повреждений.

Для прокладки кабелей сети лучше всего использовать специальные подвесные кабельные короба, настенные кабелепроводы или фальшполы. В этом случае кабели надежно защищены от механических воздействий. Самое дорогое решение – это фальшпол, представляющий собой металлические панели, установленные на подставках, и покрывающие весь пол помещения. Зато фальшпол позволяет легко и безопасно проложить огромное количество проводов, что особенно ценно в научных лабораториях, где помимо кабелей локальной сети существует множество других проводов.

Для прокладки кабеля между комнатами или этажами обычно про-

биваются отверстия в стенах или перекрытиях. По сравнению с прокладкой кабеля через двери комнат и стены коридоров это позволяет существенно сократить общую длину кабелей. Однако надо учитывать, что такое решение усложняет любые дальнейшие изменения в кабельной системе (замену кабелей, прокладку дополнительных кабелей, изменение расположения компьютеров сети и т.д.).

Кабели ни в коем случае не должны самостоятельно удерживать свой вес, так как со временем это может вызвать их обрыв. Их следует подвешивать на стальных тросах, причем для эксплуатации на открытом воздух необходимы специально предназначенные для этого кабели с оболочкой, устойчивой к атмосферным воздействиям. По возможности надо использовать для соединения далеко разнесенных зданий подземные коллекторы. Но при этом необходимо предпринимать меры по защите кабелей от воздействия влаги.

Следует также избегать чрезмерно малых радиусов изгиба кабелей (особенно это важно в случае коаксиальных и оптоволоконных кабелей), чтобы не вызвать разрушения изоляции или обрыва центральной жилы. По этой же причине крепежные элементы не должны чересчур пережимать кабель. Известны случаи, когда подобные нарушения вызывали полное прекращение связи через недели или даже месяцы после начала эксплуатации сети.

Часть из перечисленных в данном пункте мер способствует также защите от помех и защите информации (из-за ограничения непосредственного доступа к кабельной системе).

5) Кабельная система должна иметь «прозрачную» и документировано оформленную структуру. Это необходимо как для обеспечения возможности внесения изменений в эту структуру, так и для поиска неисправностей.

Для объединения концов кабелей часто используются специальные распределительные шкафы, доступ к которым должен быть ограничен. Конечно, их применение оправдано только в том случае, если кабелей много (несколько десятков). Располагать распределительные шкафы целесообразно рядом с концентраторами, коммутаторами или маршрутизаторами. Отдельные кабели в жгутах, располагающихся в коробах, под вторым полом и т.д., должны быть одинаковым образом промаркированы с помощью специальных цветных наклеек.

6) Необходимо проверить целостность кабельной системы.

В сети на коаксиальном кабеле для этого можно было использовать непосредственные измерения омметром сопротивления при наличии и отсутствии согласующих нагрузок. В более современных сетях на витой паре и оптоволокне о целостности кабельной системы можно судить по показаниям индикаторов, расположенных на сете-

вых картах вблизи сетевых разъемов. Возможно также использование для этой цели специальных приборов – кабельных сканеров (см. раздел «Оптимизация и поиск неисправностей в работающей сети»).

**Стандарты на «Структурированные кабельные системы (СКС)»** представляют собой объемные документы, детально описывающие и регламентирующие процесс создания кабельных соединений локальных сетей. Изучение стандартов СКС – предмет отдельного курса, касающегося относительно небольшой по численности категории специалистов (в сравнении с числом пользователей локальных сетей). Как и в случае сетевого администрирования, целесообразно рассмотреть лишь общие принципы создания СКС. Конечно, отдельные рекомендации стандартов СКС могут быть с успехом использованы при создании кабельной системы собственными силами (но без возможности официальной сертификации такой системы).

Структурированная кабельная система (СКС) представляет собой иерархическую кабельную систему здания или группы зданий, разделенную на структурные подсистемы. СКС состоит из набора медных и оптических кабелей, кросс-панелей, соединительных шнуров, кабельных разъемов, модульных гнезд, информационных розеток и вспомогательного оборудования. Все перечисленные элементы интегрируются в единую систему и эксплуатируются согласно определенным правилам.

Основные преимущества (или принципы) СКС:

- Универсальность: передача данных в ЛВС, видеоинформации или сигналов от датчиков пожарной безопасности либо охранных систем по единой кабельной системе, организация локальной телефонной сети.
- Гибкость: простота изменения конфигурации кабельной системы и управления перемещениями внутри и между зданиями.
- Устойчивость: тщательно спланированная СКС устойчива к внештатным ситуациям и гарантирует высокую надежность и защиту данных в течение многих лет. Так, большинство ведущих производителей дают гарантию на поставляемые ими СКС (при выполнении требуемых процедур сертификации) до 25 лет.

Основным препятствием широкого внедрения СКС является, как уже отмечалось, их высокая стоимость, что делает приемлемым это решение для относительно масштабных локальных сетей уровня предприятия. Действительно, стандарты на СКС предусматривают проведение, наряду с прочими, комплекса дорогостоящих строительных работ.

Основными стандартами на СКС являются:

- Международный стандарт ISO/IEC 11801 Generic Cabling for Customer Premises.
- Европейский стандарт EN 50173 Information technology – Generic cabling systems.

- Американский стандарт ANSI/TIA/EIA 568-B Commercial Building Telecommunication Cabling Standard.

Стандарты на СКС периодически (примерно раз в пять лет) пересматриваются в связи с развитием аппаратных средств локальных сетей (включая совершенствование медных и оптоволоконных кабелей). В настоящее время (3-й квартал 2004 г.) действуют версии стандартов ISO/IEC 11801 и ANSI/TIA/EIA 568-B, обновленные летом 2002 г.

Согласно стандартам, СКС включает следующие три подсистемы:

- магистральная подсистема комплекса;
- магистральная подсистема здания;
- горизонтальная подсистема.

Распределительные пункты (РП) обеспечивают возможность создания топологии каналов типа «шина», «звезда» или «кольцо» (см. рис. 16.2).

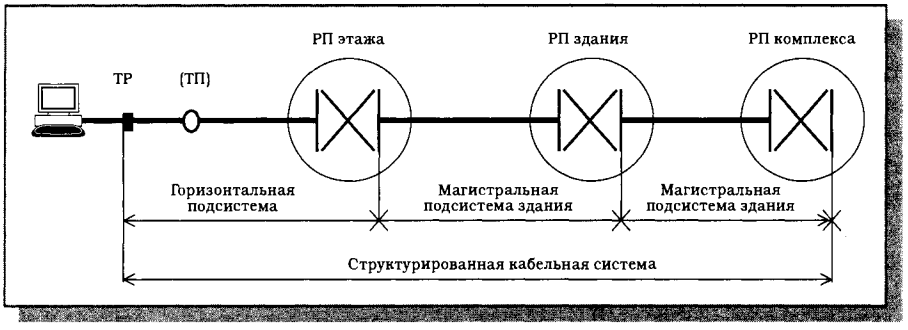



**Рис. 16.2.** Подсистемы СКС

Магистральная подсистема комплекса включает магистральные кабели комплекса, механическое окончание кабелей (разъемы) в РП комплекса и РП здания и коммутационные соединения в РП комплекса. Магистральные кабели комплекса также могут соединять между собой распределительные пункты зданий.

Магистральная подсистема здания включает магистральные кабели здания, механическое окончание кабелей (разъемы) в РП здания и РП этажа, а также коммутационные соединения в РП здания. Магистральные кабели здания не должны иметь точек перехода, электропроводные кабели не следует соединять сплайсами (тип непосредственного соединения кабелей без разъемов).

Горизонтальная подсистема включает горизонтальные кабели, механическое окончание кабелей (разъемы) в РП этажа, коммутационные соединения в РП этажа и телекоммуникационные разъемы. В горизонтальных кабелях не допускается разрывов. При необходимости возможна одна точка перехода. Точка перехода – это место горизонтальной под-

системы, в котором выполняется соединение двух кабелей разных типов (например, круглого кабеля с плоским) или разветвление многопарного кабеля на несколько четырехпарных. Все пары и волокна телекоммуникационного разъема должны быть подключены. Телекоммуникационные разъемы не являются точками администрирования. Не допускается включение активных элементов и адаптеров в состав СКС.

Абонентские кабели для подключения терминального оборудования не являются стационарными и находятся за рамками СКС. Однако стандарты определяют параметры канала, в состав которого входят абонентские и сетевые кабели.

В целом соединения в СКС образуют систему интерфейсов СКС. Интерфейсы СКС – это гнездовые разъемы каждой из подсистем, обеспечивающие постоянное или коммутируемое подключение оборудования и кабелей внешних служб. На рис. 16.3 показаны интерфейсы в виде линий в пределах распределительных пунктов, схематически обозначающих блоки гнезд на панелях.

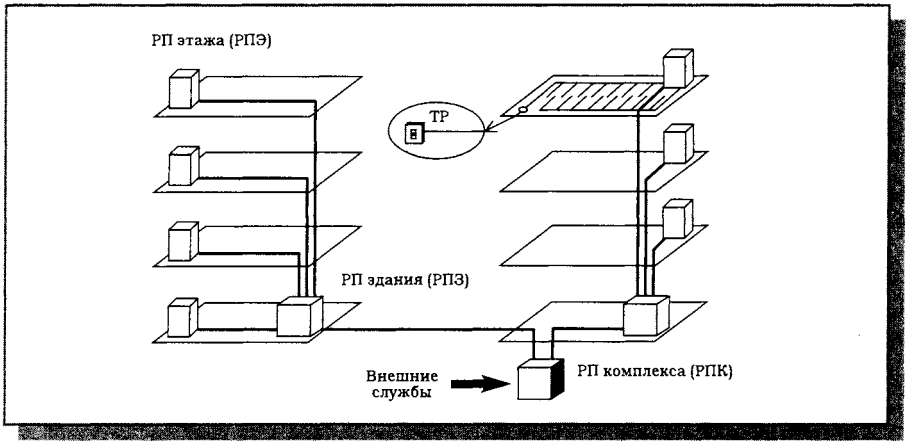



**Рис. 16.3.** Система интерфейсов СКС

Для подключения к СКС достаточно одного сетевого кабеля. В варианте коммутации используют сетевой и коммутационный кабели и дополнительную панель.

Стандарты на СКС по содержанию можно разделить на три группы – стандарты проектирования, монтажа и администрирования. Пожалуй, наиболее полезная в практическом плане группа стандартов монтажа включает рекомендуемые типы и длины отдельных сегментов кабелей в различных подсистемах. В настоящее время во вновь создаваемых кабельных системах рекомендуется использовать только витую пару (симмет-

ричный кабель в соответствии с терминологией стандартов) и оптоволоконный кабель, причем, чем выше уровень подсистемы, тем предпочтительнее использование оптоволокна.

Стандарт определяет пять классов приложений. Этим гарантируется гибкость в выборе различных систем передачи информации. Классы приложений:

- Класс А – речевые и низкочастотные приложения. Рабочие характеристики кабельных линий, поддерживающих приложения Класса А, определены до 100 КГц.
- Класс В – приложения цифровой передачи данных со средней скоростью. Рабочие характеристики кабельных линий, поддерживающих приложения Класса В, определены до 1 МГц.
- Класс С – приложения высокоскоростной цифровой передачи данных. Рабочие характеристики кабельных линий, поддерживающих приложения Класса С, определены до 16 МГц.
- Класс D – приложения сверхвысокой скорости передачи данных. Рабочие характеристики кабельных линий, поддерживающих приложения Класса D, определены до 100 МГц.
- Класс оптики – приложения с высокой и сверхвысокой скоростью цифровой передачи. Рабочие характеристики волоконно-оптических кабельных линий определены для частот 10 МГц и выше. Ширина полосы обычно не является ограничивающим фактором в системах на территории конечных пользователей.

Связь между классами линий и категорией кабелей показана в таблице 16.1.

Наиболее серьезной проблемой при создании СКС для работы высокоскоростных приложений (категория 3 и выше) является качество монтажа. По данным BICSI (Building Industry Consuleting Service International) – международной ассоциации профессионалов телекоммуникационной промышленности, 80% всех структурированных кабельных систем США, построенных на компонентах категории 5, не могут быть квалифицированы как системы категории 5 вследствие нарушения правил монтажа.

Существуют специальные требования и рекомендации по монтажу СКС, выполнение которых гарантирует сохранение исходных рабочих характеристик отдельных компонентов, собранных в линии, каналы и системы. Стандарты ISO/IEC 11801 и ANSI/TIA/EIA-568A устанавливают в качестве требований несколько основных правил монтажа, предусматривающих методы и аккуратность выполнения соединения компонентов и организации кабельных потоков, которые в значительной степени повышают производительность системы и облегчают администрирование установленных кабельных систем.

**Таблица 16.1.** Связь между классами линий и категоризvb кабелей

| Тип трассы | Класс приложений | | | | |
|---|---|---|---|---|---|
| | Класс A | Класс B | Класс C | Класс D | Класс оптики |
| Категория 3 | 2000 м | 200 м | 100 м | – | – |
| Категория 4 | 3000 м | 260 м | 150 м | – | – |
| Категория 5 | 3000 м | 260 м | 160 м | 100 м | – |
| Сбалансированный кабель с волновым сопротивлением 150 Ом | 3000 м | 400 м | 250 м | 150 м | – |
| Многомодовое волокно | – | – | – | – | 2 000 м |
| Одномодовое волокно | – | – | – | – | 3 000 м |

Уменьшению искажения передаваемого сигнала способствуют специальные методы подготовки кабеля и его терминирования (нагружения на согласующее сопротивление) в соответствии с инструкциями производителя, а также хорошая организация кабельных потоков, расположение и монтаж телекоммуникационного оборудования, обслуживающего кабельную систему.

Эти правила особенно касаются высокопроизводительных кабелей — как медных, так и волоконно-оптических. Медные кабели чувствительны к внешним аномалиям. Например, развитие пары медных проводников на величину, превышающую максимально допустимую стандартами, негативно влияет на характеристики перекрестных помех пары или пар. Нарушение требований к минимальному радиусу изгиба кабеля также влияет на его рабочие характеристики.

С увеличением частоты передачи возрастает риск того, что неправильно смонтированный кабель окажет влияние на производительность системы. Если полоса частот меньше 16 МГц, а скорость передачи равна или ниже 10 Мбит/с (например, 10BASE-T Ethernet), то можно и не заметить, что технология монтажа была нарушена. Однако этот же кабель, работающий при ширине полосы сети более 50 МГц и скорости передачи 100 Мбит/с или выше, может функционировать неправильно.

Для оценки передающих рабочих характеристик компонентов СКС используются следующие параметры: затухание, NEXT (NearEndXtalk – переходные помехи на ближнем конце), обратные потери и сопротивление постоянному току. Все они чувствительны к нарушениям непрерывности волновой среды в точках терминирования и в местах возникнове-

ния дефектов, но на NEXT особенно влияет развитие пары проводников и другие воздействия, приводящие к нарушению баланса пары и отклонениям импеданса.

Кроме искажения сигнала, неправильное терминирование может привести к возникновению эффекта рамочной антенны, который проявляется в излучении сигнала с уровнями, превышающими нормативные требования к излучению.

В табл. 16.2 приведено несколько примеров того, как качество монтажа может влиять на самый «тонкий» и «чувствительный» параметр – NEXT.

Общий закон, устанавливаемый стандартами, гласит: смонтированная кабельная система UTP классифицируется в соответствии с наихудшими рабочими характеристиками компонента линии.

**Таблица 16.2.** Влияние качества монтажа на параметр NEXT

| **Тип воздействия** | **Ухудшение NEXT** |
|---|---|
| Полный канал, правильно установленный | Эталон для сравнения |
| Кабель, изогнутый 1000 раз в пределах допустимого радиуса | Без изменений |
| Замена патч-корда длиной 0,6 м категории 5 на патч-корд такой же длины категории | 38,0 дБ |
| Замена патч-корда длиной 0,6 м категории 5 на патч-корд длиной 6 м категории | 313,0 дБ |
| Сворачивание кабеля в бухту с длиной витка 2 м и поперечным сечением 5 см | Без изменений |
| Жгутование кабелей с помощью кабельных хомутов в соответствии с правилами монтажа | Без изменений |
| Удаление 2,5 см оболочки кабеля на станционном конце | 1,2 дБ |
| Удаление 30 см оболочки кабеля на станционном конце | 2,0 дБ |
| Развитие пар кабеля 1,2 см на станционном конце | 1,5 дБ |
| Развитие пар кабеля 5 см на станционном конце | 3,8 дБ |
| Развитие пар кабеля 15 см на станционном конце | 11,6 дБ |
| Скручивание кабеля с радиусом изгиба 3,5 см | 1,9 дБ |
| Скручивание кабеля с радиусом изгиба 1,2 см | 2,1 дБ |
| «Изломленный» кабель | 2,4 дБ |

# Оптимизация и поиск неисправностей в работающей сети

Во вновь организованной локальной сети могут наблюдаться проблемы со стабильностью и скоростью работы, которая оказывается ниже потенциально возможной скорости для сети данного типа. Эти проблемы могут возникнуть также в будущем при подключении нового оборудования, установке нового ПО или при подключении данной сети к другой. Испытывая дискомфорт из-за замедления часто выполняемых операций пересылки файлов или при сетевой печати, конечные пользователи обращаются к сетевому администратору. Возможными причинами возникновения указанных проблем являются:

- недостатки используемого ПО и аппаратного обеспечения;
- неправильная настройка сетевых ОС;
- неисправности в кабельной системе;
- неисправности на уровне сетевых протоколов из-за несовместимости или неисправности сетевых устройств или их неверной настройки;
- неправильная организация локальной сети, например, недостаточное сегментирование в сетях типа Ethernet, приводящее к возникновению дополнительных коллизий пакетов.

Значительная часть этих проблем связана с ошибками, допущенными на предыдущих этапах проектирования сети. Поскольку разрешение данных проблем находится в компетенции сетевого администратора (или специально приглашенного специалиста), то снова не имеет смысла рассматривать в деталях все возможные средства и методы. Конечным пользователям локальных сетей вполне достаточно общего представления о них. Самые общие соображения состоят в том, что для локализации неисправностей целесообразно вносить изменения одно за другим, использовать количественные показатели производительности сети, специальную аппаратуру и ПО. Разумно также придерживаться определенной стратегии поиска, проверяя сначала существование наиболее вероятных и сравнительно легко устраняемых неисправностей (в указанном выше порядке их перечисления).

Недостатки используемого ПО проще устранить его заменой (переходом к более апробированной, может быть, предыдущей версии), чем в случае более дорогостоящего аппаратного обеспечения, которое может образовывать так называемый эффект «бутылочного горлышка» (bottleneck). Это означает, что один из компьютеров в сети (в том числе сервер) или какое-либо сетевое устройство по своим характеристикам уступает другим компьютерам или устройствам и «тормозит» работу сети в целом. В этом случае необходима модернизация (upgrade) или замена устройства.

Актуальность оптимизации параметров сетевых ОС связана с тем, что начальные настройки (настройки по умолчанию) этих параметров

могут не соответствовать конфигурации и интенсивности передаваемых по сети данных (трафику). Если в простых одноранговых сетевых ОС предыдущего поколения (Windows 95/98, некоторые версии NetWare и др.) можно было изменять параметры текстовых файлов конфигурирования, то в более современных сетевых ОС для сетей с выделенным сервером (Windows NT, UNIX и др.) часть функций по оптимизации берет на себя сетевая ОС. Например, в сетевой ОС Windows NT Server предусмотрено автоматическое перераспределение ресурсов (процессора, памяти на жестком диске и в ОЗУ) с помощью специального программного средства измерения производительности (Performance Monitor). Для изменения сетевых параметров в сетевых ОС Windows предусмотрены такие программы как «Сеть» и «Удаленный доступ к сети» в группе программ «Настройка» меню «Пуск», а также, на более низком уровне, изменение параметров конфигурирования в режиме сетевого администратора (хотя это и не приветствуется в связи с возможностью зависания).

Простейшим доступным средством проверки целостности соединений в сети является использование команды ping, которая работает в ОС UNIX, OS/2 и различных версиях Windows. Команда ping проверяет состояние соединения с другим компьютером или компьютерами, посылая эхо-пакеты и анализируя полученные ответы. Для работы этой команды требуется поддержка сети Интернет, то есть протоколов TCP/IP. В рамках локальной сети использование команды ping (с IP–адресом удаленного компьютера в качестве параметра) позволяет, кроме проверки наличия соединения, установить время отклика и выявить узкие места в сети.

Для поиска неисправностей в кабельной системе применяются также стандартные и специальные приборы – от простейших тестеров для определения обрывов и коротких замыканий в медных кабелях до сетевых анализаторов, предназначенных для эталонного тестирования кабелей различных категорий. Промежуточное положение по сложности занимают кабельные сканеры, позволяющие по анализу отраженных от неоднородностей сигналов определять место и тип неисправности, а также портативные устройства для сертификации кабельных систем. Аналогичные приборы разработаны для поиска неисправностей в кабельных системах на основе оптоволокна.

Если предыдущие проверки не позволили выявить неисправности, то приходится предположить существование проблем на уровне сетевых протоколов. Анализ сетевых протоколов требует высокой квалификации от специалиста, который этим занимается, а также применения специфического оборудования – анализаторов протоколов. Анализатор протоколов в общем случае представляет собой аппаратно-программный комплекс, физически подключаемый к сети и перехватывающий данные с целью деко-

дирования и анализа некоторых из них. Возможны различные варианты реализации анализаторов протоколов:

- ПК, возможно, портативный, включающий сетевую карту для соответствующей сети (Ethernet, Token Ring или др.), с установленным специализированным ПО.
- Комплект из сетевой карты и специализированного ПО.
- Специализированное ПО к стандартным сетевым картам.
- Самостоятельные устройства со специализированным ПО.

В зависимости от варианта реализации различаются и возможности соответствующего анализатора протоколов. Общий подход к использованию анализаторов протоколов состоит в измерении некоторых количественных и качественных показателей работы сети, в анализе вероятных ошибок и выработке рекомендаций по изменению параметров конфигурирования и модификации рабочих станций и файл-сервера, а также в настройке приложений. Примерами такого рода рекомендаций является установка новых версий драйверов сетевых адаптеров, исключение несовместимых форматов пакетов и регулировка длины пакетов. В целом анализатор протоколов можно сравнить с удобным диагностическим инструментом, который позволяет не только осуществлять поиск и идентификацию возможных неисправностей, но также может быть использован в профилактических целях – для анализа изменений характеристик сети при установке нового ПО или аппаратуры. Для локальных сетей разных типов (Ethernet, Token Ring и др.) разработаны пошаговые процедуры поиска и устранения неисправностей с использованием анализаторов протоколов.

# Глава 12. Подключение к глобальным сетям с помощью модемов

## Лекция 17. Формулы Шеннона и типы линий передачи, в которых используются модемы

**В этой лекции приводятся формулы Шеннона для дискретного и аналогового каналов, рассматриваются типы линий передачи, в которых применяются модемы, а также характеристики этих линий (прежде всего – скорость передачи данных).**

**Ключевые слова:** модем, теоретический и практический предел скорости передачи, последняя миля, цифровые абонентские линии.

В первоначальном смысле модем (модулятор-демодулятор) – это устройство, преобразующее цифровые данные от компьютера в аналоговые сигналы перед их передачей по последовательной линии и производящее обратное преобразование после передачи. Основная цель преобразования состоит в согласовании полосы частот, занимаемой сигналами, с полосой пропускания линии передачи. Сигналы могут занимать всю полосу пропускания линии передачи либо ее часть (при частотном разделении каналов, например, в случае организации полностью дуплексного обмена). Кроме того, модемы должны обеспечивать необходимую амплитуду и мощность сигналов для достижения большого отношения сигнал/шум и, как следствие обоих перечисленных факторов (полосы частот и отношения сигнал/шум), большей скорости передачи. Подчеркивание основной (но не единственной) выполняемой модемами функции в названии устройств данного типа исторически связано с наиболее распространенным вариантом подключения отдельных компьютеров либо локальных сетей к аналоговой телефонной линии и, через нее — к другим компьютерам и сетям, в том числе к глобальной сети Интернет. Возможно, однако, использование достаточно экзотичных (по крайней мере, в настоящее время) линий передачи (силовая линия электропитания или система кабельного телевидения) и не менее экзотичных модемов для связи компьютеров (и других устройств), подключенных к той же линии. Развиваются цифровые телефонные сети и сети передачи данных, в которых функции модемов изменяются (в частности, модуляция/демодуляция заменяется кодированием), но базовое название, тем не менее, сохраняется.

Еще 5 лет назад трудно было предсказать, что станут практически доступными решения, обеспечивающие бурный рост скорости передачи информации по обычной аналоговой телефонной линии (более чем в 200 раз

для технологии ADSL в сравнении со стандартом V.34). И это в условиях, когда, казалось бы, все резервы увеличения скорости были исчерпаны и достигнут теоретического предела скорости, определяемый теоремами Шеннона! Без сомнения, методы и средства обмена информацией между локальными сетями (или отдельными компьютерами) и глобальными сетями будут совершенствоваться и далее. Обзор доступных и перспективных технологий в этой области, представленный в данной главе, имеет целью не только их сравнительный анализ по характеристикам (прежде всего, по скорости передачи информации и расстоянию), но и пояснение принципов функционирования различных линий передачи, в которых используются модемы, и обеспечивается достижение предельных характеристик.

## Формулы Шеннона для непрерывного и дискретного каналов

Формулы Шеннона представляют собой математические записи теорем кодирования Шеннона для дискретных и непрерывных сообщений, передаваемых по каналам с ограниченной пропускной способностью на фоне шумов и помех. Каналы в зависимости от типов сигналов на входе и выходе принято делить на дискретные, непрерывные и смешанные. В общей структурной схеме канала передачи (см. рис 17.1) дискретными являются каналы от входа модулятора до выхода демодулятора и от входа кодера до выхода декодера. Непрерывный (аналоговый) канал – это собственно последовательная линия передачи (телефонная линия, скрученная пара проводов, коаксиальный кабель и др.). Дискретные каналы не являются независимыми от аналогового канала, который часто образует наиболее «узкое место» при передаче и из-за собственной ограниченной полосы пропускания, внешних шумов и помех определяет общую достижимую скорость передачи (при заданном допустимом уровне ошибок при приеме).

Прежде чем рассматривать формулы Шеннона, целесообразно обратиться к рис. 17.1 и пояснить функции отдельных устройств. Кодер/декодер в конкретной системе может совмещать, на первый взгляд, прямо противоположные функции. Во-первых, кодер может быть использован для внесения избыточности в передаваемую информацию с целью обнаружения влияния шумов и помех на приемном конце (там этим занимается соответствующий декодер). Избыточность проявляется в добавлении к передаваемой полезной информации так называемых проверочных разрядов, формируемых, как правило, аппаратурными средствами из информационной части сообщения. Известно много различных помехоустойчивых кодов, причем самый простой из них — однобитовый (бит четности/нечетности) — далеко не всегда удовлетворительно работает на практике. Вместо него в локальных сетях используются контрольная сумма или циклический код (CRC – Cyclic

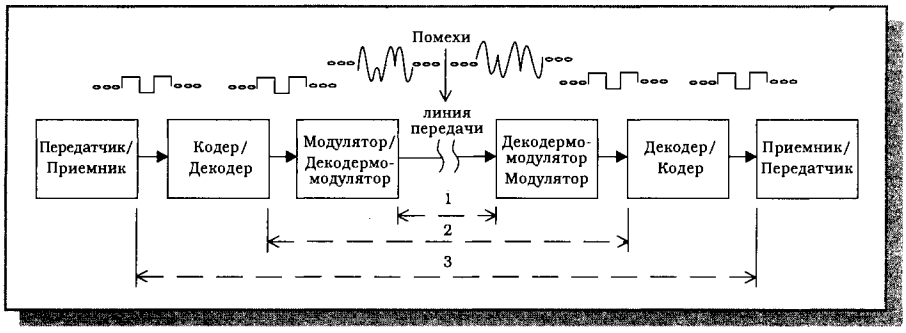



**Рис. 17.1.** Общая структурная схема канала передачи:
1 – непрерывный (аналоговый) канал; 2, 3 – дискретные каналы

Redundancy Check), занимающий в формате передаваемого сообщения 2 или 4 байта, независимо от длины в байтах информационной части сообщения. При больших объемах передаваемой информации целесообразно сжать ее до передачи. В этом случае говорят уже о статистическом кодировании. Здесь уместна аналогия с обычными программами архивации файлов (типа arj, rar, pkzip и др.), которые широко используются при организации обмена в Интернете. Если проблема с большими объемами информации и после такого обратимого сжатия до конца не решается, можно рассмотреть возможность необратимого сжатия информации с частичной ее потерей («огрублением»). Конечно, здесь не идет речь об отбрасывании части цифровых данных, но по отношению к изображениям иногда можно пойти на снижение разрешения (числа пикселей) без искажения общего вида «картинки». Понятно, что оба типа кодирования (помехоустойчивое избыточное кодирование и статистическое кодирование) служат, в конечном счете, решению одной задачи – повышению качества передачи как в смысле отсутствия или минимального допустимого уровня ошибок в принятом сообщении, так и в смысле максимального использования пропускной способности канала передачи. В высокоскоростных модемах нередко реализуются оба типа кодирования. Что касается функций модулятора/демодулятора на рис. 17.1, то они, как уже было сказано, включают согласование полосы частот, занимаемой сигналами, с полосой пропускания линии передачи. Кроме того, выходные каскады передатчиков (после модуляторов) реализуют усиление сигналов по мощности и амплитуде, это одно из средств увеличения отношения сигнал/шум. Действительно, ничто (кроме, пожалуй, техники безопасности) не заставляет разработчиков придерживаться в аналоговом канале столь жестких ограничений сигналов по амплитуде, как в дискретных (цифровых) каналах (от 0 до +5В при использовании аппаратуры в стандарте ТТЛ). Например, для распространенного стандарта последовательного порта компьютера RS-232C предусмотрена «вилка» амплитуд от –(3...12) В до +(3...12) В. Ко-

нечно, это касается амплитуд вблизи передатчика, в то время как вблизи приемника амплитуда сигналов может быть существенно ослаблена.

Формула Шеннона для непрерывного (аналогового) канала достаточна проста:

$$V_{макс}=\Delta f*\log_2(1+S/N) \quad (1)$$

где $V_{макс}$ – максимальная скорость передачи (бит/сек), $\Delta f$ – полоса пропускания линии передачи и одновременно — полоса частот, занимаемая сигналами (если не используется частотное разделение каналов), $S/N$ – отношение сигнал/шум по мощности. График этой зависимости приведен на рис. 17.2 (формуле Шеннона соответствует кривая под названием «теоретический предел»).

Под шумом понимается любой нежелательный сигнал, в том числе внешние помехи или сигнал, вернувшийся к передающему устройству – может быть, и модему – в результате отражения от противоположного конца линии. Сами по себе сосредоточенные помехи не столь существенно ограничивают пропускную способность аналогового канала, как непредсказуемый в каждый момент времени белый гауссовский шум. «Умные» высокоскоростные модемы умеют, как будет отмечено в дальнейшем, определять уровень и задержку «своих» отраженных сигналов и компенсировать их влияние.

Формула Шеннона для многопозиционного дискретного канала, построенного на базе предыдущего непрерывного канала, в отсутствие ошибок при приеме имеет следующий вид:

$$V_{макс}=2*\Delta f*\log_2 n \quad (2)$$

Здесь $n$ – общее число вариантов дискретного (цифрового) сигнала (алфавит). Если за время одной посылки (длительность элементарного аналогового сигнала типа отрезка синусоиды) передается информация о $k$

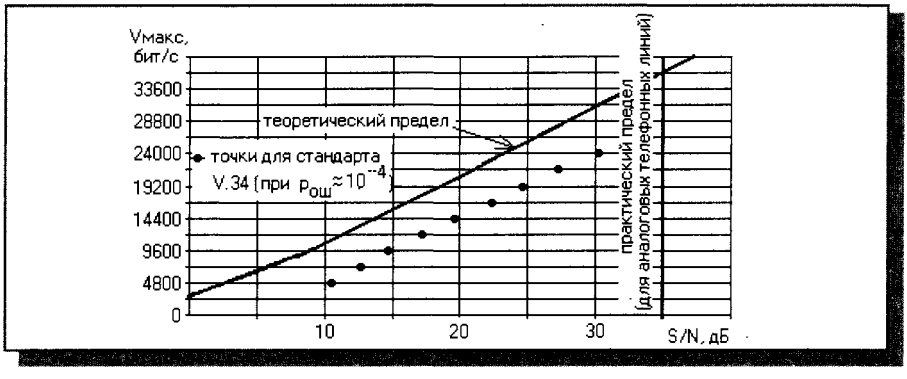



**Рис. 17.2.** Зависимость максимальной скорости передачи Vмакс для аналоговой линии от отношения сигнал-шум по мощности S/N

двоичных разрядах, то $n=2^k$. Практически расширение алфавита для дискретных сигналов приводит к появлению все менее различимых элементарных посылок, так что величина n ограничивается сверху все тем же отношением сигнал/шум S/N в аналоговом канале.

При учете ошибок при приеме формула Шеннона для многопозиционного дискретного канала, построенного на базе непрерывного канала, имеет следующий вид:

$$V_{макс}=2*\Delta f*[\log_2 n + p_{ош}*\log_2(p_{ош}/(n-1)) + (1-p_{ош})*\log_2(1-p_{ош})] \quad (3)$$

Здесь $p_{ош}$ — отношение числа бит, принятых с ошибками, к общему числу переданных бит за время наблюдения, теоретически стремящееся к бесконечности, а практически достаточное для набора статистики. Согласно стандарту ITU-T для телефонных сообщений должно выполняться условие $p_{ош}\leqslant 3*10^{-5}$, а для цифровых данных — $p_{ош}\leqslant 10^{-6}$ (в отдельных случаях для критичных данных этот порог уменьшают до $10^{-9}$). При выполнении требований стандартов влиянием ошибок при приеме на максимально-допустимую скорость передачи можно полностью пренебречь и от соотношения (3) перейти к более простому соотношению (2). В частном случае бинарного канала (k=1, n=2) при $p_{ош}=1/2$ из соотношения (3) следует, что $V_{макс}=0$, а при $p_{ош}\to 0$ и при $p_{ош}\to 1$ $V_{макс}\to 2*\Delta f$. Физический смысл такой зависимости состоит в том, что при $p_{ош}=1/2$ принятый сигнал не содержит полезной информации (каждый из принятых битов может оказаться ошибочным). При $p_{ош}\to 1$ (гипотетический случай, имеющий сугубо теоретический интерес) каждый бит с большой вероятностью инвертируется и доля полезной информации снова возрастает.

Формулы Шеннона показывают, что наиболее эффективный способ повышения максимальной скорости передачи $V_{макс}$ состоит в увеличении полосы пропускания линии передачи $\Delta f$ ($V_{макс}\sim\Delta f$). Логарифмическая зависимость $V_{макс}$ от отношения сигнал/шум S/N делает этот путь повышения $V_{макс}$ гораздо менее перспективным и более трудоемким. Однако на практике редко возможен свободный выбор линии передачи, который с точки зрения реализации максимальной скорости передачи однозначно сводится к использованию оптоволокна (ВОЛС). На практике чаще всего имеется телефонная линия, по которой и нужно организовать передачу с применением модемов. Аналоговая телефонная линия (точнее, тракт передачи, функционирующий на этой линии, с учетом фильтров) имеет фиксированную полосу пропускания $\Delta f = 3400 - 300 = 3100$ Гц, поэтому приходится бороться именно за повышение отношения сигнал/шум. Да и то хороший результат сам по себе не гарантирован, так как речь идет о реализации возможностей, близких к теоретическому пределу. Практический предел отношения сигнал/ шум в аналого-

вой телефонной линии составляет примерно 35 дБ (более 3000 раз по мощности или более 56 раз по амплитуде), что соответствует максимальной скорости $V_{макс} \approx 34822$ бит/сек (стандартное значение, реализуемое на практике, 33600 бит/сек). Популярные в настоящее время 56К–модемы реализуют заявленную скорость только в одну сторону – от провайдера (из сети) до пользователя и только при условии работы провайдера непосредственно на цифровой, несколько более широкополосной, линии передачи (чудес не бывает!)

## Типы линий передачи, в которых используются модемы (варианты решения проблемы «последней мили»)

Прокладывание по всем правилам структурированных кабельных систем (СКС) для вновь создаваемых или реорганизуемых компьютерных сетей – безусловно, полезное, но одновременно и дорогостоящее мероприятие, требующее больших первоначальных затрат на проведение капитальных работ. По этой причине производители аппаратных сетевых средств осваивают уже существующие или создаваемые линии передачи, большинство из которых не предназначены изначально для соединения компьютеров в сети. Для работы на таких линиях обычно требуются специфические модемы. В сравнении с обычными телефонными модемами эти модемы, как правило, более дорогие из-за ограниченного объема их выпуска. В то же время они по-прежнему служат для переноса спектра передаваемых сигналов в полосу рабочих частот линии передачи, выделенную для организации обмена по сети.

По сложившейся терминологии, различные методы и средства передачи информации на участке от провайдера, предоставляющего доступ к услугам глобальной сети, до конечного пользователя, принято называть вариантами решения проблемы «последней мили». Качество соединения на этом участке и его длина существенным образом сказываются на степени приближения реально достижимой скорости обмена для конечного пользователя к номинальной скорости для данной технологии.

Ниже представлен краткий обзор линий передачи, в которых используется модемная связь, и приводятся достигнутые в настоящее время технические характеристики соответствующих модемов (в первую очередь – скорость передачи).

**Однопроводная линия** – самая простая из возможных линий последовательной передачи данных (см. рис. 17.3). Из-за большого территориального удаления передатчика от приемника в сети (до нескольких сотен метров или даже свыше километра) возникает заметная разница потенциалов между точками заземления аппаратуры и возрастает влияние ничем не скомпенсированных помех. Поэтому на практике такие линии передачи в сетях не используются.

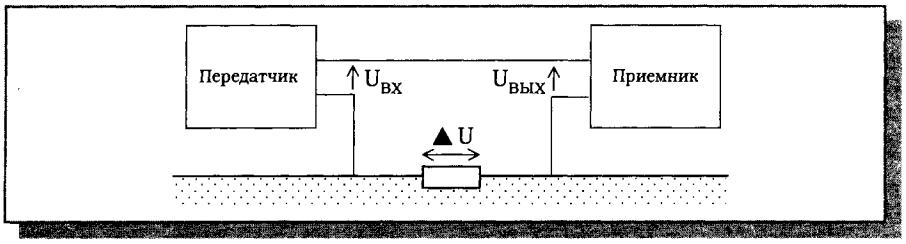



**Рис.17.3.** Однопроводная линия передачи (при симплексном режиме обмена данными)

**Обычную линию силового электропитания на 220 В (электропроводку)** в последнее время успешно используют для организации двунаправленной системы домашней автоматики, связывающей различные бытовые приборы (осветительные приборы, стиральную машину, телевизор и др.) и датчики (температуры, потребляемой мощности и др.). Цель состоит как в управлении этими приборами, так и в сигнализации об опасных ситуациях (пожар, утечка газа и т.д.). «Побочное» использование электропроводки для организации домашней локальной сети напрашивается само собой, однако при этом надо иметь в виду далеко не идеальные характеристики такой линии. Измерения на реальных линиях электропроводки в диапазоне частот 100...150 кГц, наиболее перспективном для передачи данных, показали существенный разброс модуля импеданса линии (1,5...80 Ом), затухания (2...40 дБ) и уровня шума (до –15 дБ). Эти характеристики существенно зависят от количества одновременно включенных бытовых приборов.

Для организации домашней локальной сети, использующей линию электропроводки, необходимы специальные модемы (power line modems). Первоначально скорость передачи информации по линии электропроводки была невысокой – до 10 Кбит/с или несколько больше. В такой сети устройства обмениваются данными примерно с такими же скоростями, как если бы это происходило в сети Интернет, хотя и находятся в соседних помещениях. Это не столь важно при обмене цифровыми данными, однако может создавать проблемы при передаче оцифрованной речи и изображений (особенно динамических). Недавно появился промышленный стандарт передачи данных по бытовой сети со скоростями передачи, характерными для сетей Ethernet (до 14 Мбит/с). Ранее область действия обычной сети домашней автоматики ограничивалась расстоянием до распределительного трансформатора. Новым стандартом предусмотрена возможность подключения локальной сети на основе электропроводки непосредственно к Интернету (минуя телефонную сеть). В некоторых странах Европы (Германия, Австрия) такая возможность, пусть и в ограниченном масштабе, уже реализована на практике.

**Двухпроводная телефонная линия** в пределах отдельных зданий представляет собой простой двухжильный провод (симметричный кабель), но и

это уже прогресс по сравнению с рассмотренной ранее однопроводной линией, так как отсчет принятого сигнала ведется не от потенциала «земли», а от второго провода в линии. В таких линиях просто организуется симплексный и полудуплексный режим обмена данными, в то время как дуплексный обмен возможен только ценою снижения скорости передачи (при частотном или временном разделении «прямого» и «обратного» каналов). Если учесть ограниченную полосу пропускания аналоговой телефонной линии, то выделение в ней «прямого» и «обратного» каналов с равными скоростями обмена в обоих направлениях оказывается неэффективным решением. Правда иногда требуется передавать в одном из направлений служебную информацию (сообщение о состоянии удаленного модема, его режимах работы и др.), для которой скорость передачи некритична. Тогда параллельный канал может быть организован практически без потери скорости по основному каналу.

**Четырехпроводная телефонная линия** преодолевает недостаток обычной двухпроводной линии, так как позволяет организовать дуплексный обмен без потери скорости в обоих направлениях. Однако линии такого типа не столь широко распространены, как двухпроводные (тем более в России).

**Многопарный телефонный кабель** используется в магистральной части телефонной линии (для внешних соединений) и отличается от «внутренних» телефонных линий большей полосой пропускания, которая необходима для уплотнения множества телефонных каналов.

**Линии на основе коаксиального кабеля, применяемые в системах кабельного телевидения (CATV)**, подобны соединениям во многих локальных сетях. В этих линиях используется еще один тип специализированных модемов, «заслуживших» собственное название: cable modems. Обычный телевизионный сигнал и цифровые данные при передаче по кабелю должны быть разнесены по разным частотным диапазонам. Поэтому увеличение скорости не такое заметное, как в локальных сетях, монопольно использующих высокочастотные кабели (100 Мбит/с в сетях типа Fast Ethernet и др.). Компромиссное решение для локальных сетей, основанных на системах кабельного телевидения, состоит в выборе неравных скоростей при передаче запросов от пользователя в сеть (до 10 Мбит/с) и при получении информации в обратном направлении (до 40 Мбит/с). Безусловно, вторая скорость важнее.

Основные области применения модемов данного типа – доступ к Интернет, передача видео- и аудио-трафика, IP-телефония (голос и факсы) по виртуальным частным сетям (VPN).

**Цифровые абонентские линии (Digital Subscriber Loop – xDSL)** постепенно замещают аналоговые телефонные линии. Общие преимущества от перехода к цифровым методам обработки сигналов в данном случае дополняются заметным увеличением максимально доступной скорости передачи и реализацией постоянных (некоммутируемых) соединений. Некоторые из вариантов xDSL требуют использования четырехпроводной линии, другие могут функциониро-

вать на обычных двухпроводных линиях. Это позволяет организовать высокоскоростную передачу данных, не прибегая к замене старых абонентских линий и прокладке новых выделенных каналов. Повышение скорости достигается за счет более полного использования полосы пропускания линии и усложнения алгоритма обработки передаваемой информации, в том числе ее уплотнения. При этом необходима замена оборудования в магистральной части линии и применение xDSL–модемов со стороны пользователя и провайдера.

Различные варианты xDSL – технологий перечислены ниже:

- HDSL – высокоскоростные цифровые абонентские линии;
- ADSL – асимметричные цифровые абонентские линии;
- ISDL – ISDN цифровые абонентские линии;
- SDSL – симметричные высокоскоростные цифровые абонентские линии;
- VDSL – Very HDSL;
- RADSL – цифровые абонентские линии с подстройкой скорости передачи данных;
- UADSL – универсальные асимметричные цифровые абонентские линии.

Наиболее «старые» ISDN цифровые абонентские линии появились за рубежом около 20-ти лет назад. При работе на двух-проводной линии они обеспечивают для пользователя скорость передачи до 128 Кбит/с (поток данных в линии до 160 Кбит/с). В нашей стране наибольшее распространение получили 2 варианта xDSL–технологий:

- ADSL, для которой скорость потока данных в сторону пользователя (абонента) составляет от 8 до 1,5 Мбит/с, а в обратную сторону – от 1,5 Мбит/с до 640 Кбит/с. На практике из-за снижения качества линий на участке «последней мили» и влияния перекрестных помех реальная скорость в сторону пользователя может оказаться ниже 1 Мбит/с.
- SDSL, для которой скорость в обоих направлениях достигает 2 Мбит/с (реально по Москве средняя скорость составляет 1,5 Мбит/с).

**Линии на основе оптоволоконного кабеля** практически снимают скоростные ограничения для всех видов информации (включая динамические изображения высокого разрешения). Это – технология будущего, которая не нашла широкого применения в районах с уже сложившейся инфраструктурой. Причина в том, что необходимо вкладывать дополнительные средства в организацию «последней мили». Зачастую прокладку оптических сетей делает невозможной архитектура построенных несколько лет назад зданий. В таких случаях гораздо дешевле применять старый и проверенный xDSL. При строительстве же новых зданий оптические технологии «последней мили» прочно заняли свою нишу и реально используются в странах Юго-Восточной Азии и континентальной Америки.

**Беспроводные (радио-) линии** привлекательны для тех пользователей, ко-

торые не имеют фиксированного рабочего места (учащиеся институтов и университетов, инженеры на производстве и т.д.). Обычно в локальной сети стационарные проводные участки (сегменты) сочетаются с удаленными пользователями или сегментами, обслуживаемыми с помощью радио-модемов (radio modems). Высокая частота несущей (2000...2500 МГц) выбирается из условия малого влияния на передаваемую информацию погодных условий. Возможны также варианты с использованием других диапазонов, расположенных как ниже, так и выше по оси частот. Полоса используемых частот, которая определяет достижимую скорость передачи, ограничена как из-за влияния помех, так и вследствие общей занятости радио-диапазонов. В результате максимальная скорость передачи по беспроводным линиям составляет примерно 2 Мбит/с. Следует заметить, что беспроводная связь на высоких частотах (свыше ~ 900 МГц) устойчиво работает только в условиях прямой видимости абонентов (отсутствия препятствий для радиоволн) на расстоянии до 50 км.

**Линии передачи с использованием искусственных спутников Земли** в качестве ретрансляторов сигналов в глобальных или региональных компьютерных сетях в целом напоминают наземные варианты беспроводных линий. Для передачи в разных направлениях теперь используются две частоты несущей: 6/4 ГГЦ (другой вариант – 14/12 ГГц). Однако скорость передачи обычно не превышает 50 Мбит/с. Основная проблема в таких линиях связана с заметной временной задержкой сигналов, передаваемых по длинному маршруту. Например, при числе работающих абонентов, равном 100, применяемый алгоритм временного разделения каналов (TDMA) приводит к величине временной задержки 100*2*(37100 км/300000 км/с) ≈ 24 с. Для компенсации этой задержки, создающей дискомфорт при «живом» общении, используются специальные наземные станции-накопители информации SDU (Satellite Delay compensation Unit).

Перечисление линий передачи, в которых применяются модемы, можно продолжить. Стоит упомянуть технологии HPNA (Ethernet на телефонной линии) и Bluetooth (высокоскоростная беспроводная технология). Однако разрешение вопроса о том, какая из упомянутых или еще не заявившаих о себе технологий найдет широкое применение на практике – это проблема прогнозирования, которое не может дать ответ со сто-процентной гарантией по определению. Кроме ограниченной развитости линий (например, отечественные телевизионные кабельные сети), сдерживающими факторами могут быть технические особенности отдельных линий (в частности, ограничение области действия сети на основе силовой проводки пределами тех помещений, которые «питаются» от одного силового трансформатора). Как уже отмечалось, стоимость специфических модемов (типа power line modems, cable modems или radio modems) в настоящее время достаточно высока в сравнении со стоимостью обычных телефонных модемов. Наконец, такие глобальные линии передачи, которые использу-

ют искусственные спутники Земли, не всегда доступны рядовому пользователю, хотя неявно их эксплуатируют многие пользователи Интернет.а

С достаточной уверенностью можно утверждать, что в ближайшие несколько лет в отечественных условиях будут преобладать решения на основе обычной телефонной линии, то есть модемы, удовлетворяющие стандартам V.34, V.90 и V.92. Более производительные подключения по цифровым линиям xDSL сначала станут широко использоваться в корпоративных сетях, а затем, по мере снижения цен – также и рядовыми пользователями. Этот прогноз может скорректировать появление в ближайшем будущем доступных (в том числе по цене) оптоволоконных линий и аппаратуры для передачи по ним данных (как у провайдеров, так и у конечных пользователей), что в настоящее время представляется маловероятным.

Среди наиболее распространенных при модемной связи телефонных линий есть такие их разновидности и такие режимы работы, которые, опять же, не всегда доступны на практике. Ниже в двух колонках представлены желательные типы и режимы работы телефонных линий, а справа – доступные широкому кругу пользователей (применительно к отечественным условиям):

| | |
|---|---|
| Четырехпроводные телефонные линии | Двухпроводные телефонные линии |
| Выделенные (leased) линии | Переключаемые (switched) линии |
| Многоточечные (many points) линии | Двухточечные (point-to-point) линии |
| Линии с тональным набором номера (tone dial) | Линии с импульсным набором номера (pulse dial) |

В современных стандартах для модемов (например, в стандарте V.34) предусматривается возможность работы на двухпроводных переключаемых двухточечных линиях, широко распространенных во всем мире. При работе на выделенных линиях, аренда которых из-за высоких цен считается оправданной только при достаточно высокой и постоянной во времени загрузке (трафике), а также при использовании довольно популярных (но не в России) линий с тональным набором номера существенно снижается уровень помех, и более полно реализуются скоростные возможности модемов. Многоточечные линии обеспечивают дополнительный сервис – возможность одновременного подключения к линии нескольких пользователей для проведения так называемых «селекторных совещаний», в отличии от случающегося иногда многоточечного соединения в обычной линии с прослушиванием посторонних абонентов.

В отношении качества отечественных телефонных линий высказываются обоснованные претензии, связанные с искажениями сигналов из-за множества факторов.

Значительную долю искажений вносят *абонентские линии*:

- затухание (уменьшение мощности) полезного сигнала;
- изменение амплитудно-частотной характеристики по сравнению со стандартными требованиями (изменение мощности сигнала в зависимости от частоты), причем высокочастотные сигналы затухают более сильно;
- импеданс линии при нормативе 600 Ом ±20% в реальных линиях может лежать в диапазоне от 400 до 1800 Ом. Это означает, что в российских условиях преимущество имеют модемы с перестраиваемым выходным сопротивлением;
- постоянное напряжение смещения (то самое, благодаря которому работают микрофоны) может иметь значительные отклонения от номинала.

При междугородней связи наибольшее влияние оказывают *участки переприема*, в которых происходит преобразование сигналов из высокочастотных, передаваемых по магистральным линиям с использованием частотного уплотнения каналов, в сигналы звукового диапазона 300..3400 Гц и наоборот. Общее число таких участков может доходить до 8–12. Вносимые искажения во многом зависят от качества настройки полосовых фильтров на телефонных станциях. Основные искажения:

- фазочастотные искажения (отклонение группового времени прохождения относительно его значения на частоте 1900 Гц);
- дополнительные амплитудно-частотные искажения (затухание на краях полосы пропускания);
- смещение несущей частоты (спектр сигнала равномерно смещается на несколько герц);
- джиттер фазы (дрожание фазы по периодическому или случайному закону);
- скачки фазы (случайный поток скачкообразных изменений начальной фазы сигнала).

Существует еще целый ряд искажений, которые могут возникнуть на всем пути сигнала: шумы, импульсные помехи, замирание сигнала – временное уменьшение его мощности до уровня ниже распознавания модемом, колебания амплитуды и др.

«Ответ» модема на все эти искажения, независимо от их природы и места возникновения, один и тот же – снижение реальной скорости передачи, вплоть до временного прекращения связи в процессе автоматической адаптации модема к характеристикам линии (см. последующие пункты данного раздела). Так, если рассматривать влияние на скорость передачи только отношения сигнал-шум по мощности S/N, то, как следует из графика на рис. 17.2, даже для достижения сравнительно «скромной» скорости на уровне 10 Кбит/с в соответствии со стандартом V.34 требуемое отношение сигнал-шум должно быть больше 15 дБ. Измерения на реальных отечественных телефонных линиях, особенно при междугородней связи, показывают возможность снижения отношения сигнал-шум и до меньших величин.

# Лекция 18. Структура модема, методы модуляции, стандарты и программные средства для модемов

**В данной лекции рассматриваются типовая структурная схема модема для аналоговых телефонных линий, методы модуляции, используемые в высокоскоростных модемах, особенности стандартов V.34, V.90 и V.92, классификация модемов и программные средства для них.**

**Ключевые слова:** кодер, скремблер, эквалайзер, методы модуляции AM, ФМ, ЧМ, QAM, TCM, цифровой модем, телекоммуникационные программы.

## Структура модема

Одна из возможных структурных схем модема показана на рис. 18.1. Она содержит типовые функциональные узлы обработки и преобразования сигналов, из числа которых намеренно исключены некоторые второстепенные узлы, предназначенные для организации синхронизации и обработки служебных сигналов. Далее узлы, осуществляющие прямое и обратное преобразования в передающей и приемной части модема, рассматриваются попарно.

*Кодер/декодер* предназначены для защиты от ошибок и «сжатия» данных. Защита от ошибок предполагает включение в пакеты передаваемых данных избыточного циклического кода (CRC), как и в локальных компьютерных сетях (см. раздел «Использование помехоустойчивых кодов для обнаружения ошибок в сети» лекции 10). При этом в качестве стандартных протоколов, более подробно описывающих форматы дан-

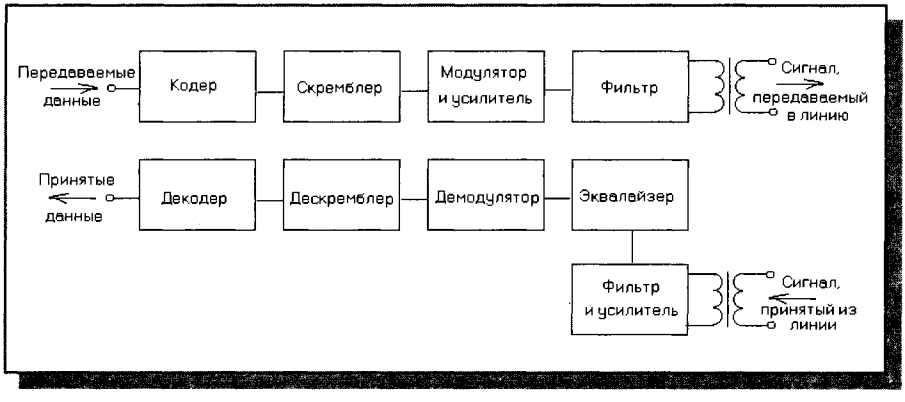



**Рис. 18.1.** Структурная схема модема

ных (в том числе число бит в коде CRC – 16 или 32), используются протоколы серии MNP (Microcom Networking Protocol компании Microcom) или V.42 / V.44 (международный стандарт ITU-T). Протокол V.42bis представляет собой протокол сжатия данных. Если нельзя увеличить пропускную способность линии передачи из-за ограничения, накладываемого теоремой Шеннона, то можно уменьшить избыточность передаваемой текстовой информации, используя свойство повторяемости цепочек символов в словах. Для этого на передающем и приемном конце линии модемы (точнее, их кодеры и декодеры) организуют и поддерживают идентичные динамические словари в виде структур типа дерева с отдельными символами в качестве узлов (см. рис. 18.2). Достаточно передавать не сами слова, а, фактически, специальным образом описанные (в виде чисел) части словарей (пути в дереве), содержащие требуемые последовательности символов. Так, часть словаря на рис. 18.2 позволяет описать строки

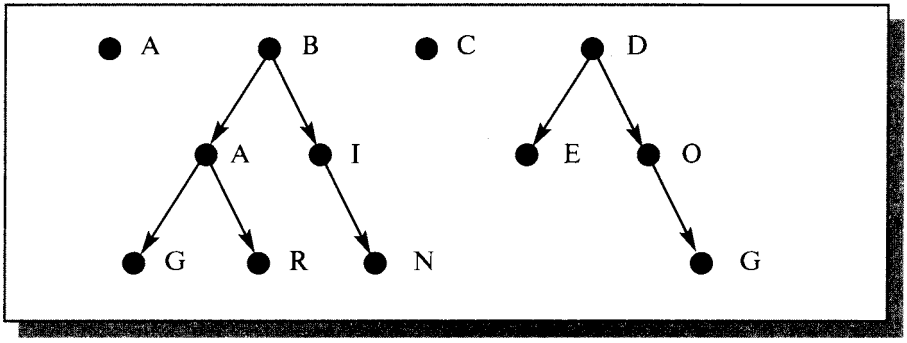



**Рис. 18.2.** Пример представления части словаря при работе протокола сжатия V.42bis

символов A, B, BA, BAG, BAR, BI, BIN, C, D, DE, DO и DOG относительно соответствующих корневых узлов.

*Скремблер/дескремблер* производят такое преобразование передаваемого и принятого сигналов, которое исключает влияние длинных цепочек из логический нулей или единиц, а также коротких повторяющихся последовательностей на надежность синхронизации в приемной части модема. Скремблер при необходимости «разреживает» такие последовательности за счет принудительно вставляемых логических нулей или единиц, делая преобразованные данные псевдослучайными, а дескремблер удаляет лишние биты, восстанавливая исходный вид данных. Описанная проблема (зависимость качества синхронизации от вида передаваемых данных) существенна, конечно, не только при модемной связи, но и при любых видах обменов цифровыми данными по последовательной линии передачи, в которой не предусмотрена посылка отдельного синхросигна-

ла. Такая ситуация характерна для компьютерных сетей, в которых для решения указанной проблемы вместо простых кодов передачи используются самосинхронизирующиеся коды (типа двухуровневых кодов Манчестер-2 или трехуровневых кодов с высокой плотностью единиц – КВП или BNZS в английском варианте названия).

*Эквалайзер* включается в приемной части модема и служит для компенсации зависимости группового времени запаздывания в линии от частоты. Для улучшения качества передачи речевых сигналов их спектральные составляющие на разных частотах должны приходить к удаленному модему с одинаковой задержкой. Идеальная компенсация показана на рис. 18.3. На практике в высокоскоростных модемах собственное групповое время запаздывания эквалайзера подстраивается автоматически.

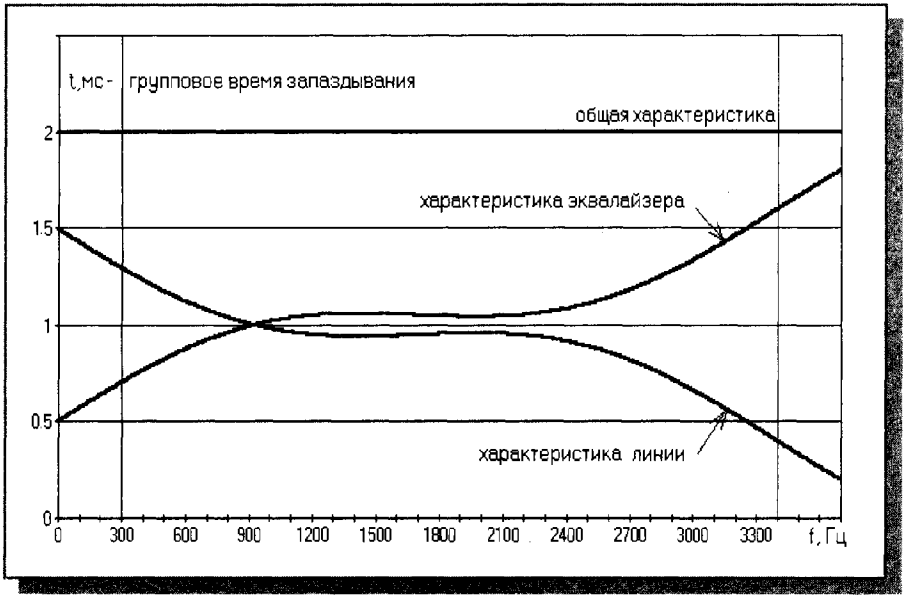



**Рис.18.3.** Идеальная компенсация эквалайзером зависимости группового времени запаздывания в линии от частоты

В приемной части модемов, работающих в дуплексном режиме на обычной двухпроводной телефонной линии, требуется осуществлять также *эхо-компенсацию*. Соответствующий функциональный узел на рис. 18.1 не показан. Проблема состоит в том, что при дуплексном обмене передающий модем может воспринять порожденный им же сигнал, отраженный от другого конца линии, как пришедший от удаленного модема. В стандартах для высокоскоростных модемов (в частности, в стандарте V.34) предусмотрена процедура эхо-компенсации и установлены огра-

ничения на уровень отраженного сигнала (он должен быть меньше полезного сигнала не менее чем на 25–30 дБ) и его максимальную задержку (не более 200–300 мс). Практическая реализация эхо-компенсации в высокоскоростных модемах предусматривает автоматическое определение параметров отраженного сигнала (его амплитуды и задержки) на этапе установления соединения.

*Фильтры и усилители* на рис. 18.1 являются традиционными устройствами при обработке сигналов на фоне шумов и помех и не нуждаются в более подробном описании. В то же время модулятор и демодулятор в модемах реализуют специфические и достаточно сложные методы модуляции, которые рассматриваются в разделе «Методы модуляции, используемые в высокоскоростных модемах».

В современных модемах большая часть функций выполняется программой, управляющей работой цифрового сигнального процессора (ЦСП). Для исключения эффекта наложения спектров принципиально использование непрерывных аналоговых фильтров. Нужны также аналоговые усилители, АЦП и ЦАП для преобразования аналоговых сигналов в цифровые и обратно.

## Методы модуляции, используемые в высокоскоростных модемах

Известно, что «классические» методы модуляции при прочих равных условиях существенно отличаются между собой по степени устойчивости к помехам. В отношении посылок ограниченных во времени отрезков синусоидальных сигналов, несущих информацию о логических нулях и единицах, возможна простая интерпретация преимущества одних методов модуляции перед другими (см. рис. 18.4). На рис. 18.4 $s_1(t)$ и $s_2(t)$ – сигналы, соответствующие логическому нулю и единице (при бинарной передаче, когда каждая элементарная посылка несет информацию только об одном бите). АМ, ЧМ и ФМ – соответственно амплитудная, частотная и фазовая модуляции. Из графиков на рис. 18.4 видно, что в наибольшей степени отличаются между собой посылки сигналов при фазовой модуляции, в наименьшей – при амплитудной модуляции. Поэтому по степени устойчивости к помехам «классические» методы модуляции должны быть расставлены в том же порядке:

АМ→ЧМ→ФМ.

В высокоскоростных модемах для дальнейшего улучшения помехоустойчивости (при неизменном отношении сигнал-шум в линии) используются обычно комбинации из «классических» методов модуляции, в частности, различные варианты амплитудно-фазовой модуляции. Для по-

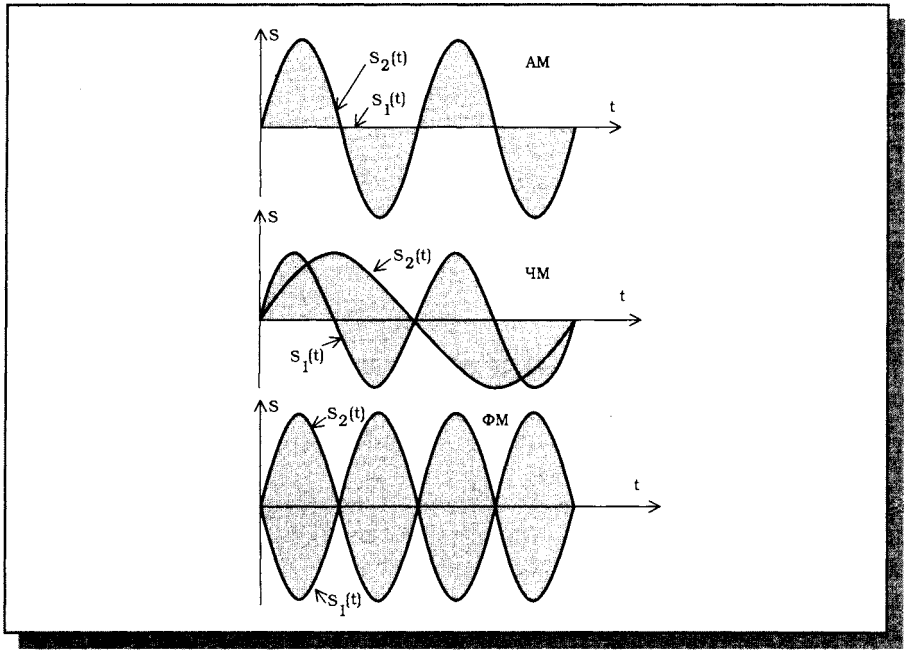



**Рис. 18.4.** Качественное сравнение «классических» методов модуляции по степени устойчивости к помехам

яснения преимущества таких комбинированных методов модуляции над «классическими» методами могут быть применены так называемые констелляционные (от слова constellation – созвездие) или треллис (от слова trellis – решетка) диаграммы. Используется еще и третий вариант названия – квадратурные диаграммы. Этот вариант напрямую связан со способом изображения на комплексной плоскости гармонических функций при их разложении на синусоидальную («мнимую» – Im) и косинусоидальную («вещественную» – Re) составляющие.

На рис. 18.5 показан фрагмент сигнала для простой бинарной дифференциальной фазовой модуляции (DPSK), при использовании которой передаче логической 1 в исходной цифровой последовательности соответствует сдвиг фазы гармонической посылки на 180°, а логическому 0 – отсутствие такого сдвига. В аналитическом виде этот сигнал описывается соотношением $s(t) = \cos(\omega_c t \pm \pi/2)$ и на комплексной плоскости представляется в виде двух точек на окружности. В современных высокоскоростных модемах этот вид модуляции не используется, хотя он ранее применялся в модемах со скоростью передачи до 4800 бит/с. Ограничение скорости передачи связано с неэффективным размещением сигналов в пространстве, при котором минимальное расстояние между

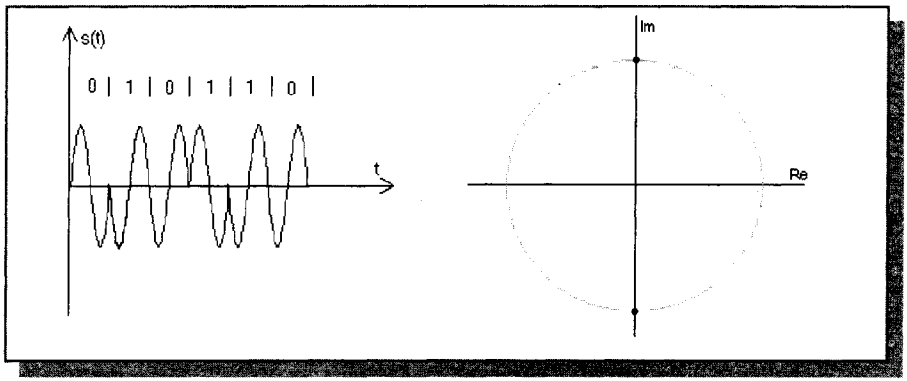



**Рис. 18.5.** Фрагмент сигнала для простой бинарной дифференциальной фазовой модуляции (2 – DPSK) и его отображение на комплексной плоскости

ними (а значит, и степень устойчивости к помехам) далеко от теоретического предела. Для метода DPSK максимальное число бит, информация о которых может быть «закодирована» в одной посылке гармонического сигнала (на одном бодовом интервале), составляет 3, что означает улучшение скорости передачи по сравнению с бинарным кодированием только в 3 раза и общее число гармонических посылок, различающихся по фазе, равное $2^3$=8. При попытке дальнейшего «дробления» фаз метод модуляции DPSK становится неконкурентоспособным с точки зрения помехоустойчивости в сравнении с более совершенными комбинированными амплитудно-фазовыми методами модуляции. Переход от фазовой к амплитудно-фазовой модуляции позволяет увеличить минимальное достижимое расстояние между гармоническими посылками (в смысле расстояния между точками в евклидовом пространстве) при заданном числе этих посылок, как это показано на рис. 18.6. На этом рисунке сравниваются два метода модуляции (16-DPSK и 16-QAM), причем минимальное расстояние между посылками d, очевидно, больше для второго метода модуляции. Здесь QAM (Quadrature Amplitude Modulation) – многопозиционная амплитудно-фазовая модуляция, при использовании которой достижимое число бит на один бодовый интервал может быть увеличено до 8. Существует усовершенствованный метод модуляции – TCM (Trellis Coded Modulation), модуляция с решетчатым кодированием или треллис-модуляция. Преимущество метода TCM перед QAM состоит не столько в увеличении числа бит, передаваемых за время посылки (оно может составлять от 1 до 9), сколько в снижении требования к телефонной линии по величине отношения сигнал-шум на 3–6 дБ. Если ограничиться кратким пояснением без привлечения ря-

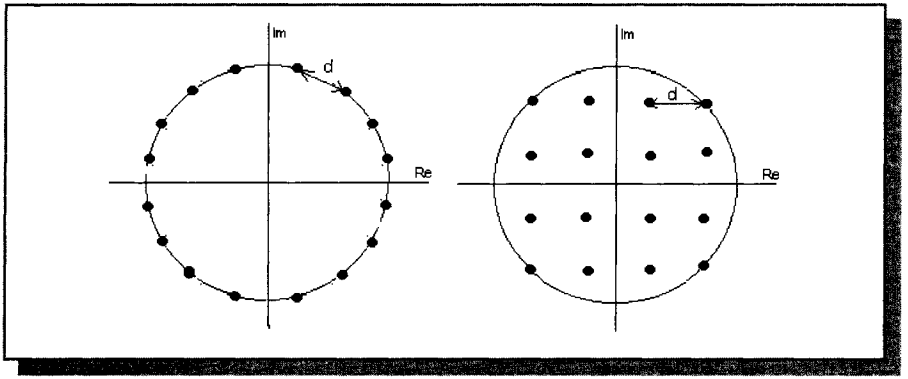



**Рис. 18.6.** Сравнение двух методов модуляции (16-DPSK и 16-QAM) по величине минимального расстояния между посылками d

да дополнительных и необязательных для широкого круга пользователей терминов, то к одним из основных решений, заложенных в метод модуляции TCM, следует отнести введение избыточного бита, полученного с помощью сверточного кодирования. После этого применяется метод модуляции QAM. Несмотря на то, что введение избыточного бита приводит к увеличению общего числа посылок в два раза, использование при декодировании эффективного алгоритма обработки сигналов на фоне шумов и помех (алгоритма Витгерби) позволяет компенсировать эту избыточность и получить отмеченный выше выигрыш в отношении сигнал-шум. Анализ принятого избыточного бита и учет ранее принятых сигналов дает возможность более уверенно выбрать наиболее вероятную точку в пространстве сигналов. Усложнение алгоритмов обработки сигналов и увеличение общего числа посылок ведет к увеличению требуемой производительности (вычислительной мощности) декодера, однако современный уровень развития цифровых сигнальных процессоров позволяет решить эту задачу. Модемы со скоростью передачи до 33600 бит/с, предназначенные для работы на аналоговых телефонных линиях и отвечающие рекомендациям стандарта V.34, используют метод модуляции TCM. На рис. 18.7 в качестве примера представлены проекции сигналов на комплексную плоскость для метода модуляции TCM при числе точек, равном 24, 128, 256 и 960 (соответствующие скорости передачи в стандарте V.34 9600, 19200, 24000 и 28800+200 бит/с). В последнем случае за счет временного уплотнения помимо основного канала вводится независимый дополнительный (параллельный) низкоскоростной канал (со скоростью передачи 200 бит/с), который может использоваться для служебных целей. Общий вид проекций сигналов на комплексную плоскость на рис. 12.10 делает понятными ра-

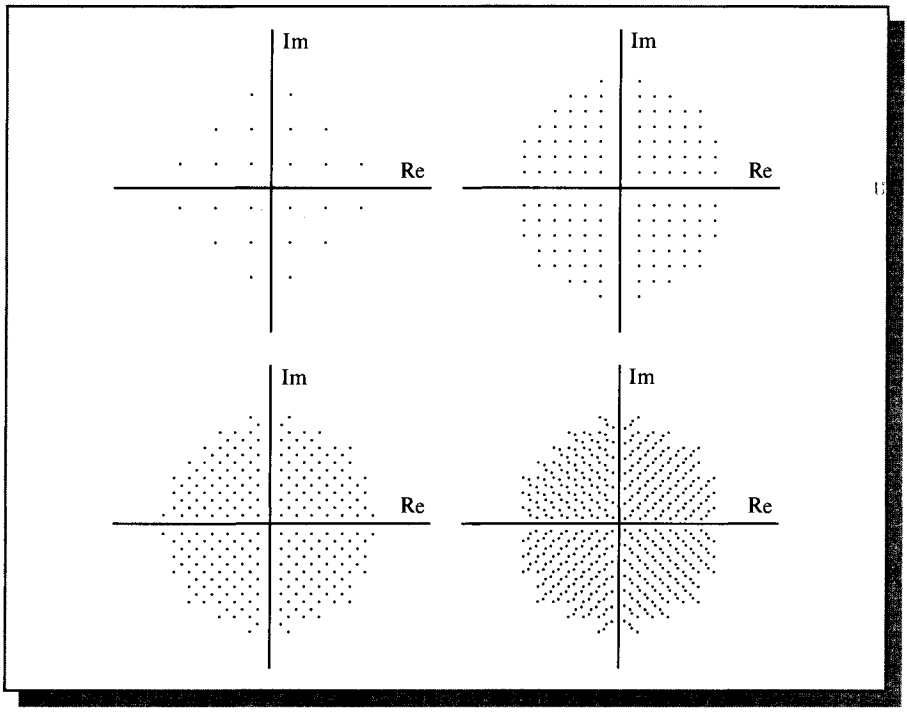



**Рис. 18.7.** Проекции сигналов на комплексную плоскость для метода модуляции TCM при числе точек, равном 24, 128, 256 и 960

нее упоминаемые варианты названий квадратурных диаграмм: констелляционные (constellation – созвездие) или треллис (решетчатые).

Стоит сделать замечание относительно двух возможных способов описания скоростей модемов. Скорость в бодах (baudrate) представляет собой физическую частоту смены посылок. Она обычно ограничена полосой пропускания телефонной линии (от 300 до 3400 Гц, то есть 3100 Гц). Частота несущей выбирается близкой к середине полосы пропускания телефонной линии; для стандарта V.34 предусмотрен ряд возможных частот несущей в диапазоне от 1600 до 2000 Гц («уход» в ту или иную сторону от центра полосы пропускания может несколько улучшить качество связи). Таким образом, бодовый интервал (длительность одной элементарной посылки) может содержать менее одного периода гармонического колебания (в отличие от случая, показанного на рис. 18.4). Информационная скорость передачи может задаваться либо в бит/с (в англоязычной литературе в bps – bit per second), либо в числе символов/с=байт/с (в англоязычной литературе в cps — characters per second). Скорость в бит/с всегда больше или равна скорости в бодах, причем отношение этих скоростей

совпадает с числом бит, приходящихся на один бодовый интервал в том или ином методе модуляции. Произведение 3100 (стандартная полоса пропускания телефонной линии в Гц) × 9 (максимальное число бит, приходящихся на один бодовый интервал в методе модуляции QAM) все еще меньше 33600 бит/с. Это означает необходимость использования более широкой полосы пропускания (и большей частоты смены посылок), что и является одной из особенностей стандарта V.34 (см. следующий раздел). Скорость в символах/с или байт/с (cps) нельзя получить просто делением на 8 скорости в бит/с, так как она учитывает «непроизводительные» потери (служебные поля в пакетах и интервалы между ними). Путем непосредственных измерений установлено, что при таком пересчете дополнительно должен использоваться множитель, немного превышающий 0,9 и зависящий от длины пакета (чем больше длина пакета, тем меньше «непроизводительные» потери).

## Особенности стандартов V.34, V.90 и V.92

Стандарт V.34 имеет длинное название, в переводе имеющее следующий вид: «Модем, обеспечивающий передачу данных со скоростями до 28800 (33600) бит/с для использования на коммутируемой сети общего пользования и на двухточечных двухпроводных выделенных каналах телефонного типа». Таким образом, этот стандарт ориентирован на применение в наиболее распространенных типах телефонных линий. Стандарт V.34 имеет две «версии» или редакции – в первой редакции стандарта (от 1994 г. предусматривалась скорость передачи не выше 28800 бит/с, во второй от 1998 г.) этот предел был увеличен до 33600 бит/с. Кроме перечисленных ранее, этот стандарт имеет ряд других принципиальных особенностей:

- более полное использование полосы пропускания телефонной линии. Из шести предусмотренных стандартом V.34 символьных скоростей передачи две наибольшие (3200 и 3429 символов/с) требуют ширины полосы пропускания линии, превышающей стандартное значение 3100 Гц, но достижимой для ряда реальных телефонных линий;
- введение в передаваемый сигнал наряду с линейными также и нелинейных предыскажений для частичной компенсации нелинейных искажений, вносимых аппаратурой с импульсно-кодовой модуляцией (ИКМ), работающей на линии. На комплексной плоскости такие предыскажения выглядят в виде неравномерного (отличающегося от строго решетчатого) расположения сигнальных точек;
- развитый сервис, включающий возможность организации асимметричной передачи (разные скорости, несущие частоты, число точек на комплексной плоскости и другие режимы работы для модемов на

противоположных концах линии), полудуплексного обмена (эхокомпенсация не используется) и дополнительного канала;

- автоматический адаптивный выбор режимов работы модемов в соответствии с параметрами реальной телефонной линии. Для этого модемы попеременно передают друг другу последовательность из 21 гармонических колебаний с частотами в диапазоне от 150 до 3750 Гц, определяют возможные режимы работы и обмениваются информацией о них. Настройка скорости работы модемов в соответствии с качеством связи (отношением сигнал-шум) означает, что фактически скорость может уменьшаться с шагом 2400 бит/с и в случае отношения сигнал-шум менее 20 дБ (реальная цифра для некоторых отечественных телефонных линий, особенно при междугородней связи) окажется не более 9600 бит/с. Связь ряда достижимых значений скоростей передачи с отношением сигнал-шум для стандарта V.34 показана на рис. 17.2.

Как следует из анализа особенностей стандарта V.34, он практически полностью использует возможности, предоставляемые стандартными аналоговыми телефонными линиями. Дальнейший рост скорости передачи по линии возможен только при использовании линий с большей полосой пропускания, что и предусмотрено в стандарте V.90 для модемов со скоростью передачи до 56 Кбит/с, часто обозначаемых как V.90- или 56K–модемы. Стандарт V.90 на 56K–модемы утвержден ITU-T в сентябре 1998 года. На рис. 18.8 приведена иллюстрация принципа работы обычных (со скоростью передачи до 33600 бит/с на основе стандарта V.34) и 56K(V.90)–модемов в телефонной сети общего пользования. Несмотря на то, что большая часть сети — цифровая, при работе на обоих концах линии модемы, соответствующие протоколу V.34, применяют ее как полностью аналоговую. Это означает необходимость использования аналого-цифровых преобразователей (АЦП) при передаче сигналов в обоих направлениях. В результате дискретизации сигналов по амплитуде АЦП вносят заметный вклад в ухудшение отношения сигнал-шум и скорость передачи в обоих направлениях становится одинаковой (при самых благоприятных условиях — до 33600 бит/с). Однако если на одном из концов линии (у провайдера) использовать специальный цифровой V.90-модем, подключенный непосредственно к цифровой части телефонной сети, а на другом конце (у клиента) аналоговый V.90-модем, то в направлении от провайдера к пользователю АЦП отсутствует и скорость (теоретически) может быть увеличена до 56 Кбит/с. Сама по себе цифровая телефонная сеть имеет скорость передачи 64 Кбит/с, однако наличие дополнительных искажений и шумов от работы ЦАП и АТС, хотя и меньших по уровню, чем шум дискретизации АЦП, ограничивает достижимую скорость передачи. Кроме того, тестирование 56K-модемов показывает возможность достижения ско-

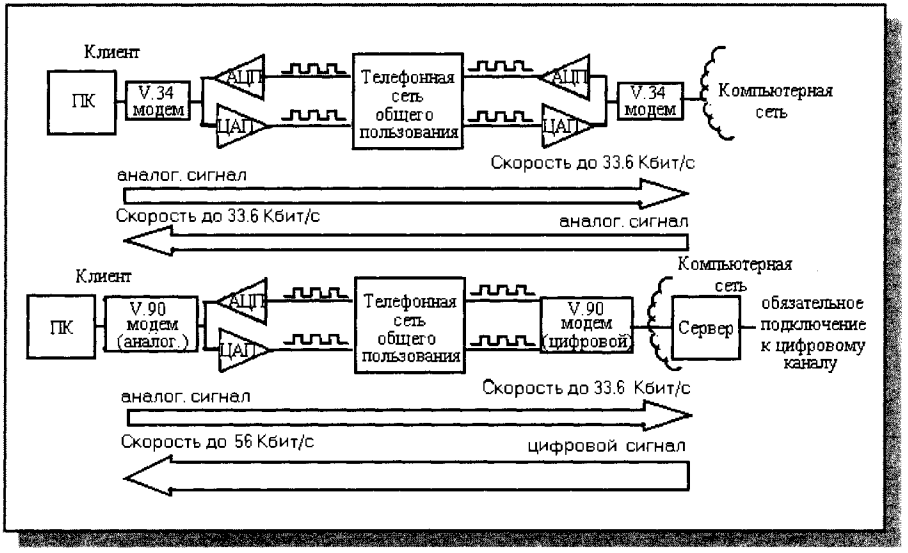



**Рис. 18.8.** Иллюстрация принципа работы обычных и 56K(V.90)–модемов

рости в диапазоне 40–50 Кбит/с при связи с местной телефонной станцией и 28–33 Кбит/с при работе на международных линиях.

Таким образом, достижение скорости передачи 33,6 Кбит/с и тем более 56 Кбит/с требует выполнения целого ряда условий. В первую очередь сама по себе телефонная линия со всем оборудованием, которое используется для преобразования сигналов и коммутации каналов, должна быть достаточно качественной, с наименьшим количеством вносимых искажений сигналов.

Для работы со скоростью 56 Кбит/с необходимо выполнение дополнительных трех условий:

1. Цифровое подключение на одном из концов (со стороны провайдера).
2. Поддержка стандарта V.90 на обоих концах. Стандарт V.90 должен поддерживаться на обоих концах соединения — как аналоговым модемом пользователя, так и сервером удаленного доступа или модемным пулом на стороне хост-компьютера. Переход к стандарту V.90 не означает обязательного приобретения нового модема, так как некоторые из них допускают сугубо программный «upgrade».
3. Одно аналого-цифровое преобразование. На пути следования сигнала между цифровым модемом V.90 и аналоговым модемом может быть только одно аналого-цифровое преобразование.

В июне 2000 г. обнародована серия новых протоколов V.92, V.44 и V.59. Протокол V.92 является развитием протокола V.90 по части выравнивания

скоростей передачи в обоих направлениях обмена. Максимальная исходящая скорость от пользователя увеличена с 33,6 (V.90) до 48 Кбит/с. Это достигается за счет изменения способа кодирования информации (ИКМ). Исходящая от пользователя информация может передаваться со скоростями от 24 до 48 Кбит/с с шагом 1,333 Кбит/с как и в протоколе V.90. Кроме того, уменьшается время вхождения в связь с 20 (V.90) до 10 с (более быстрое соединение – Quick Connect). Второй протокол V.44 позволяет увеличить степень сжатия передаваемых данных как 6:1, то есть на 25% в сравнении с V.42bis, который обеспечивал сжатие 4:1. Производительность (*информационная* скорость передачи) может увеличиться до 300 Кбит/с. И, наконец, третий протокол V.59 вводит такую услугу как возможность прерывания передачи данных на время от 0 до 16 минут и ответ входящему вызову. Для реализации сервисов, предоставляемых стандартом V.92, необходимо выполнение таких же условий, как и для стандарта V.90.

## Классификация модемов

Выше уже упоминались разные типы модемов, однако этот список необходимо дополнить. В табл. 12.1 представлен вариант классификации модемов по следующим трем признакам:

- типы линий передачи, в которых используются модемы;
- виды сервиса и характеристики модемов;
- особенности внутреннего устройства и конструктивного исполнения модемов.

Следует отметить, что модемы относятся к категории массовых и быстро развивающихся телекоммуникационных средств. Их разработкой, изготовлением и продвижением до конечного пользователя занимается множество фирм. С этим связано существование множества неустоявшихся, частично пересекающихся названий модемов. Поэтому краткое название модема может оказаться недостаточным для определения его истинного назначения и особенностей, весьма существенных для пользователя. Так, имеется два абсолютно несовпадающих типа V.90-модемов – один, аналоговый, для применения у пользователя и другой, цифровой, для поддержки стандарта V.90 со стороны провайдера. Путаница также может возникнуть с понятием голосового модема (voice modem) в связи с наличием в некоторых модемах близкой по названию, но совершенно отдельной функции голосовой почты — voice mail, (см. табл. 18.1).

## Программные средства для модемов

Программные средства для модемов (другое наименование *телекоммуникационные программы*), можно разделить на три уровня:

**Таблица 18.1.** Классификация модемов

| Основное название группы модемов | Другие названия или области использования | Основные особенности модемов данной группы |
|---|---|---|
| 1. По типам линий передачи, в которых используются модемы | | |
| – | телефонные | автоматическая адаптация к характеристикам реальных телефонных линий |
| power line или PLC (power line carrier) | для работы в линии силового электропитания (электропроводке) | передача данных со скоростью телефонных от 10 Кбит/с до 14 Мбит/с (для наиболее широкополосных модемов) |
| cable | для работы в сети кабельного телевидения | неравные скорости при передаче запросов от пользователя в сеть и при получении информации в обратном направлении (до ≅ 40 Мбит/с) |
| radio | радио | передача данных со скоростью до 2 Мбит/с по беспроводным (радио-) линиям в условиях прямой видимости абонентов на расстоянии до ≅ 50 км |
| 2. По видам сервиса и характеристикам | | |
| fax | факс | сочетание функций модема и факсимильного аппарата |
| voice mail | голосовая почта | сочетание функций модема и автоответчика с дополнительной возможностью автоматического обзвона ряда номеров для передачи заданного сообщения |
| voice | голосовые | передача наряду с данными голоса (возможно, одновременно с данными), в том числе для звукового сопровождения документов |
| V.34 | – | передача данных по аналоговым телефонным линиям со скоростью до 33,6 Кбит/с |
| V.90 /92 (56K) | аналоговые V.90/92-модемы | передача данных по телефонным линиям со скоростью до 56 Кбит/с (по направлению к пользователю), возможная только при выполнении ряда условий, в том числе при цифровом подключении со стороны провайдера и поддержке стандарта V.90/92 на обоих концах линии |

| 3. По особенностям внутреннего устройства и конструктивному исполнению | | |
|---|---|---|
| Win (US Robotics) | RPI, WinRPI, софт, программные | выполнение части функций модема программными средствами, что несколько снижает стоимость модема, но приводит к значительной нагрузке на процессор компьютера |
| цифровые V.90/92-модемы | – | поддержка стандарта V.90/92 со стороны провайдера |
| internal /external | внутренние /внешние | наличие собственного корпуса и источника питания, возможность простого подключения/отключения (для внешних модемов); реализация в виде платы расширения, несколько меньшая стоимость (для внутренних модемов) |
| xDSL-модемы | – | поддержка передачи данных по цифровым xDSL-линиям |

- низкоуровневые средства по типу языка Ассемблера для компьютеров. Широко распространен набор так называемых Hayes-команд компании Hayes Microcomputer Products. Hayes-команды начинаются с префикса AT, за которым следуют буквенно-цифровые обозначения. Существует командный режим, в котором устанавливаются, изменяются или восстанавливаются параметры модема по умолчанию, а также режим передачи (рабочий). Вряд ли нужно здесь приводить полный список и описание Hayes-команд. Если есть проблемы с использованием конкретного модема, можно попытаться найти столь же конкретный ответ в одной из конференций в Интернете. Если же таких проблем нет, то можно положиться на строки инициализации AT..., «зашитые» в телекоммуникационных программах более высокого уровня;
- средства, встроенные в ОС, в том числе в MS DOS, Norton Commander и Windows. В MS DOS (различных версий) это команда MODE (настройка параметров), а также команды INTERLINK и INTERSRV (собственно передача). В Norton Commander версии 5.0 можно найти программу Term95 или строчку Terminal Emulation в верхнем меню, вызывающую ту же программу. Теперь настройка параметров и передача вызываются в одной программе и просто входят в разные пункты меню. В русскоязычном Windows 95 (OSR2) в группу программ «Стандартные» входит «Программа связи» (Hyper Terminal). Кроме того, в Windows входит отдельная программа настройки модемов («Модемы» в «Панели управления»), а также средст-

ва подключения к Интернету. Упомянутые программы удобнее и «мощнее», чем низкоуровневые команды, однако еще большими возможностями обладают программные средства из следующей группы;

- «внешние» специализированные программы, такие как Lucent Winmodem tune 2.5, VentaFax & Voice 5.5, ChatterBox v1.6 и другие, которые могут поставляться вместе с конкретным модемом (но обычно способны поддерживать работу модемов разных типов) и доступны как свободно распространяемое ПО из Интернета либо на CD.

Ниже перечислены основные установочные параметры телекоммуникационных программ:

- скорость передачи в бодах (baudrate). Стоит отметить, что уже в ранних версиях программы Term предусматривалась скорость, много большая, чем это возможно при модемной передаче (до 115 200 бод для программы Term90, версия 2.3). Дело в том, что связь между компьютерами на небольшие расстояния (до 2 и до 15 м при использовании интерфейсов Centronix и RS232C соответственно) может быть организована без участия модемов с помощью так называемых «нуль-модемных» кабелей, соединяющих параллельные или последовательные порты. В случае применения параллельных портов верхняя граница достижимой скорости передачи доходит до 100 Кбайт/с (то есть до 800 Кбод);
- протоколы передачи (ASCII, Kermit, Xmodem, Ymodem, Zmodem и их разновидности). Здесь под протоколами понимается одна из составляющих этого понятия – формат пакетов. Возможные форматы отличаются по числу бит на символ (для протокола ASCII предусмотрено только 7 бит на символ и, соответственно, возможна передача только текстов, написанных английскими буквами), по длине пакета в байтах и по способу проверки отсутствия ошибок (без проверки, с использованием бита четности/нечетности, контрольной суммы или циклического кода – CRC);
- управление передачей (flow control). Это вторая часть общепринятого понятия протоколов, включающая простой механизм проверки готовности удаленного устройства типа «запрос – ответ» с помощью пары сигналов, образуемых за счет аппаратных средств (RTS/CTS – уровни сигналов на контактах разъема RS232C) или программно (Xon/Xoff – служебные символы кодовой таблицы ASCII). Считается, что аппаратный способ более надежен, и он необходим для использования с модемами, поддерживающими стандарты сжатия информации v.42/V.42bis и MNP5;
- эмуляция удаленного терминала (Teletype – TTY, DEC102, ANSI и др.). На экране «местного» компьютера может быть получено изображение, идентичное изображению на мониторе удаленного компьютера.

# Приложение. Организации, занимающиеся стандартизацией сетей

В различных источниках информации по компьютерным сетям можно встретить «нерасшифрованные» обозначения стандартов, к примеру, X.25 или IEEE 802.3. В обозначении последнего стандарта, по крайней мере, фигурирует название широко известной организации. На самом деле для обозначения стандартов используется сложившаяся система с определенной группы обозначений, «монополизированных» той или иной организацией. Среди организаций, занимающихся стандартизацией в области компьютерных сетей, наиболее часто упоминаются 4 международных центра, которые расположены в Женеве (Швейцария), и 4 организации США (см. табл. П.1). Если сокращенное русское название организации при ссылке на нее или на соответствующие стандарты не применяется (или широко не распространено), то в табл. П.1 на этом месте поставлен прочерк.

До официального принятия («де-юре») некоторые из стандартов являются таковыми «де-факто», представляя собой получившие широкое распространение программные или аппаратные продукты крупных фирм. Примером могут служить классические локальные сети, в частности Ethernet, для которых первоначальный вариант сетевой топологии, формата пакетов и метода доступа был предложен совместно фирмами Xerox, DEC и Intel. Еще один пример – технологии для модемов на скорость передачи 56 Кбит/с K56Flex и X2.

В табл. П.2 приведены некоторые обозначения стандартов, характерные для разных организаций. В одних случаях название организации входит в обозначение стандарта, в других – нет. В графе «Краткое описание содержания стандарта» приведены официальные формулировки во избежание неточных толкований.

**Таблица П.1.** Организации, занимающиеся стандартизацией в области компьютерных сетей

| Статус организации | Сокращенное название | | Полное название | |
|---|---|---|---|---|
| | англ. | русское | английское | русское |
| междун. | ITU-T | МТС-Т | International Telecommunication Union – Telecom | Международный телекоммуникационный союз – Телеком |
| междун. | ISO | МОС | International Organization for Standardization | Международная Организация по Стандартизации |
| междун. | ECMA | — | European Computer Manufactures Association | Европейская ассоциация изготовителей компьютеров |
| междун. | ETSI | — | European Telecommunications Standards Institute | Европейский институт стандартов в области телекоммуникаций |
| национ. (США) | IEEE | — | Institute of Electronic and Electrical Engineers | Институт Инженеров по Электротехнике и Радиоэлектронике |
| национ. (США) | EIA | — | Electronic Industries Association | Ассоциация электронной промышленности |
| национ. (США) | ANSI | — | American National Standards Institute | Американский национальный институт стандартов |
| национ. (США) | TIA | — | Telecommunication Industry of America | Телекоммуникационная индустрия Америки |
| национ. (США) | CBEMA | — | Computer and Business Equipment Manufactures Association | Ассоциация производителей компьютеров и оргтехники (американский аналог ECMA) |
| национ. (США) | DoD | — | Department of Defence | Министерство обороны (разработчик стека протоколов TCP/IP) |

**Таблица П.2.** Примеры обозначений стандартов

| Организация | Примеры обозначений | Краткое описание содержания стандарта | Соответствующие стандарты* |
|---|---|---|---|
| ITU-T | V.34 | Модем, обеспечивающий передачу данных со скоростями до 28800 (33600) бит/с, применяется в коммутируемой сети общего пользования и на двухточечных двухпроводных выделенных каналах телефонного типа | — |
| | X.25 | Интерфейс между оконечным оборудованием данных (ООД) и аппаратурой передачи данных (АПД) для терминалов, работающих в пакетном режиме и подключаемых к сетям передачи данных общего пользования | ECMA-40, ISO 6526 |
| ISO | ISO 646 | Набор 7-разрядных символов для обмена данными в системах обработки информации | CCITT V.3; ANSI X3.4 |
| ECMA | ECMA-40 | Структура канала HDLC | CCITT X.25, X.75; ANSI X3.66; ISO 3309 |
| | ECMA-82 | Локальные вычислительные сети. Канальный уровень. Передача в основной полосе частот с использованием CSMA/CD | IEEE 802.3 |
| EIA | RS-232C | Интерфейс между оконечным оборудованием данных (ООД) и аппаратурой передачи данных (АПД), использующих последовательный обмен двоичными данными | CCITT V.24, V.28; ISO 2110 |

* Соответствие может быть неполным.

## В серии изданы


1. Справочник по теоретическим основам радиоэлектроники / Под ред. Кривицкого Б. Х., В 2-х т. Т.2. – М.: Энергия, 1977. – 472 с.
2. Емельянов Г.А., Шварцман В.О. Передача дискретной информации: Учебник для вузов. – М.: Радио и связь, 1982. – 240 с.
3. Прангишвили И.В., Подлазов В.С., Стецюра Г.Г. Локальные микропроцессорные вычислительные сети. – М.: Наука, 1984. – 176 с.
4. Флинт Д. Локальные сети ЭВМ: Пер. с англ. – М.: Финансы и статистика, 1986. – 357 с.
5. Интерфейсы систем обработки данных: Справочник / Мячев А.А., Степанов В.Н., ЩербоВ.К., Под ред. Мячева А.А. – М.: Радио и связь, 1989. – 416 с.
6. Овчинников В.В., Рыбкин И.И. Техническая база интерфейсов локальных вычислительных сетей. – М.: Радио и связь, 1989. – 272 с.
7. Дженнингс Ф. Практическая передача данных: Модемы, сети и протоколы: Пер. с англ. – М.: Мир, 1989. – 272 с.
8. Блэк Ю. Сети ЭВМ: Протоколы, стандарты, интерфейсы: Пер. с англ. – М.: Мир, 1990. – 506 с.
9. Чернега В.С., Василенко В.А., Бондарев В.Н. Расчет и проектирование технических средств обмена и передачи информации. – М.: Высшая школа, 1990. – 224 с.
10. Райс Л. Эксперименты с локальными сетями микроЭВМ: Пер. с англ. – М.: Мир, 1990. – 268 с.
11. Шевкопляс Б.В. Микропроцессорные структуры. Инженерные решения: Справочник. – М.: Радио и связь, 1990. – 512 с.
12. Передача дискретных сообщений: Учебник для вузов / Шувалов В. П., Захарченко Н. В., Шварцман В. О. и др./ Под ред. Шувалова В. П. – М.: Радио и связь, 1990. – 464 с.
13. Игнатов В.А. Теория информации и передачи сигналов: Учебник для вузов. – 2-е изд., перераб. и доп. – М.: Радио и связь, 1991. – 280 с.
14. Технологии электронных коммуникаций. Том 23. Локальные сети NETWARE. – М.: «Эко-Трендз», «Электронные знания», 1992. – 156 с.

15. Кондратенко С.В.
Лабораторный практикум «Отладка цифровых устройств и систем»: Учебное пособие. – М.: МИФИ, 1992. – 100 с.
16. Фролов А.В., Фролов Г.В.
Локальные сети персональных компьютеров. – М.: «ДИАЛОГ-МИФИ», 1993. – 176 с.
17. Веттиг Д.
Novell NetWare: Пер. с нем. – Киев: Торгово-издательское бюро BHV, 1993. – 528 с.
18. Герасименко В.А.
Защита информации в автоматизированных системах обработки данных: развитие, итоги, перспективы. – Зарубежная радиоэлектроника, 1993, №3, с. 3–21.
19. Лапшинский А.В.
Локальные сети персональных компьютеров: В 2-х ч. – М.: МИФИ, 1994.с.
20. Модемы и их применение для передачи данных: Учебное пособие / Под общ. ред. В. М. Немчинова. – М.: МИФИ, 1994. – 56 с.
21. Технологии электронных коммуникаций. Т.62: МОДЕМЫ: Разработка и использование в России. – М.: Экотрендз, 1995. – 128 с.
22. Саломаа А.
Криптография с открытым ключом: Пер. с англ. – М.: Мир, 1995. – 318 с. (http://ateha.vvsu.ru/docs/science/crypt/).
23. Ведев Д.Л.
Защита данных в компьютерных сетях. – Открытые системы, 1995, №3(11) с. (http://www.osp.ru/os/1995/03/12.htm).
24. Фролов А.В., Фролов Г.В.
Глобальные сети компьютеров. – М.:ДИАЛОГ-МИФИ, 1996. – 288 с.
25. Нанс Б.
Компьютерные сети: Пер. с англ. – М.: «БИНОМ», 1996. – 400 с.
26. Spurgeon Ch.
Ethernet Configuration Guidelines. – Peer-to-Peer Communications, Inc., 1996. – 178 p.
27. Gigabit Ethernet. – Gigabit Ethernet Alliance, 1996. – 17 p.
28. Гук М.
Локальные сети Novell. Карманная энциклопедия. – СПб.: Питер, 1996. – 288 с.

29. Нессер Д. Дж.
Оптимизация и поиск неисправностей в сетях: Пер. с англ. – К.: «Диалектика», 1996. – 384 с.
30. Просис Дж.
Цифровая подпись: принципы работы. – PC Magazine, April 9, 1996, p. 237 ©СК Пресс 12/96. (http://pcmag.newman.ru/9612/129611.htm).
31. Компьютерные сети. Учебный курс / Пер. с англ. – М.: Издательский отдел «Русская Редакция» ТОО «Channel Trading Ltd.», 1997. – 832 с.
32. Новиков Ю.В., Калашников О.А., Гуляев С.Э.
Разработка устройств сопряжения для персонального компьютера типа IBM PC. – М.: ЭКОМ, 1997. – 224 с.
33. Жатченко С.
Средства защиты информации. – Открытые системы, 1997, №6,, с. 66–68.
(http://dtnn.da.ru/literature/sredstva.htm).
34. Новиков Ю.В., Карпенко Д.Г.
Оптоволоконная локальная сеть персональных компьютеров типа «звезда»// Информационные технологии и системы. Hardware Software Security. Тенденции и перспективы. Сборник статей / Сост. Мельников Д.Я. – М., Международная академия информатизации, 1997, с. 24–33.
35. Новиков Ю.В., Карпенко Д.Г.
Комбинированный метод доступа к каналу для волоконно-оптической сети компьютеров типа «кольцо»//Электроника и информатика – 97. Вторая всероссийская научно-техническая конференция с международным участием: Во 2 ч. Тезисы докладов. – М.: МИЭТ, 1997, с. 64–65.
36. Новиков Ю.В., Карпенко Д.Г.
Аппаратура локальных сетей: функции, выбор, разработка. – М.: ЭКОМ, 1998.– 288 с.
37. Новиков Ю.В., Карпенко Д.Г.
Волоконно-оптическая сеть персональных компьютеров типа «кольцо» //Информационные продукты, процессы и технологии. Computer-Aided Software and Hardware Engineering. – М.: Технология машиностроения, 1998, с. 66–73.
38. Мюллер С.
Модернизация и ремонт персональных компьютеров. / Пер. с англ. – М.: ЗАО «Издательство БИНОМ», 1998. – 944 с.
39. Куин Л., Рассел Р.
Fast Ethernet. – К.: Издательская группа BHV, 1998. – 448 с.

40. Гук М.
Аппаратные средства IBM PC. Энциклопедия. –
СПб.: Питер Ком, 1999. – 816 с.
41. Новиков Ю.В., Кондратенко С.В.
Локальные сети. Архитектура, алгоритмы, проектирование. –
М.: ЭКОМ, 2000. – 312 с.
42. Закер К.
Компьютерные сети. Модернизация и поиск неисправностей. –
СПб.: БХВ-Петербург, 2001. – 1008 с.
43. Гук М. Аппаратные средства локальных сетей. –
СПб.: Питер, 2001.– 576 с.
44. Ирвин Дж., Харль Д.
Передача данных в сетях: инженерный подход: Пер. с англ. –
СПб.: БХВ-Петербург., 2003. – 448 с.
45. Хамбракен Д.
Компьютерные сети: Пер. с англ. – М.: ДМК Пресс, 2004. – 448 с.
46. Сунчелей И.Р., Стрижаков С.К., Семенов А.Б.
Структурированные кабельные системы. 5-е изд.
Издательство: Компания АйТи, ДМК. 2004, — 640 с.
47. Погорелов, А. В. Черемушкин, С. И. Чечета
Об определении основных криптографических понятий
/ Интернет-публикация (http://www.cryptography.ru/db/msg.html)
48. «Последняя миля» – варианты решения / Интернет-публикация
(http://www.russ.ru/netcult/20020404–dorozhkin.html)
49. Решения компании Cisco Systems по обеспечению безопасности
корпоративных сетей (издание II) / Интернет-публикация
(http://www.cisco.com/global/RU/isp/broch/Security.pdf)
50. Информационные материалы фирмы «Телеком-сервис ИТ»
/ Интернет-публикация (http://www.teleserv.ru)
51. Информационные материалы фирмы «ЭКОЛАН ТЕК»
/ Интернет-публикация ( http://www.ecolan.ru)
52. http://www.wiley/com/compbooks/fastethernet
53. http://www.gigabit-ethernet.org
54. http://www.microsoft.com/rus
55. http://www.novell.ru

# Словарь терминов и сокращений

**10BASE2** – стандарт сегмента сети Ethernet на тонком коаксиальном кабеле.
**10BASE5** – стандарт сегмента сети Ethernet на толстом коаксиальном кабеле.
**10BASE-T** – стандарт сегмента сети Ethernet на витой паре.
**10BASE-FL** – стандарт сегмента сети Ethernet на оптоволоконном кабеле.
**100BASE-T4** – стандарт сегмента сети Fast Ethernet на счетверенной витой паре.
**100BASE-TX** – стандарт сегмента сети Fast Ethernet на сдвоенной витой паре.
**100BASE-FX** – стандарт сегмента сети Fast Ethernet на оптоволоконном кабеле.
**100VG-AnyLAN** – локальная сеть в соответствии со стандартом IEEE 802.12 со скоростью передачи 100 Мбит/с, централизованным управлением обменом, топологией типа «звезда» и средой передачи «витая пара».
**1000BASE-SX** – стандарт сегмента сети Gigabit Ethernet на оптоволоконном кабеле с длиной волны света 0,85 мкм.
**1000BASE-LX** – стандарт сегмента сети Gigabit Ethernet на оптоволоконном кабеле с длиной волны света 1,3 мкм.
**1000BASE-CX** – стандарт сегмента сети Gigabit Ethernet на экранированной витой паре.
**1000BASE-T** – стандарт сегмента сети Gigabit Ethernet на неэкранированной витой паре.
**4B/5B** – самосинхронизирующийся код для передачи данных, применяемый в сети FDDI, в котором 4 бита данных преобразуются в 5 бит, передаваемых в сеть.
**5B6B** – самосинхронизирующийся код передачи данных, применяемый в сети 100VG-AnyLAN, в котором 5 бит данных преобразуются в 6 бит, передаваемых в сеть.
**8B6T** – код передачи данных, используемый в сегменте сети Fast Ethernet 100BASE-T4, в котором 8 передаваемых бит преобразуются в 6 трехуровневых сигналов.
**8B/10B** – код передачи данных, который будет использоваться в сети Gigabit Ethernet.
**AC (Access Control)** – управление доступом.
**AM (Amplitude Modulation)** – амплитудная модуляция, АМ.
**ANSI (American National Standards Institute)** – Национальный институт стандартов США.
**API (Application Programming Interfaces)** – интерфейсы прикладных программ (относятся к 6 уровню модели OSI).
**Arcnet (ARCnet, Attached Resource Computer Net)** – локальная сеть, разработанная фирмой Datapoint Corporation (скорость передачи – 2,5 Мбит/с, метод доступа – маркерный).

**ARP (Address Resolution Protocol)** – высокоуровневый протокол определения адресов абонентов сети.

**ASCII (American Standard Code for Information Interchange)** – американский стандартный код обмена информацией (8 разрядов).

**ASN.1 (Abstract Syntax Notation 1)** – абстрактное описание синтаксиса, формат описания данных в протоколе SNMP.

**ATM (Asynchronous Transfer Mode)** – технология передачи информации, при которой по сети одновременно передаются данные, аудио- и видеосигналы, а также соответствующие технические средства одноименной сети, обеспечивающие обмен информацией на скорости до 622 Мбит/с.

**AUI (Access Unit Interface)** – тип разъема и кабеля для подключения сетевого адаптера Ethernet к трансиверу (MAU) толстого коаксиального кабеля.

**Auto-Negotiation** – протокол автодиалога для автоматического согласования скоростей передачи в сети Fast Ethernet.

**Backbone network** – стержневая, базовая, опорная сеть, представляющая собой линию связи, или аппаратура с высокой пропускной способностью, соединяющая отдельные части единой локальной сети или несколько локальных сетей.

**Balun (Balance-Unbalance)** – согласующее пассивное устройство.

**Bandwidth** – пропускная способность (вместимость) информационного канала или среды передачи, обычно измеряется в Мбит/с или МГц.

**Baud** – бод.

**Baudrate** – скорость передачи в бодах.

**BFOC/2.5** – стандарт оптоволоконного байонетного ST-разъема.

**BER (Bit Error Ratio)** – относительное количество ошибочных бит.

**BNC (Bayonet Neill Concelnan)** – разъем байонетного типа, применяющийся, в частности, в сети Ethernet для соединения адаптера с тонким коаксиальным кабелем.

**BPDU (Bridge Protocol Data Units)** – элементы данных протокола моста, применяемого мостами сети для установления структуры сети и устранения петель.

**Broadcast** – широковещательная передача, при которой пакет (сообщение) получают все абоненты сети независимо от их сетевого адреса.

**BSC (Binary Synchronous Communications)** – двоичная синхронная передача данных.

**BT (Bit Time)** – время передачи одного бита в сети.

**CAN (Campus Area Network)** – сеть, объединяющая группу близко расположенных зданий.

**CCITT (Consultative Committee on International Telephony and Telegraphy)** – Международный консультативный комитет по телефонии и телеграфии, МККТТ.

**CD (Collision Detection)** – обнаружение коллизий, столкновений пакетов.

**CDDI (Copper Distributed Data Interface)** – реализация сети FDDI на электрическом (медном) кабеле, то же, что TPDDI и SDDI.

**Cheapernet** – довольно распространенное название сети или сегмента Ethernet на тонком коаксиальном кабеле (в отличие от сегмента или сети на толстом коаксиальном кабеле).

**Collapse** – крах сети, резкое падение производительности сети из-за перегрузки передаваемым потоком информации.

**Collision domain** – область (зона) конфликта, то есть часть сети (например, Ethernet), на которую распространяется ситуация конфликта (коллизии) передаваемых пакетов.

**CRC (Cyclic Redundancy Check)** – метод контроля правильности передачи с использованием помехоустойчивого циклического кода, а также циклическая контрольная сумма (обычно 16- или 32-разрядная).

**Crosstalk** – взаимное влияние кабелей и проводов друг на друга, перекрестные наводки.

**CS (Control Sum)** – контрольная сумма.

**CSMA/CA (Carrier-Sense Multiple Access/Collision avoidance)** – децентрализованный метод доступа к сети с контролем несущей (с контролем наличия передачи) и избежанием конфликтов.

**CSMA/CD (Carrier-Sense Multiple Access/Collision detection)** – децентрализованный метод доступа к сети с контролем несущей (с контролем наличия передачи) и обнаружением конфликтов, применяемый, в частности, в сети Ethernet. Распространенное сокращение – МДКН/ОК.

**Cut-Trough** – тип коммутаторов, в которых не происходит полного приема коммутируемого пакета.

**DA (Destination Address)** – адрес получателя.

**DAC (Dual-Attachment Concentrator)** – концентратор сети FDDI двойного подключения.

**DAS (Dual-Attachment Stations)** – абоненты (станции) сети FDDI двойного подключения.

**DB9** – стандартный 9-контактный разъем, используемый в сети Token-Ring.

**DB15** – стандартный 15-контактный разъем, используемый при подключении трансиверов Ethernet.

**DCE (Data Communications Equipment)** – аппаратура передачи данных, например, модем (АПД).

**DES (Data Encryption Standard)** – стандарт шифрования данных США (с 1976 г.), относящийся к группе методов симметричного шифрования.

**DIX** – объединение фирм DEC (Digital), Intel и Xerox, созданное для поддержки и стандартизации сети Ethernet.

**DMI (Desktop Management Interface)** – интерфейс управления настольными компьютерами.

**DPSK (Differential Phase Shift Keying)** – дифференциальная фазоразностная модуляция, использовавшаяся в модемах с относительно низкой скоростью передачи (до 4800 бит/с). В настоящее время в высокоскоростных модемах применяются более совершенные методы модуляции QAM и TCM.

**DTE (Data Terminal Equipment)** – оконечное оборудование данных (ООД), источник или приемник информации — например, компьютер.

**ECS (Excessive Collision Error)** – множественные коллизии, то есть больше 60 коллизий подряд (ошибка в сети Ethernet).

**ECMA (European Computer Manufacturers Association)** – Европейская Ассоциация производителей компьютеров, международная организация.

**ECTP (Ethernet Configuration Test Protocol)** – протокол тестирования конфигурации сети Ethernet.

**EIA/TIA 568 (Commercial Building Telecommunications Cabling Standard)** – стандарт на кабели для локальных сетей, определяющий их основные характеристики (затухания на различных частотах, отражения, количество витков на метр длины и т.д.).

**Ethernet** – наиболее распространенная в мире локальная сеть, предложенная фирмой Xerox (топология – шина, метод доступа — CSMA/CD, скорость передачи – 10 Мбит/с). Удовлетворяет стандарту IEEE 802.3.

**ETR (Early Token Release)** – раннее формирование маркера (в сети Token-Ring).

**Fast Ethernet** – высокоскоростная разновидность сети Ethernet, обеспечивающая скорость передачи 100 Мбит/с. Удовлетворяет доработанному стандарту IEEE 802.3u (стандарт утвержден в 1995 году).

**FCC (Federal Communications Commission)** – Федеральная комиссия по связи.

**FCE (False Carrier Event)** – ложная несущая, передача данных без признака начала пакета (ошибка в сети Ethernet).

**FCS (Frame Check Sequence)** – проверочная последовательность кадра, контрольная сумма.

**FDDI (Fiber Distributed Data Interface)** – кольцевая оптоволоконная высокоскоростная локальная сеть (метод доступа – маркерный, скорость передачи – 100 Мбит/с).

**FIRL** – то же, что FOIRL.

**FLP (Fast Link Pulse)** – сигналы, передаваемые в промежутках между пакетами в сети Fast Ethernet в режиме автодиалога (автоматического согласования скоростей передачи).

**FM (Frequency Modulation)** – частотная модуляция, ЧМ.

**FOIRL (Fiber Optic Inter-Repeater Link)** – стандарт оптоволоконной связи между двумя репитерами сети Ethernet.

**FOMAU (Fiber Optic MAU)** – оптоволоконные трансиверы сети Ethernet.

**Frame** – кадр, пакет, единица передаваемой по сети информации.

**FTP (File Transfer Protocol)** – протокол передачи файлов, используемый в сети Интернет.

**Full duplex** – режим полнодуплексной передачи, при котором передача может идти по линии связи в две стороны одновременно.

**GAN (Global Area Network)** – глобальная сеть.

**Gigabit Ethernet** – разрабатываемая сверхвысокоскоростная версия сети Ethernet, обеспечивающая скорость передачи 1 Гбит/с.

**Half duplex** – режим полудуплексной передачи, при котором передача может идти по линии связи в две стороны, но не одновременно.

**HST (High-Speed Technology)** – технология быстрой передачи данных (один из стандартов модуляции сигналов в модемах).

**HTML (Hypertext Markup Language)** – язык, используемый для создания страниц WWW-серверов, а также сами эти страницы.

**HTTP (Hypertext Transport Protocol)** – протокол передачи по сети страниц WWW-серверов.

**I-connector** – соединитель двух кусков тонкого коаксиального кабеля, оснащенных разъемами BNC на концах.

**IAB (Internet Activities Board)** – Комиссия по деятельности в сети Интернет.

**IEC (International Electrotechnical Committee)** – Международный электротехнический комитет (МЭК).

**IEEE (Institute of Electrical and Electronic Engineers)** – Институт инженеров по электронике и радиотехнике (ИИЭР), организация, занимающаяся, в частности, стандартизацией локальных сетей.

**IEEE 802.1** – стандарт IEEE на объединение сетей.

**IEEE 802.2** – стандарт IEEE на управление логической связью в сетях.

**IEEE 802.3** – стандарт IEEE, которому удовлетворяет сеть Ethernet (топология — шина, метод доступа — CSMA/CD, среда передачи – коаксиальный кабель, скорость передачи — 10 Мбит/с и т.д.).

**IEEE 802.3u** – стандарт IEEE, которому удовлетворяет сеть Fast Ethernet.

**IEEE 802.3z** – стандарт IEEE, которому удовлетворяет сеть Gigabit Ethernet.

**IEEE 802.4** – стандарт IEEE, который определяет широкополосную маркерную шину со скоростью передачи 10 Мбит/с, максимальной длиной 1,5 км и с числом абонентов до 64.

**IEEE 802.5** – стандарт IEEE, которому удовлетворяет сеть IBM Token-Ring (топология — кольцо, маркерный доступ, среда передачи – витая пара, скорость передачи — 4 Мбит/с и т.д.).

**IEEE 802.6** – стандарт IEEE на городскую сеть (Metropolitan Area Network, MAN).

**IEEE 802.7** – стандарт IEEE на широковещательную технологию.

**IEEE 802.8** – стандарт IEEE на оптоволоконную технологию.

**IEEE 802.9** – стандарт IEEE на интегрированные сети с передачей речи и данных.

**IEEE 802.10** – стандарт IEEE на безопасность сетей.

**IEEE 802.11** – стандарт IEEE на беспроводные сети.

**IEEE 802.12** – стандарт IEEE, которому удовлетворяет сеть 100VG-AnyLAN (скорость передачи — 100 Мбит/с, топология — звезда, централизованное управление доступом и т.д.).

**IP (Internet Protocol)** – протокол доставки дейтаграмм в Интернет.

**IP-address** – адрес, идентифицирующий пользователей сети Интернет.

**IPG (InterPacket Gap)** – межпакетная щель, межкадровый интервал, минимально допустимый временной промежуток между пакетами Ethernet (96 битовых интервалов).

**IPX (Internet Packet Exchange)** – протокол обмена пакетами в сети без логического соединения.

**IPX/SPX** – набор протоколов низких уровней, используемый в сетях Novell NetWare.

**ISA (Industrial System Architecture)** – наиболее распространенная в настоящее время системная магистраль персональных компьютеров типа IBM PC. Имеет 16 разрядов данных.

**ISDN (Integrated Services Digital Network)** – цифровая сеть с интеграцией служб передачи телефонных, телевизионных сигналов и данных по одной линии.

**ITU-T (International Telecommunication Union – Telecom)** – Международный Телекоммуникационный союз – Телеком (МТС-Т).

**Jabber** – ошибка в сети Ethernet/Fast Ethernet, чрезмерно затянувшаяся передача пакета, то есть, время передачи составляет более 400 мкс (в сети Fast Ethernet) или свыше 4000 мкс (в сети Ethernet).

**K56Flex** – стандарт «де-факто» от фирм 3COM, Rockwell и Lucent Technologies для аналоговых модемов со скоростью обмена, достигающей 33,6 Кбит/с (при передаче данных в сеть) и 56 Кбит/с (при приеме данных от цифрового модема провайдера). Широко применялся до появления международного стандарта V.90 в 1998 году.

**LAN (Local Area Network)** – локальная (вычислительная) сеть, ЛВС.

**LAPM (Link Access Procedure for Modems)** – процедура доступа к линии связи для модемов.

**LED (Light Emitted Diode)** – светодиод.

**LLC (Logical Link Control)** – верхний подуровень второго уровня модели OSI (уровня управления линией передачи), отвечающий за управление логическими связями.

**Login** – процесс подтверждения личности пользователя компьютерной сети, используемый для контроля доступа к сети.

**MAC (Media Access Control)** – нижний подуровень второго уровня модели OSI (уровня управления линией передачи), отвечающий за управление доступом к среде передачи.

**MAC-адрес** – уникальный 48-битный адрес сетевого адаптера, устанавливаемый производителем адаптера. Применяется в сетях Ethernet, Token-Ring, FDDI.

**MAN (Metropolitan Area Network)** – глобальная сеть в масштабах города.

**Manchester-II** – самосинхронизирующийся двухуровневый код передачи данных, применяющийся, в частности, в сети Ethernet.

**MAU (Medium Attachment Unit)** – трансивер сети Ethernet на толстом коаксиальном кабеле, устанавливаемый непосредственно на кабеле. См. также MSAU.

**Mbps (Mb/s, Mbits per second)** – мегабит в секунду (Мбит/с), единица измерения скорости передачи и пропускной способности среды передачи.

**MDI (Medium Dependent Interface)** – интерфейс, зависящий от среды, средства непосредственной связи со средой передачи, например, разъем.

**MIB (Management Information Base)** – база данных управляющей информации, используемая в протоколе SNMP.

**MII (Medium Independent Interface)** – интерфейс, не зависящий от среды передачи, связывающий адаптер или концентратор с трансивером среды.

**MMF (Multimode Fiber-optic cable)** – мультимодовый оптоволоконный кабель.

**MNP (Microcom Networking Protocol)** – стандартный набор протоколов модемной связи, предложенный фирмой Microcom.

**MSAU или MAU (Multistation Access Unit)** – концентраторы сети IBM Token-Ring.

**NDIS (Network Driver Interface Specification)** – спецификация интерфейса сетевого драйвера.

**NE2000** – популярный тип адаптера сети Ethernet (фирма Novell), ставший одним из фактических стандартов.

**NetBEUI** – расширенный интерфейс NetBIOS.

**NetBIOS (Network Basic Input/Output System)** – сетевое программное обеспечение сеансового уровня модели OSI, разработанное первоначально фирмой IBM и ставшее впоследствии фактическим стандартом.

**NEXT (Near End CrossTalk)** – ослабление перекрестной наводки на ближнем конце.

**NIC (Network Interface Card)** – сетевой адаптер (контроллер), сетевая карта.

**NLP (Normal Link Pulse)** – сигналы, передаваемые в сегментах 10BASE-T между пакетами для контроля целостности линии связи.

**NMS (Network Monitoring Station)** – станция управления сетью, работающая с протоколом SNMP.

**NOS (Network Operational System)** – сетевая операционная система.

**NVP (Nominal Velocity of Propagation)** – скорость распространения сигнала в кабеле, выражается в долях от скорости света С, например, NVP = 0,7С.

**NRZ (Non-Return to Zero)** – простейший несамосинхронизирующийся код передачи данных (без возврата к нулю), применяемый, например, в интерфейсе RS-232C.

**ODI (Open Data link Interface)** – открытый интерфейс канала данных, спецификация, позволяющая сетевому адаптеру работать с сетями Novell NetWare и совместимыми с ними.

**OSI (Open System Interchange)** – модель взаимодействия открытых систем (ВОС), которая выделяет семь уровней в сетевых функциях: 1 — физический, 2 – канальный, 3 – сетевой, 4 – транспортный, 5 – сеансовый, 6 – представительский, 7 – уровень приложений.

**Overload** – перегрузка сети чрезмерно большим потоком передаваемой информации.

**PCI (Peripheral Component Interconnect)** – быстродействующая 32- или 64-разрядная магистраль, применяющаяся в персональных компьютерах типа IBM PC.

**PDU (Protocol Data Unit)** – модуль данных протокола, блок данных в дейтаграмме, используемый в протоколе SNMP.

**PDV (Path Delay Value)** – двойное (круговое) время задержки прохождения сигнала по сети. Учитывает суммарную задержку в кабельной системе, сетевых адаптерах, репитерах и других сетевых устройствах.

**PGP (Pretty Good Privacy)** – метод шифрования данных, относящийся к группе методов несимметричного шифрования. Широко используется в сети Интернет для защиты сообщений, передаваемых посредством электронной почты.

**PHY** – средства взаимодействия с физической средой передачи в сети (входят в первый уровень модели OSI), также приемопередатчик.

**Plenum** – тип кабеля в тефлоновой оболочке, более устойчивый к воздействиям окружающей среды, чем обычный кабель (non-plenum); при горении не выделяет токсичных газов.

**Plug and Play (PnP, P&P)** – стандартная технология автоматической настройки параметров плат, подключаемых к компьютеру, фирм Microsoft, Compaq, Intel и Phoenix Technologies.

**PM (Phase Modulation)** – фазовая модуляция.

**PMD (Physical Medium Dependent)** – нижний подуровень первого (физического) уровня модели OSI, зависящий от типа среды передачи.

**PMI (Physical Medium Independent)** – верхний подуровень первого (физического) уровня модели OSI, не зависящий от типа среды передачи.

**PPP (Point-to-Point Protocol)** – протокол связи с Интернетом по телефонному каналу.

**PVC** – поливинилхлоридная оболочка кабеля.

**QAM (Quadrature Amplitude Modulation)** – многопозиционная амплитудно-фазовая модуляция, используемая в высокоскоростных модемах (скорость передачи до 9600 бит/с). Улучшенный вариант – метод TCM.

**RG-11** – распространенный тип толстого коаксиального кабеля сети Ethernet с волновым сопротивлением 50 Ом.

**RG-58 A/U** – распространенный тип тонкого коаксиального кабеля сети Ethernet с волновым сопротивлением, равным 50 Ом.

**RG-62 A/U** – распространенный тип коаксиального кабеля для сети Arcnet с волновым сопротивлением 93 Ом.

**RJ-11** – четырехконтактный разъем, используемый для подключения телефонных кабелей.

**RJ-45** – тип разъема для присоединения кабеля на основе витых пар (8 контактов).

**RL (Ring Latency)** – кольцевая задержка.

**RMON (Remote Network Monitoring)** – система удаленного мониторинга сети.

**RS-232C** – стандартный интерфейс последовательной передачи данных компьютера.

**RSA (Rivest, Shamir, Adleman)** – метод шифрования данных, относящийся к группе методов несимметричного шифрования.

**Runt frame** – карликовый кадр (пакет), кадр в сети Ethernet, имеющий длину меньше минимальной (512 бит).

**RXC (Received Clock)** – принимаемый синхроимпульс.

**RX, RXD (Received Data)** – принимаемые данные.

**RZ (Return to Zero)** – самосинхронизирующийся трехуровневый код передачи данных.

**SA (Source Address)** – адрес отправителя.

**SAC (Single-Attachment Concentrator)** – концентратор сети FDDI одинарного подключения.

**SAF** – см. Store-and-Forward.

**SAS (Single-Attachment Stations)** – абоненты (станции) сети FDDI одинарного подключения.

**SCS (Structured Cabling System)** – структурированная кабельная система для локальной сети (СКС).

**SDDI (Shielded Distributed Data Interface)** – реализация сети FDDI на экранированной витой паре; то же, что CDDI и TPFDDI.

**SDLC (Synchronous Data Link Control)** – стандарт синхронного управления передачей данных.

**SFD (Start of Frame Delimiter)** – признак начала кадра.

**Simplex** – режим симплексной передачи, при котором передача может идти только в одном направлении: от передатчика к приемнику.

**SLAN (Switched Local Area Network)** – коммутируемая локальная сеть, то есть сеть, содержащая коммутаторы (переключатели).

**Slot time** – максимально допустимое время окна коллизий в сети Ethernet (512 битовых интервалов).

**SMF (Single Mode Fiber-optic cable)** – одномодовый оптоволоконный кабель.

**SMTP (Simple Mail Transfer Protocol)** – протокол передачи сообщений электронной почты, используемый в сети Интернет.

**SNA (System Network Architecture)** – архитектура сетевых систем, предложенная фирмой IBM и ориентированная на объединение компьютеров самых разных типов.

**SNMP (Simple Network Management Protocol)** – протокол обмена для удаленной управляющей станции в сети Ethernet, служащей для контроля нагрузки сети, интенсивности ошибок в сети, а также для автоматического отключения неисправных сегментов.

**SPD (Simple Propagation Delay)** – простая (не двойная, не круговая) задержка распространения сигнала в сети.

**Store-and-Forward** – тип коммутаторов, в которых производится полный прием (хранение) коммутируемых пакетов.

**STP (Shielded Twisted-Pair cable)** – кабель на основе экранированных витых пар, сами экранированные витые пары.

**SPX (Sequenced Packet Exchange)** – протокол обмена пакетами с логическим соединением.

**T-connector** – Т-образный соединитель, служащий для подключения двух кусков тонкого коаксиального кабеля к сетевому адаптеру.

**TCM (Trellis Coded Modulation)** – модуляция с решетчатым кодированием, многопозиционная амплитудно-фазовая модуляция. Улучшенный вариант метода QAM, использующий его на одном из этапов преобразования сигналов.

**TCP (Transmission Control Protocol)** – протокол гарантированной доставки пакетов в Интернет.

**TCP/IP** – набор протоколов нижних уровней для связи в гетерогенной среде, применяемый в сети Интернет.

**Terminator** – терминатор, согласующее устройство, выполняющее электрическое согласование кабеля на обоих его концах. Представляет собой резистор с сопротивлением, равным волновому сопротивлению применяемого кабеля. Присоединяется к кабелю с помощью разъема.

**TIA (Telecommunication Industry Association)** – Ассоциация телекоммуникационной промышленности.

**Token-Ring** – кольцевая локальная сеть компании IBM с маркерным методом доступа и скоростью передачи 4 Мбит/с.

**TP (Twisted Pair)** – витая пара.

**TPFDDI (TDDI)** – версия сети FDDI на электрическом кабеле (витой паре) со скоростью передачи данных 100 Мбит/с, то же, что CDDI и SDDI.

**TXC (Transmitted Clock)** – принимаемый синхроимпульс.

**TX, TXD (Transmitted Data)** – передаваемые данные.

**UART (Universal Asynchronous Receiver/Transmitter)** —универсальный асинхронный приемопередатчик (УАПП).

**UPS (Uninterruptable Power Supply)** – источник бесперебойного питания на основе аккумулятора.

**UTP (Unshielded Twisted-Pair cable)** – кабель на основе неэкранированных витых пар, сами неэкранированные витые пары.

**URL (Uniform Resource Locator)** – адрес ресурсов специального вида, применяемый в сети Интернет.

**USART (Universal Synchronous/Asynchronous Receiver/Transmitter)** – универсальный синхронно-асинхронный приемопередатчик (УСАПП).

**V.34** – стандарт ITU-T для аналоговых модемов, обеспечивающих передачу данных со скоростями до 33,6 Кбит/с для использования на коммутируемой сети общего пользования и на двухточечных двухпроводных выделенных каналах телефонного типа.

**V.90** – стандарт ITU-T для модемов, обеспечивающих передачу данных со скоростями до 56 Кбит/с. После принятия в 1998 году подвел итог борьбе двух стандартов «де-факто» — K56Flex и X2.

**WAN (Wide Area Network)** – глобальная (вычислительная) сеть, ГВС.

**WLAN (Wireless LAN)** – беспроводная локальная сеть.

**WWW (World Wide Web)** – гипертекстовая мультимедийная служба в сети Интернет, содержащая информацию в гипертекстовом виде.

**X2** – аналог стандарта «де-факто» K56Flex. Принадлежит фирме US Robotics.

**xDSL** – цифровые абонентские линии интегрального облуживания, замещающие обычные аналоговые телефонные линии, имеющие ряд преимуществ (большая скорость передачи информации, постоянные подключения вместо коммутируемых, дополнительные виды сервиса).

**Абонент сети (узел)** – любое устройство, подключенное к сети и общающееся с ней (компьютер, принтер, сканер и т.д.).

**Адаптер сетевой** – электронная плата (карта) для сопряжения компьютера со средой передачи информации в сети.

**АМ** – амплитудная модуляция.

**АЦП** – аналого-цифровой преобразователь.

**Бездисковые компьютеры** – компьютеры без жестких и гибких дисков, начальная загрузка которых производится из сети с помощью загрузочного ПЗУ на плате сетевого адаптера.

**Бод (Baud)** – одно изменение сигнала в секунду. В случае кода NRZ 1 Бод равен 1 бит/с.

**Вероятность ошибки** – допустимое стандартами относительное число ошибочных бит в информации, принятой после передачи по протяженной последовательной линии с помехами. Для цифровых данных

может задаваться на уровне 10-6...10-9, что соответствует не более чем одному ошибочному биту из 106...109 принятых бит.

**Виртуальный канал** – последовательность логических соединений между посылающим и принимающим компьютером, происходящих при передаче информации.

**Витая пара** – среда передачи информации из двух перекрученных между собой электрических проводов, характеризующаяся наибольшей простотой монтажа и низкой стоимостью.

**Волновое сопротивление (импеданс)** – характеристика кабеля, определяющая его свойства по передаче сигналов на большие расстояния (измеряется в Омах).

**Время канала (slot time)** – максимально допустимое окно коллизий для сегмента в сетях типа Ethernet и Fast Ethernet, равное 512 • BT, то есть 51,2 мкс и 5,12 мкс соответственно.

**Время доступа** – временной интервал между возникновением заявки на передачу данного абонента и получением права на передачу.

**Выделенный (dedicated) сервер** – компьютер в сети, работающий исключительно как сервер сети и не способный выполнять другие (не сетевые) задачи.

**Гаммирование** – один из простейших способов шифрования данных, основанный на сложении их цифрового представления с маской конечной или бесконечной длины.

**Группа** – логическое объединение компьютеров сети, решающих общие задачи и имеющих одинаковые права доступа.

**Датаграмма, дейтаграмма** – способ передачи пакетов без подтверждения получения в произвольном порядке; правильный порядок восстанавливается принимающим абонентом.

**Децентрализованное управление обменом** – метод управления обменом в сети, при котором нет выделенного центра управления, и все абоненты равноправны (хотя и могут иметь разные приоритеты по захвату сети).

**Децибел** – логарифмическая единица отношения двух физических величин.

**Диаметр сети** – путь максимальной длины в сети Ethernet, то есть путь между двумя абонентами с максимальной для данной сети задержкой распространения сигнала.

**Домен** – в сетях Microsoft – логическое объединение компьютеров, в отношении которых проводится единая политика безопасности.

**Доменная система имен** – система преобразования имен пользователей сети Интернет в IP-адреса, строящаяся по многоуровневому принципу.

**Драйвер адаптера** – программа, осуществляющая взаимодействие аппаратуры драйвера и сетевого программного обеспечения.

**Затухание сигнала** – ослабление передаваемого сигнала при его прохождении по сети, доля мощности сигнала, потерянная при прохождении по кабелю. Измеряется в децибелах (дБ).

**Затянувшаяся передача** – см. Jabber.

**Захват сети** – получение абонентом сети права на передачу пакета.

**Защита информации (компьютерная безопасность)** – совокупность методов и средств, обеспечивающих целостность, конфиденциальность и доступность информации в условиях воздействия угроз естественного или искусственного происхождения, реализация которых может привести к нанесению ущерба владельцам или пользователям информации.

**Звезда (star)** – вид топологии локальной сети, в котором к одному центральному абоненту (концентратору) подключаются несколько периферийных абонентов; при этом все управление сетью и (или) передачу всей информации в ней осуществляет центральный абонент.

**Зона конфликтов (область коллизий)** – множество абонентов (узлов) сети Ethernet, осуществляющих доступ к сети по методу CSMA/CD. Часть сети, на которую распространяется ситуация конфликта. Может включать в себя всю сеть.

**Инкапсуляция (encapsulating)** – процесс последовательного вложения пакетов при переходе между уровнями модели OSI.

**Источник бесперебойного питания** – устройство, обеспечивающее электроснабжение потребителей (компьютеров, концентраторов, принтеров и т.д.) при сбоях в электросети.

**Кадр** – базовый элемент передаваемых данных в сети, снабжен служебной информацией. Часто то же самое, что и пакет.

**Клиент** – абонент, не отдающий своего ресурса в сеть, но имеющий доступ к ресурсам сети. Иногда клиенты называются также рабочими станциями в противоположность серверу.

**Коаксиальный кабель** – среда передачи информации, электрический кабель, состоящий из центрального проводника и металлической оплетки, разделенных диэлектриком.

**Кодер/Декодер** – одно из устройств модема, осуществляющее статистическое сжатие/распаковку данных, а также их защиту от помех за счет формирования и анализа помехоустойчивого циклического кода, добавляемого в конец пакета с данными.

**Коллизия** – ситуация, при которой в сеть передаются несколько пакетов одновременно, что вызывает искажение информации. Называется также конфликтом или столкновением.

**Кольцо (ring)** – вид топологии локальной сети, в котором все абоненты последовательно передают информацию друг другу по цепочке, замкнутой в кольцо.

**Концентратор (hub)** – устройство, служащее для объединения нескольких сегментов единой сети и не преобразующее передаваемую информацию.

**Комбинированный маршрутизатор (brouter)** – устройство (компьютер), являющееся комбинацией моста и маршрутизатора.

**Коммутатор, коммутирующий концентратор, переключатель (switching hub, switch)** – концентратор, передающий на другие сегменты только те пакеты, которые адресованы им, с целью снижения нагрузки на сеть.

**Коммутатор Cut-Through** – коммутатор, начинающий ретранслировать пакеты (кадры) до того как полностью получит их.

**Коммутатор Store-and-Forward** – коммутатор, который получает и хранит полный пакет (кадр) перед тем, как ретранслировать его.

**Конфликт, коллизия (collision)** – ситуация, при которой в сеть передаются несколько пакетов, что вызывает искажение информации.

**Концентратор (Hub)** – промежуточное устройство в сети, объединяющее несколько сегментов сети. По умолчанию предполагается репитерный концентратор, ретранслирующий приходящие на него пакеты без обработки.

**Криптография** – преобразование информации с целью исключения доступа к ней со стороны нелегальных пользователей и подмены информации. Включает в себя шифрование и комплекс мер для достижения второй цели (цифровые подписи, имитовставки и хэш-функции).

**Кэширование** – хранение в оперативной памяти копии наиболее часто требуемой информации с целью ускорения доступа к ней.

**ЛВС** – локальная вычислительная сеть.

**Локальная сеть** – компьютеры или другие устройства, соединенные линиями связи для высококачественной передачи информации между ними, как правило, на сравнительно небольшие расстояния.

**ЛС** – локальная сеть.

**Маркер** – уникальная комбинация битов или пакет специального вида, использующийся для процедуры захвата сети.

**Маркерное кольцо** – детерминированный метод доступа в локальных сетях, альтернативный случайному методу доступа CSMA/CD и обеспечивающий, в отличие от него, отсутствие коллизий и гарантированное сверху время доставки данных в сетях при отсутствии перегрузок. Допускает организацию системы приоритетов между абонентами.

**Маршрутизатор (router)** – устройство (компьютер), служащее для определения маршрута, по которому наиболее целесообразно пересылать пакет.

**Межкадровый интервал (межпакетная щель, IPG)** – интервал между двумя пакетами (кадрами).

**Метод доступа** – способ определения, какой из абонентов сети может захватить сеть и начать передачу своего пакета.

**Модем (модулятор-демодулятор)** – устройство, преобразующее цифровые данные от компьютера в аналоговые сигналы перед их передачей по последовательной линии и производящее обратное преобразование после передачи. Кроме функции согласования полосы частот, занимаемой передаваемыми сигналами, с полосой пропускания реальной линии передачи, выполняют много других функций, как правило, аппаратными средствами (сжатие данных, формирование и проверка помехоустойчивого циклического кода, эхо-компенсация и др.).

**Модуляция** – преобразование цифровых данных в аналоговую форму для передачи по аналоговым линиям связи.

**Модемы, разновидности по типам линии передачи** – специальные типы модемов для работы в линии электропроводки (power line modems), в системах кабельного телевидения (cable modems) и в беспроводных (радио-) линиях (radio modems).

**Моноканал** – сеть (или среда передачи), в которой используется узкополосная передача.

**Мост (bridge)** – устройство (компьютер), служащее для объединения в одну сеть нескольких сетей разных типов (например, Ethernet и Arcnet), а также для снижения нагрузки в сети.

**Невыделенный сервер** – сервер, который может выполнять помимо функций по обслуживанию сети еще и другие задачи.

**Несимметричное шифрование (в системах с открытыми ключами – public-key systems)** – метод шифрования, при использовании которого каждый пользователь имеет пару ключей – открытый для шифрования и закрытый (секретный) — для дешифрования.

**НСД** – несанкционированный доступ.

**Область коллизий (collision domain)** – см. зона конфликтов.

**Оболочка сетевая** – сетевое программное обеспечение, реализующее связь операционной системы компьютера с сетью.

**Одноранговая сеть (peer-to-peer network)** – сеть, в которой нет выделенных серверов и иерархии среди компьютеров. Все компьютеры могут быть серверами и клиентами.

**Окно коллизий** – величина двойной (круговой) задержки в зоне конфликта (области коллизий).

**Оптоволоконный кабель** – среда передачи информации, представляющая собой стеклянное или пластиковое волокно в оболочке, по которому распространяется световой сигнал.

**ОС** – операционная система.

**Отражение сигнала** – возникновение обратной электромагнитной волны при несогласованных концах электрического кабеля, искажающее сигнал в сети.

**Ошибки передачи** – искажения передаваемой информации в сетях вследствие внешних помех, некачественных кабелей, неисправностей сетевого оборудования, неправильного согласования электрических кабелей, отсутствия гальванической развязки, а также вследствие конфликтов (коллизий) передачи.

**Пакет** – единица информации, передаваемой по сети. Может быть коротким (порядка десятков байт и даже единиц байт), а также длинным (порядка нескольких килобайт). Включает в себя данные (необязательно), адреса и управляющие коды.

**Петля** – замкнутый контур передачи информации в топологии сети.

**Перегрузка (overload)** – ситуация, при которой сеть не может работать при полной нагрузке большую часть времени. В сетях, использующих метод доступа CSMA/CD, перегрузка связана с ростом числа коллизий из-за конкуренции абонентов в сети.

**Переключатель** – то же, что коммутатор.

**Перекрестные помехи** – взаимное влияние (наводки) двух расположенных рядом проводов, искажающее сигналы в этих проводах.

**Перестановка** – один из простейших способов шифрования данных, основанный на изменении расположения символов исходного сообщения. Новая последовательность расположения символов определяется выбранным ключом.

**ПО** – программное обеспечение.

**Повторитель, репитер (repeater)** – устройство для восстановления и усиления сигналов в сети, служащее для увеличения ее длины.

**Подсеть** – логический фрагмент крупной сети. Часто также называется сетью.

**Подстановка** – один из простейших способов шифрования данных, основанный на использовании альтернативного алфавита (или нескольких алфавитов при многоэтапной подстановке) вместо исходного алфавита.

**Показатель использования сети (network utilization)** – отношение числа байтов данных, фактически переданных по сети в течение определенного времени, к максимально возможному для данной сети числу. В сетях, использующих метод доступа CSMA/CD, этот показатель связан, в частности, и с количеством коллизий.

**Порождающий полином** – полином, представляющий собой альтернативную запись числа в двоичной системе счисления, ненулевые коэффициенты которого определяют структуру кодера и декодера циклического кода (структуру обратных связей в сдвиговом регистре).

**Предложенная нагрузка (offered load)** – количество данных или кадров, которое должна передать сеть.

**Пробка** – 32-битная последовательность, передаваемая абонентом сети Ethernet при обнаружении коллизии для усиления конфликта с целью его обнаружения всеми абонентами, участвующими в конфликте.

**Протокол** – набор правил, алгоритм обмена информацией между абонентами сети.

**Рабочая группа** – группа компьютеров сети, совместно использующая ресурсы.

**Рабочая станция** – другое название абонента сети, клиента сети (в противоположность серверу) или специального компьютера, ориентированного на работу в сети (обычно мощного).

**Размножение кадров** – нарушение обмена в сети с топологией шина при наличии в ней петель.

**Реднректор** – программа, обрабатывающая запросы операционной системы и разделяющая их на локальные и удаленные.

**Репитер** – то же, что повторитель.

**Ресурс** – компонент аппаратного или программного обеспечения (например, память, процессор, диск, база данных).

**Ретрансляция** – прием и передача информации без ее изменения, но с восстановлением уровней сигналов и их формы.

**РП** – распределительный пункт.

**Сеанс** – логическое соединение между абонентами сети для обмена информацией; включает в себя передачу нескольких пакетов.

**Сегмент** – часть сети, ограниченная разделяющими устройствами (репитерами, концентраторами, мостами, маршрутизаторами, шлюзами);иногда используется как синоним понятия сети.

**Сервер** – абонент сети, отдающий в сеть свой ресурс и имеющий или не имеющий доступа к ресурсам сети. Также сервером называют специализированный компьютер, предназначенный для работы в сети (имеет быстродействующие диски большого объема, быстрый процессор, большую память).

**Сервер базы данных** – специализированный компьютер, обеспечивающий клиентов сети доступом к базе данных (по сети пересылаются только запросы и запрашиваемая информация).

**Сервер печати** – компьютер, обеспечивающий доступ клиентам сети к совместно используемому принтеру.

**Сетевая операционная система** – программное обеспечение, управляющее работой сети и позволяющее поддерживать связь и совместно использовать ресурсы.

**Сетевой адаптер (он же контроллер, интерфейс, сетевая карта)** – электронная плата, сопрягающая аппаратуру абонента сети и линии связи сети.

**Сетевые атаки** – реализация угроз нарушения целостности систем защиты информации (см. определение термина «защита информации») в

локальной сети, осуществляемая хакерами через внешние подключения этой сети (в том числе через подключения к сети Интернет).

**Сеть на основе сервера** – сеть, в которой имеется четкое разделение абонентов на клиентов и серверы, и в которой есть хотя бы один выделенный сервер.

**Симметричное шифрование** – шифрование, при котором один и тот же ключ используется как для шифрования, так и для дешифрования (расшифрования) данных.

**СКС** – структурированная кабельная система.

**Скремблер/Дескремблер** – одно из устройств модема, служащее для снижения вероятности сбоя синхронизации на приемном конце линии из-за длинной цепочки единиц или нулей в передаваемых данных.

**Среда передачи информации** – электрический кабель (коаксиальный, витая пара), волоконно-оптический кабель, радиоканал, инфракрасный канал — то есть то, что используется в данной сети для связи абонентов; характеризуется стоимостью, удобством подключения, пропускной способностью (то есть предельной скоростью передачи), предельной длиной линии связи (затуханием сигнала с расстоянием на данной частоте), помехоустойчивостью, секретностью передаваемых данных (возможностью подслушивания), требуемой сложностью адаптеров абонентов, а также рядом специфических параметров, менее важных для пользователей сети.

**Станция** – то же, что абонент сети.

**Стек протоколов** – то же, что набор взаимосвязанных протоколов, используемых совместно.

**Топология** – метод соединения, структура связей абонентов сети. Основные топологии – это звезда, шина и кольцо, реже встречаются топологии «цепочка» и «дерево»; топологии различаются требуемой длиной соединительного кабеля, удобством соединения, возможностями подключения дополнительных абонентов, отказоустойчивостью, возможностями управления обменом.

**Трансивер (TRANSmitter-+reCEIVER)** – приемопередатчик сети, служащий для умощнения сигналов или для преобразования физической природы сигналов (например, электрических сигналов в световые и наоборот).

**Узел** – компьютер или другое устройство, подключенное к сети. То же, что абонент.

**Узкополосная передача (baseband)** – способ передачи данных по кабелю без модуляции (каждый бит кодируется определенным сочетанием уровней сигнала).

**ФМ** – фазовая модуляция.

**ЦАП** – цифроаналоговый преобразователь.

**Централизованное управление обменом** – метод управления обменом в сети, при котором один компьютер или одно специальное устройство управляет всем обменом в сети.

**Циклический код (CRC)** – эффективный помехоустойчивый код, позволяющий обнаружить большое число ошибок в принятой информации при малой избыточности и применяемый, в частности, в составе передаваемых по сети пакетов.

**ЧМ** – частотная модуляция.

**Шеннона теорема** – соотношение, связывающее максимально возможную скорость передачи данных по линии связи с ее полосой пропускания и отношением сигнал/шум.

**Шина (bus)** – вид топологии локальной сети, в котором все абоненты параллельно подключены к линейному отрезку кабеля, согласованного на концах.

**Широковещательное сообщение** – сообщение, предназначенное для всех пользователей сети и принимаемое всеми абонентами.

**Широковещательная область (broadcast domain)** – часть сети (или вся сеть), по которой распространяются широковещательные пакеты (сообщения).

**Широкополосная сеть** – сеть, в которой используется модуляция передаваемых сигналов и несколько частотных каналов передачи информации.

**Шифрование** – способ защиты информации от несанкционированного доступа за счет ее обратимого преобразования с использованием одного или нескольких ключей.

**Шлюз (gateway)** – устройство (компьютер), служащее для объединения сетей с принципиально различными протоколами обмена.

**Шум** – временные или фазовые искажения сигнала в сети, которые могут нарушить обмен.

**Эквалайзер** – одно из устройств модема, служащее для компенсации искажений амплитудно-частотной характеристики линии, в которой используется модем.

**Электронная почта** – система передачи сообщений между пользователями сети.

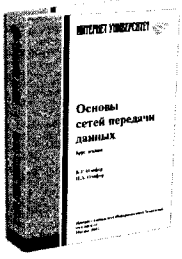
**Электронные конференции** – система публичного обмена новостями и обсуждения новостей в сети по разнообразным темам.

**Эхо-компенсация** – одна из функций модема, состоящая в подавлении собственного сигнала модема, отраженного от противоположного конца линии, при дуплексном обмене.

**Ячеистая сеть** – сеть, имеющая множество маршрутизированных соединений между составляющими ее локальными сетями.

**Ячейка** – 53-байтный пакет данных, используемый в ATM.

## Серия «Основы информационных технологий»




Серия учебных пособий «Основы информационных технологий» открыта в издательстве Интернет-Университета Информационных Технологий в 2003 году и предполагает издание более 100 книг. В настоящее время в ее рамках вышли более 30 учебных пособий по самым разным направлениям информационных и коммуникационных технологий. Авторами этой серии являются известные профессора и преподаватели ведущих российских вузов, а также представители компьютерного бизнеса и академической среды. Ряд учебных курсов создаются при активном участии и поддержке ведущих отечественных и иностранных компаний, а также общественных организаций и коммерческих ассоциаций в области информационных технологий.

## Книги серии

### Сетевые технологии и интернет

1. **Основы Web-технологий**,
   П.Б. Храмцов и др., 2003, 512 с., ISBN 5-9556-0001-9.
2. **Основы сетей передачи данных**,
   В.Г. Олифер, Н.А. Олифер, 2005, 176 с., ISBN 5-9556-0035-3.
3. **Основы локальных сетей**,
   Ю.В. Новиков, С.В. Кондратенко, 2005, 360 с., ISBN 5-9556-0032-9.

### Информационная безопасность

4. **Основы информационной безопасности**, 2-е издание,
   В.А. Галатенко, 2004, 264 с., ISBN 5-9556-0015-9.
5. **Стандарты информационной безопасности**,
   В.А. Галатенко, 2004, 328 с., ISBN 5-9556-0007-8.
6. **Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия**,
   О.Р. Лапонина, 2005, 608 с., ISBN 5-9556-0020-5.

### Информационные системы

7. **Интеграция приложений на основе WebSphere MQ**,
   В.А. Макушкин, Д.С. Володичев, 2005, 336 с., ISBN 5-9556-0031-0.
8. **Проектирование информационных систем**,
   В.И. Грекул и др., 2005, 296 с., ISBN 5-9556-0033-7.

## Архитектура ЭВМ

9. **Основы микропроцессорной техники**, 2-е издание, Ю.В. Новиков, П.К. Скоробогатов, 2004, 440 с., ISBN 5-9556-0016-7.
10. **Основы теории и организации ЭВМ**, В.В. Гуров, В.О. Чуканов, 2005, 280 с., ISBN 5-9556-0040-X.
11. **Архитектуры и топологии многопроцессорных вычислительных систем**, А.В. Богданов, В.В. Корхов, В.В. Мареев, Е.Н. Станкова, 2004, 176 с., ISBN 5-9556-0018-3.
12. **Архитектуры и технологии IBM eServer zSeries**, В.А. Варфоломеев, Э.К. Лецкий, М.И. Шмаров, В.В. Яковлев, 2005, 640 с., ISBN 5-9556-0036-1.

## Программирование

13. **Язык Си и особенности работы с ним** Н.И. Костюкова, Н.А. Калинина, 2005, 208с., ISBN 5-9556-0026-4.
14. **Язык программирования Си++**, 2-е издание, А.Л. Фридман, 2004, 264 с., ISBN 5-9556-0017-5.
15. **Программирование на языке Pascal**, Т.А. Андреева, 2005, 240 с., ISBN 5-9556-0025-6.
16. **Основы программирования на PHP**, Н.В. Савельева, 2005, 264 с., ISBN 5-9556-0026-4.
17. **Основы программирования на языке Пролог**, П.А. Шрайнер, 2005, 176 с., ISBN 5-9556-0034-5.
18. **Программирование на Java**, Н.А. Вязовик, 2003, 592 с., ISBN 5-9556-0006-X.
19. **Основы функционального программирования**, Л.В. Городняя, 2004, 280 с., ISBN 5-9556-0008-6.
20. **Введение в теорию программирования**, С.В. Зыков, 2004, 400 с., ISBN 5-9556-0009-4.
21. **Стили и методы программирования**, Н.Н. Непейвода, 2005, 320 с., ISBN 5-9556-0023-X.
22. **Программирование в стандарте POSIX. Часть 1**, В.А. Галатенко, 2004, 560 с., ISBN 5-9556-0011-6.
23. **Программирование в стандарте POSIX. Часть 2**, В.А. Галатенко, 2005, 384 с., ISBN 5-9556-0021-3.
24. **Основы тестирования программного обеспечения**, В.П. Котляров, 2005, 360 с., ISBN 5-9556-0027-2.
25. **Основы менеджмента программных проектов**, И.Н. Скопин, 2004, 336 с., ISBN 5-9556-0013-2.

**Технологии баз данных**

26. **Основы баз данных**,
    С.Д. Кузнецов, 2005, 488 с., ISBN 5-9556-0028-0.
27. **Основы SQL**,
    Л.Н. Полякова, 2004, 368 с., ISBN 5-9556-0014-0.
28. **Проектирование приложений баз двнных**,
    И.Ю. Баженова, 2005, 320 с., ISBN 5-9556-0014-0.

**Операционные системы**

29. **Основы операционных систем**, 2-е издание,
    В.Е. Карпов, К.А. Коньков, 2004, 536 с., ISBN 5-9556-0044-2.
30. **Операционная система UNIX**,
    Г.В. Курячий, 2004, 320 с., ISBN 5-9556-0019-1.
31. **Операционная система Linux**,
    Г.В. Курячий, К. Маслинский, 2005, 392 с., ISBN 5-9556-0029-9.
32. **Операционная система Solaris**,
    Ф.И. Торчинский, 2005, 472 с., ISBN 5-9556-0022-1.

**Интеллектуальные системы и робототехника**

33. **Интеллектуальные робототехнические системы**,
    В.Л. Афонин, В.А. Макушкин, 2005, 208 с., ISBN 5-9556-0024-8.

---

**Серия «Архитектор информационных систем»**

34. **Архитектура и стратегия. «Инь» и «янь» информационных технологий предприятия**,
    А. Данилин, А. Слюсаренко, 2005, 504 с., ISBN 5-9556-0045-0.

---

**Серия «Современные офисные технологии»**

35. **Я могу работать в современном офисе**,
    А. Прохоров, 2005, 264 с., ISBN 5-9556-0046-9.

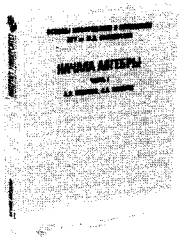
---

**Дополнительная литература**

36. **Объектно-ориентированное конструирование программных систем**,
    Бертран Мейер, 2005, 1232 с., ISBN 5-7502-0255-0.
37. **Готовы ли Вы к войне за клиента? Стратегия управления взаимоотношениями с клиентами (CRM)**,
    П. Черкашин, 2004, 384 с., ISBN 5-9556-0016-7.

*продолжение следует*

## «Основы информатики и математики»



Новая серия учебных пособий по информатике и ее математическим основам открыта в 2005 году с целью современного изложения широкого спектра направлений информатики на базе соответствующих разделов математических курсов, а также примыкающих вопросов, связанных с информационными технологиями.

Особое внимание предполагается уделять возможности использования материалов публикуемых пособий в преподавании информатики и ее математических основ для непрофильных специальностей. Редакционная коллегия также надеется представить вниманию читателей широкую гамму практикумов по информатике и ее математическим основам, реализующих основные алгоритмы и идеи теоретической информатики.

Выпуск серии начат при поддержке корпорации Microsoft в рамках междисциплинарного научного проекта МГУ имени М.В. Ломоносова.

## Книги серии

1. **Преподавание информатики и математических основ информатики**, под. ред. А.В. Михалева, 2005, 144 с., ISBN 5-9556-0037-X.
2. **Начала алгебры, часть I**, А.В. Михалев, А.А. Михалев, 2005, 272 с., ISBN 5-9556-0038-8.
3. **Основы программирования**, В.В. Борисенко, 2005, 328 с., ISBN 5-9556-0039-6.
4. **Работа с текстовой информацией. Microsoft Office Word 2003**, О.Б. Калугина, В.С. Люцарев, 2005, 160 с., ISBN 5-9556-0040-0.

*продолжение следует*

**Серия «Основы информационных технологий»**

**Ю.В. Новиков, С.В. Кондратенко**

**Основы локальных сетей**
**Курс лекций. Учебное пособие**

Литературный редактор И. Черкесова
Корректор Ю. Голомазова
Компьютерная верстка Ю. Волшмид
Обложка М. Автономова

Формат 60x90 $^{1}/_{16}$. Усл. печ. л. 22,5. Бумага офсетная.
Подписано в печать 25.06.2005. Тираж 2000 экз. Заказ № 5409.

Санитарно-эпидемиологическое заключение о соответствии
санитарным правилам №77.99.02.953.Д.006052.08.03 от 12.08.2003

ООО «ИНТУИТ.ру»
Интернет-Университет Информационных Технологий, www.intuit.ru
123056, Москва, Электрический пер., 8, стр. 3.

Отпечатано с готовых диапозитивов на ФГУП ордена «Знак Почета»
Смоленская областная типография им. В.И.Смирнова.
Адрес: 214000, г. Смоленск, проспект им. Ю. Гагарина, д. 2.