

Санкт-Петербургский государственный морской технический университет

**кафедра Судовой автоматики и измерений**

# **Сети ЭВМ и их защита**

(PDF-версия на <http://irodov.nm.ru/other/files.htm>)

Учебное пособие

Доцент Галушин Сергей Яковлевич

Санкт – Петербург  
2000

## Оглавление

1. Типы компьютерных сетей .....	4
1.1. Назначение компьютерной сети .....	4
1.2. Основные типы сетей .....	4
1.2.1. Одноранговые сети .....	5
1.2.2. Сети на основе сервера .....	6
1.2.3. Преимущества сетей на базе сервера .....	8
1.3. Компоновка сети .....	9
1.4. Базовые топологии .....	9
1.4.1. Шина .....	10
1.4.2. Звезда .....	12
1.4.3. Кольцо .....	12
1.5. Концентраторы .....	13
1.6. Комбинированные топологии .....	14
1.7. Выбор топологии .....	15
2. Сетевые кабели .....	16
2.1. Коаксиальный кабель .....	16
2.1.1. Тонкий коаксиальный кабель .....	17
2.1.2. Толстый коаксиальный кабель .....	18
2.1.3. Компоненты кабельной системы на базе коаксиальных кабелей .....	18
2.2. Витая пара .....	19
2.2.1. Неэкранированная витая пара .....	19
2.2.2. Экранированная витая пара .....	20
2.2.3. Компоненты кабельной системы на базе витой пары .....	20
2.3. Оптоволоконный кабель .....	21
2.4. Передача сигналов .....	22
2.5. Сравнение кабелей .....	23
2.6. Беспроводные сети .....	24
2.6.1. Локальные беспроводные сети .....	25
2.6.2. Расширенные беспроводные сети .....	27
2.6.3. Мобильные сети .....	27
3. Сетевые адаптеры .....	28
3.1. Назначение сетевого адаптера .....	28
3.2. Параметры конфигурации сетевого адаптера .....	30
4. Сетевые модели OSI и IEEE Project 802 .....	34
4.1. Модель OSI .....	34
4.1.1. Взаимодействие уровней модели OSI .....	35
4.2. IEEE Project 802 .....	38
4.3. Драйверы .....	39
4.4. Сетевые протоколы .....	40
5. Сетевая архитектура Ethernet .....	42
5.1. Стандарты IEEE на 10 Мбит/с .....	43
5.2. Стандарты IEEE на 100 Мбит/с .....	46
6. Аппаратура для создания больших сетей .....	49
6.1. Репитеры .....	49
6.2. Мосты .....	51
6.3. Различия между мостами и репитерами .....	53
6.4. Маршрутизаторы .....	54
6.5. Различия между мостами и маршрутизаторами .....	57
6.6. Мосты-маршрутизаторы .....	58

6.7. Шлюзы.....	59
7. Стандарты передачи данных в глобальных вычислительных сетях.....	61
7.1. Аналоговая связь.....	61
7.2. Цифровая связь.....	63
7.2.1. Сети с коммутацией пакетов.....	65
7.2.2. Беспроводной канал связи.....	66
8. Передовые технологии связи в глобальных вычислительных сетях.....	66
8.1. X.25.....	67
8.2. Frame relay.....	67
8.3. Асинхронный режим передачи (ATM).....	68
8.4. Цифровая сеть комплексных услуг (ISDN).....	70
8.5. Оптический интерфейс передачи данных (FDDI).....	71
8.6. Синхронная оптическая сеть (SONET).....	73
8.7. Коммутируемая мультимегабитная цифровая служба (SMDS).....	74
9. Аппаратные мероприятия по защите данных.....	75
9.1. Тестирование и хранение.....	77
9.2. Источник бесперебойного питания.....	78
9.3. Отказоустойчивые системы.....	79
9.3.1. Избыточные массивы недорогих дисков.....	79
9.3.2. Замена секторов.....	80
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ.....	82

# 1. Типы компьютерных сетей

## 1.1. Назначение компьютерной сети

Самая простая сеть (network) состоит как минимум из двух компьютеров, соединенных друг с другом кабелем. Это позволяет им использовать данные совместно. Все сети (независимо от сложности) основываются именно на этом простом принципе. Хотя идея соединения компьютеров с помощью кабеля не кажется нам особо выдающейся, в свое время она явилась значительным достижением в области коммуникаций.

Рождение компьютерных сетей было вызвано практической потребностью — иметь возможность для совместного использования данных. Персональный компьютер — прекрасный инструмент для создания документа, подготовки таблиц, графических данных и других видов информации, но при этом Вы не можете быстро поделиться своей информацией с другими. Когда не было сетей, приходилось распечатывать каждый документ, чтобы другие пользователи могли работать с ним, или в лучшем случае — копировать информацию на дискеты. Одновременная обработка документа несколькими пользователями исключалась. Подобная схема работы называется работой в автономной среде. Сетью называется группа соединенных компьютеров и других устройств. А концепция соединенных и совместно использующих ресурсы компьютеров носит название сетевого взаимодействия.

Основное назначение компьютерных сетей — совместное использование ресурсов и осуществление интерактивной связи как внутри одной фирмы, так и за ее пределами. Ресурсы (resources) — это данные, приложения и периферийные устройства, такие, как внешний дисковод, принтер, мышь, модем или джойстик. Понятие интерактивной связи компьютеров подразумевает обмен сообщениями в реальном режиме времени /1,2/.

До появления компьютерных сетей каждый пользователь должен был иметь свой принтер, плоттер и другие периферийные устройства. Чтобы совместно использовать принтер, существовал единственный способ — пересечься за компьютер, подключенный к этому принтеру. Теперь сети позволяют целому ряду пользователей одновременно "владеть" данными и периферийными устройствами. Если нескольким пользователям надо распечатать документ, все они могут обратиться к сетевому принтеру.

## 1.2. Основные типы сетей

Несмотря на определенные сходства, сети разделяются на два типа: одноранговые (peer-to-peer) и на основе сервера (server based) /3/.

Различия между одноранговыми сетями и сетями на основе сервера имеют принципиальное значение, поскольку определяют разные возможности этих сетей. Выбор типа сети зависит от многих факторов:

- размера предприятия;
- необходимого уровня безопасности;
- вида бизнеса;
- уровня доступности административной поддержки;
- объема сетевого трафика;
- потребностей сетевых пользователей;
- финансовых затрат.

### 1.2.1. Одноранговые сети

В одноранговой сети все компьютеры равноправны: нет иерархии среди компьютеров и нет выделенного (dedicated) сервера (рис. 1.1). Как правило, каждый компьютер функционирует и как клиент, и как сервер; иначе говоря, нет отдельного компьютера, ответственного за администрирование всей сети. Все пользователи самостоятельно решают, какие данные на своем компьютере сделать общедоступными по сети.

Одноранговая сеть

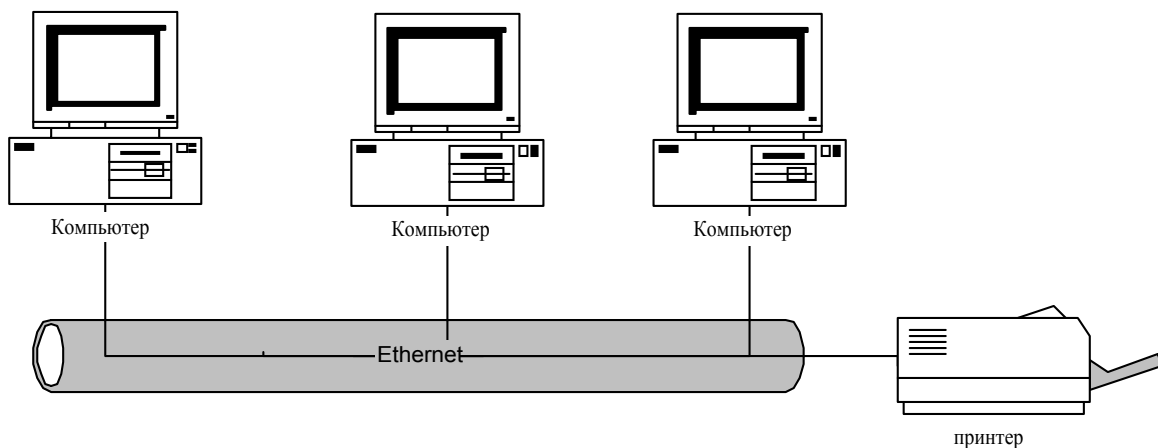


Рис. 1.1

Одноранговые сети называют также рабочими группами. Рабочая группа — это небольшой коллектив, поэтому в одноранговых сетях чаще всего не более 10 компьютеров.

Одноранговые сети относительно просты. Поскольку каждый компьютер является одновременно и клиентом, и сервером, нет необходимости в мощном центральном сервере или в других компонентах, обязательных для более сложных сетей. Одноранговые сети обычно дешевле сетей на основе сервера, но требуют более мощных (и более дорогих) компьютеров.

В одноранговой сети требования к производительности и к уровню защиты для сетевого программного обеспечения, как правило, ниже, чем в сетях с выделенным сервером. Выделенные серверы функционируют исключительно в качестве серверов, но не клиентов или рабочих станций (workstation). О них мы еще поговорим подробнее на этом занятии, но чуть позже.

В такие операционные системы, как Microsoft Windows NT Workstation, Microsoft Windows for Workgroups и Microsoft Windows 95/98, встроена поддержка одноранговых сетей. Поэтому, чтобы установить одноранговую сеть, дополнительного программного обеспечения не требуется.

Одноранговая сеть характеризуется рядом стандартных решений: компьютеры расположены на рабочих столах пользователей; пользователи сами выступают в роли администраторов и обеспечивают защиту информации; для объединения компьютеров в сеть применяется простая кабельная система.

Одноранговая сеть вполне подходит там, где:

- количество пользователей не превышает 10 человек;
- пользователи расположены компактно;

- вопросы защиты данных не критичны;
- в обозримом будущем не ожидается значительного расширения фирмы и, следовательно, сети.

Если эти условия выполняются, то, скорее всего, выбор одноранговой сети будет правильным (чем сети на основе сервера).

Сетевое администрирование (administration) решает ряд задач, в том числе: управление работой пользователей и защитой данных; обеспечение доступа к ресурсам; поддержка приложений и данных; установка и модернизация прикладного программного обеспечения.

В типичной одноранговой сети системный администратор, контролирующий всю сеть, не выделяется. Каждый пользователь сам администрирует свой компьютер. Все пользователи могут "поделиться" своими ресурсами с другими. К совместно используемым ресурсам относятся каталоги, принтеры, факс-модемы и т.п.

В одноранговой сети каждый компьютер должен:

- большую часть своих вычислительных ресурсов предоставлять локальному пользователю (сидящему за этим компьютером);
- для поддержки доступа к ресурсам удаленного пользователя (обращающегося к серверу по сети) подключать дополнительные вычислительные ресурсы.

Сеть на основе сервера требует более мощных серверов, поскольку они должны обрабатывать запросы всех клиентов сети.

Защита подразумевает установку пароля на разделяемый ресурс, например на каталог. Централизованно управлять защитой в одноранговой сети очень сложно, так как каждый пользователь устанавливает ее самостоятельно, да и "общие" ресурсы могут находиться на всех компьютерах, а не только на центральном сервере. Такая ситуация представляет серьезную угрозу для всей сети, кроме того, некоторые пользователи могут вообще не установить защиту. Если вопросы конфиденциальности являются принципиальными, рекомендуется выбрать сеть на основе сервера.

Поскольку в одноранговой сети каждый компьютер функционирует и как клиент, и как сервер, пользователи должны обладать достаточным уровнем знаний, чтобы работать и как пользователи, и как администраторы своего компьютера.

## **1.2.2. Сети на основе сервера**

Если к сети подключено более 10 пользователей, то одноранговая сеть, где компьютеры выступают в роли и клиентов, и серверов, может оказаться недостаточно производительной. Поэтому большинство сетей использует выделенные серверы. Выделенным - называется такой сервер, который функционирует только как сервер (исключая функции клиента или рабочей станции). Они специально оптимизированы для быстрой обработки запросов от сетевых клиентов и для управления защитой файлов и каталогов. Сети на основе сервера стали промышленным стандартом, и именно они будут использоваться в качестве примера (рис.1.2).

С увеличением размеров сети и объема сетевого трафика необходимо увеличивать количество серверов. Распределение задач среди нескольких серверов гарантирует, что каждая задача будет выполняться самым эффективным способом из всех возможных.

Круг задач, которые должны выполнять серверы, многообразен и сложен. Чтобы приспособиться к возрастающим потребностям пользователей, серверы в больших сетях стали специализированными (specialized). Например, в сети Windows NT существуют различные типы серверов (рис.1.3):

## Сеть на основе сервера

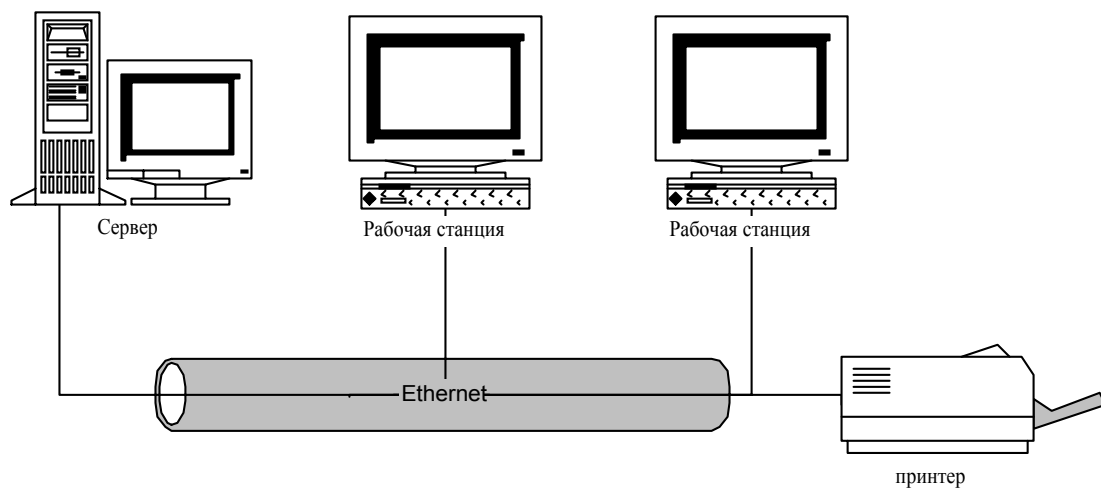


Рис. 1.2

**ФАЙЛ-СЕРВЕРЫ И ПРИНТ-СЕРВЕРЫ.** Они управляют доступом пользователей соответственно к файлам и принтерам. Например, чтобы работать с текстовым процессором, Вы прежде всего должны запустить его на своем компьютере. Документ текстового процессора, хранящийся на файл-сервере, загружается в память Вашего компьютера, и, таким образом, Вы можете работать с этим документом на своем компьютере. Другими словами, файл-сервер предназначен для хранения файлов и данных.

**СЕРВЕРЫ ПРИЛОЖЕНИЙ.** На серверах приложений выполняются прикладные части клиент-серверных приложений, а также находятся данные, доступные клиентам. Например, чтобы упростить извлечение данных, серверы хранят большие объемы информации в структурированном виде. Эти серверы отличаются от файл- и принт-серверов. В последних файл или данные целиком копируются на запрашивающий компьютер. А в сервере приложений на запрашивающий компьютер пересылаются только результаты запроса. Приложение-клиент на удаленном компьютере получает доступ к данным, хранимым на сервере приложений. Однако вместо всей базы данных на Ваш компьютер с сервера загружаются только результаты запроса. Например, Вы можете получить список работников, родившихся в ноябре.

**ПОЧТОВЫЕ СЕРВЕРЫ.** Они управляют передачей электронных сообщений между пользователями сети.

**ФАКС-СЕРВЕРЫ.** Факс-серверы управляют потоком входящих и исходящих факсимильных сообщений через один или несколько факс-модемов.

**КОММУНИКАЦИОННЫЕ СЕРВЕРЫ.** Коммуникационные серверы управляют потоком данных и почтовых сообщений между этой сетью и другими сетями, мейнфреймами или удаленными пользователями через модем и телефонную линию. Служба каталогов предназначена для поиска, хранения и защиты информации в сети Windows NT Server объединяет компьютеры в логические группы — домены (domain), - система защиты которых наделяет пользователей различными правами доступа к любому сетевому ресурсу.

В расширенной сети использование серверов разных типов приобретает особую актуальность. Необходимо поэтому учитывать все возможные нюансы, которые могут проявиться при разрастании сети, с тем, чтобы изменение роли определенного сервера в дальнейшем не отразилось на работе всей сети.

### Специализированные серверы

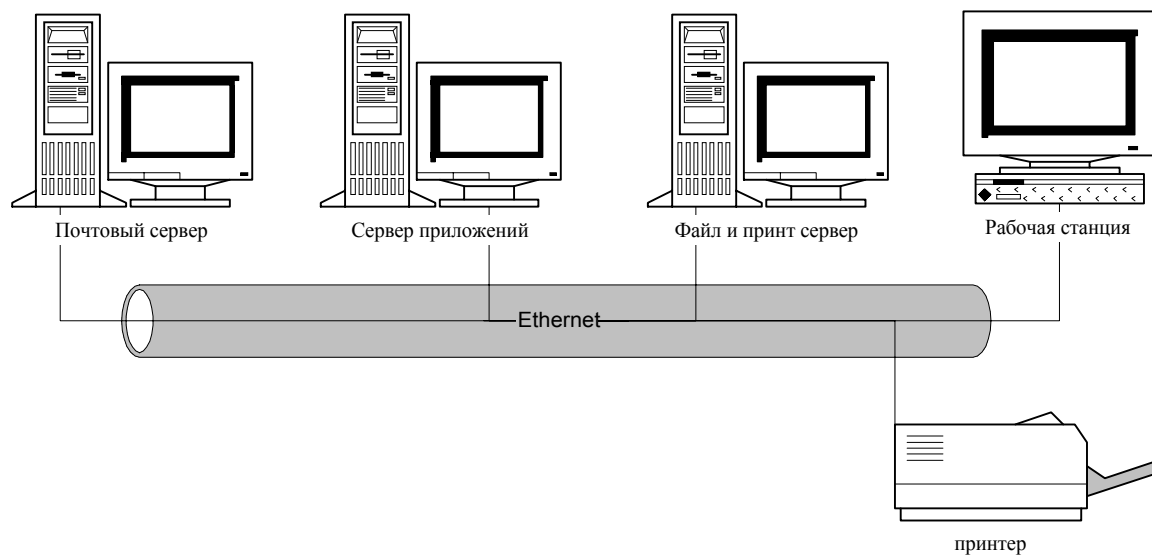


Рис.1.3

Сетевой сервер и операционная система работают как единое целое. Без операционной системы даже самый мощный сервер представляет собой лишь грудку железа. А операционная система позволяет реализовать потенциал аппаратных ресурсов сервера. Некоторые системы, например Microsoft Windows NT Server, были созданы специально для того, чтобы использовать преимущества наиболее передовых серверных технологий. Так, Windows NT Server реализует следующие возможности сервера (таблица 1).

Возможности Windows NT 4

Таблица 1

Категория	Свойства
Симметричная многопроцессорная обработка (SMP)	Системные и прикладные задачи распределяются между всеми доступными процессорами
Поддержка множества платформ	Быстрые процессоры, такие, как Intel* 386/486 и Pentium", MIPS" R4000 RISC и Digital Alpha AXP
Длина имени файла/каталога	255 символов
Размер файла	16 эб (эксабайтов)
Размер раздела жесткого диска	16 эб

### 1.2.3. Преимущества сетей на базе сервера

Сервер спроектирован так, чтобы предоставлять доступ к множеству файлов и принтеров, обеспечивая при этом высокую производительность и защиту. Администрирование и управление доступом к данным осуществляется централизованно. Ресурсы, как правило, расположены также централизованно, что облегчает их поиск и поддержку. Например, в системе Windows NT Server разделение каталогов осуществляется через File Manager

Основным аргументом при выборе сети на основе сервера является, как правило, защита данных. В таких сетях, например, как Windows NT Server, проблемами



безопасности может заниматься один администратор: он формирует политику безопасности (security policy) и применяет ее в отношении каждого пользователя сети. Поскольку жизненно важная информация расположена централизованно, т.е. сосредоточена на одном или нескольких серверах, нетрудно обеспечить ее регулярное резервное копирование (backup).

Благодаря избыточным системам данные на любом сервере могут дублироваться в реальном времени, поэтому в случае повреждения основной области хранения данных информация не будет потеряна — легко воспользоваться резервной копией. Сети на основе сервера способны поддерживать тысячи пользователей. Сетями такого размера, будь они одноранговыми, было бы невозможно управлять.

Так как компьютер пользователя не выполняет функций сервера, требования к его характеристикам зависят от потребностей самого пользователя. Типичный компьютер-клиент имеет, по крайней мере, процессор Pentium или Pentium 2 (или совместимые с ними) и от 16 до 128 Мб оперативной памяти.

### 1.3. Компонировка сети

Термин "топология", или "топология сети", характеризует физическое расположение компьютеров, кабелей и других компонентов сети. Топология — это стандартный термин, который используется профессионалами при описании основной к сети. Кроме термина "топология", для описания физической компоновки ют также следующие:

- физическое расположение;
- компоновка;
- диаграмма;
- карта.

Топология сети обуславливает ее характеристики. В частности, выбор иной топологии влияет:

- на состав необходимого сетевого оборудования;
- характеристики сетевого оборудования;
- возможности расширения сети;
- способ управления сетью.

Чтобы совместно использовать ресурсы или выполнять другие сетевые задачи компьютеры должны быть подключены друг к другу. Для этой цели в большинстве сетей применяется кабель.

Однако просто подключить компьютер к кабелю, соединяющему другие компьютеры, не достаточно. Различные типы кабелей в сочетании с различными сетевыми платами, сетевыми операционными системами и другими компонентами требуют и различного взаимного расположения компьютеров. Каждая топология сети налагает ряд условий. Например, она может диктовать не только тип кабеля, но и способ его прокладки. Топология может также определять способ взаимодействия компьютеров в сети. Различным видам топологий соответствуют различные методы взаимодействия, и эти методы оказывают большое влияние на сеть.

### 1.4. Базовые топологии

Все сети строятся на основе трех базовых топологий:

- шина (bus);
- звезда (star);
- кольцо (ring).

Если компьютеры подключены вдоль одного кабеля [сегмента (segment)], топология называется шиной. В том случае, когда компьютеры подключены к сегментам кабеля, исходящим из одной точки, или концентратора, топология называется звездой. Если кабель, к которому подключены компьютеры, замкнут в кольцо, такая топология носит название кольца. Хотя сами по себе базовые топологии несложны, в реальности часто встречаются довольно сложные комбинации, объединяющие свойства нескольких топологий.

### 1.4.1. Шина

Топологию "шина" часто называют "линейной шиной" (linear bus). Данная топология относится к наиболее простым и широко распространенным топологиям. В ней используется один кабель, именуемый магистралью или сегментом, вдоль которого подключены все компьютеры сети (рис.1.4).

Сеть с топологией "шина".

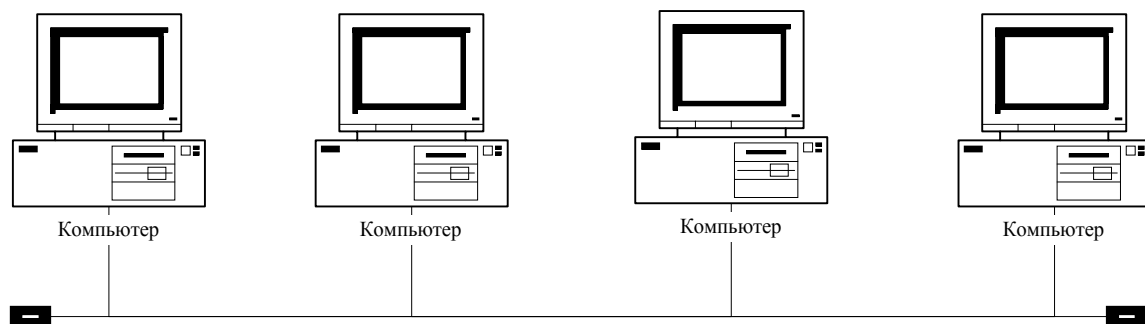


Рис. 1.4

В сети с топологией "шина" компьютеры адресуют данные конкретному компьютеру, передавая их по кабелю в виде электрических сигналов. Чтобы понять процесс взаимодействия компьютеров по шине, необходимо определить следующие понятия:

- передача сигнала;
- отражение сигнала;
- терминатор.

Данные в виде электрических сигналов передаются всем компьютерам сети, однако информацию принимает только тот, адрес которого соответствует адресу получателя, зашифрованному в этих сигналах. Причем в каждый момент времени только один компьютер может вести передачу.

Так как данные в сеть передаются лишь одним компьютером, ее производительность зависит от количества компьютеров, подключенных к шине. Чем их больше, т.е. чем больше компьютеров, ожидающих передачи данных, тем медленнее сеть. Однако вывести прямую зависимость между пропускной способностью сети и количеством компьютеров в ней нельзя. Ибо, кроме числа компьютеров, на быстродействие сети влияет множество факторов, в том числе:

- характеристики аппаратного обеспечения компьютеров в сети;
- частота, с которой компьютеры передают данные;
- тип работающих сетевых приложений;
- тип сетевого кабеля;

- расстояние между компьютерами в сети.

Шина — пассивная топология. Это значит, что компьютеры только "слушают" передаваемые по сети данные, но не перемещают их от отправителя к получателю. Поэтому, если один из компьютеров выйдет из строя, это не скажется на работе остальных. В активных топологиях компьютеры регенерируют сигналы и передают их по сети.

Данные, или электрические сигналы, распространяются по всей сети — от одного конца кабеля к другому. Если не предпринимать никаких специальных действий, сигнал, достигая конца кабеля, будет отражаться и не позволит другим компьютерам осуществлять передачу. Поэтому, после того как данные достигнут адресата, электрические сигналы необходимо погасить.

Чтобы предотвратить отражение электрических сигналов, на каждом конце кабеля устанавливают терминаторы (terminators), поглощающие эти сигналы. Все концы сетевого кабеля должны быть к чему-нибудь подключены, например, к компьютеру или к баррел-коннектору — для увеличения длины кабеля. К любому свободному — неподключенному — концу кабеля должен быть подсоединен терминатор, чтобы предотвратить отражение электрических сигналов.

Разрыв сетевого кабеля происходит при его физическом разрыве или отсоединении одного из его концов. Возможна также ситуация, когда на одном или нескольких концах кабеля отсутствуют терминаторы, что приводит к отражению электрических сигналов в кабеле и прекращению функционирования сети. Сеть "падает". Сами по себе компьютеры в сети остаются полностью работоспособными, но до тех пор, пока сегмент разорван, они не могут взаимодействовать друг с другом.

Увеличение участка, охватываемого сетью, вызывает необходимость ее расширения. сети с топологией "шина" кабель обычно удлиняется двумя способами. Для соединения двух отрезков кабеля можно воспользоваться баррел-коннектором (barrel connector). Но злоупотреблять ими не стоит, так как сигнал при этом ослабевает. Лучше купить один длинный кабель, чем соединять несколько коротких отрезков. При большом количестве "стыковок" нередко происходит искажение сигнала.

Для соединения двух отрезков кабеля служит репитер (repeater) (рис.1.5). В отличие от коннектора, он усиливает сигнал перед передачей его в следующий сегмент. Поэтому предпочтительнее использовать репитер, чем баррел-коннектор или даже один длинный кабель: сигналы на большие расстояния пойдут без искажений.

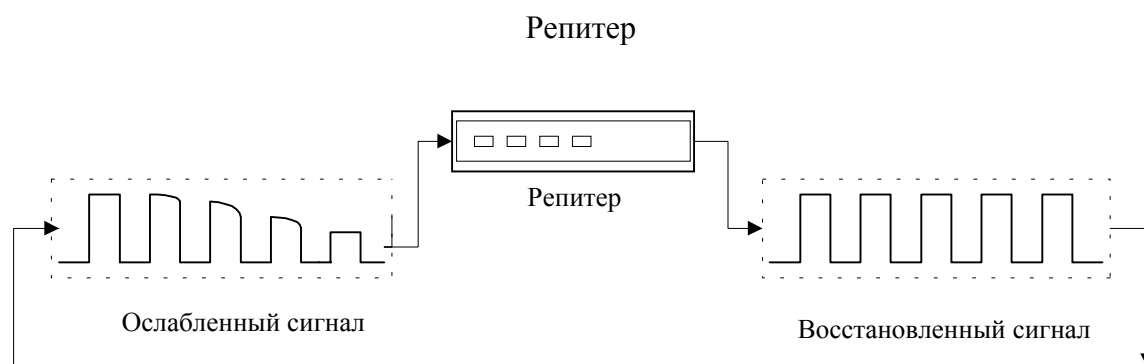
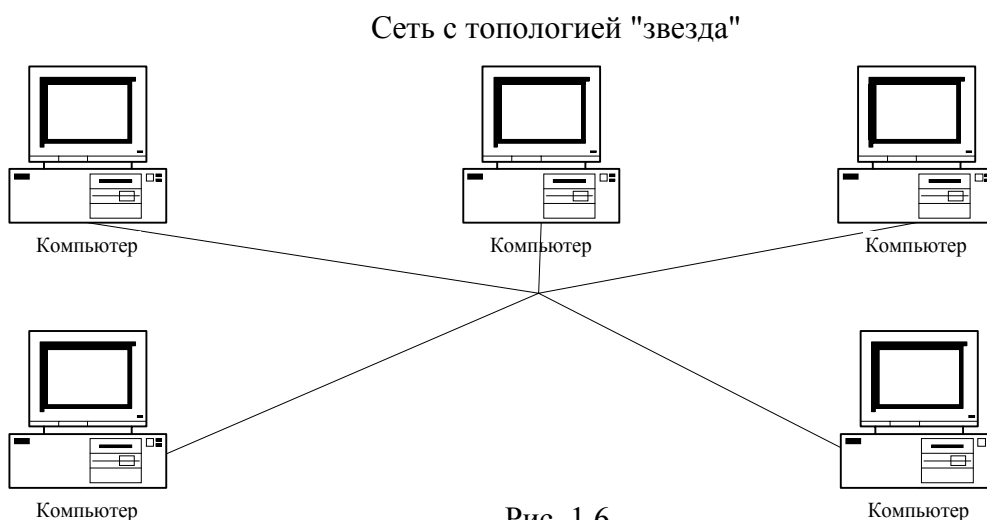


Рис. 1.5

### 1.4.2. Звезда

При топологии "звезда" все компьютеры с помощью сегментов кабеля подключаются к центральному компоненту, именуемому концентратором (hub) (рис.1.6). Сигналы от передающего компьютера поступают через концентратор ко всем остальным. Эта топология возникла на заре вычислительной техники, когда компьютеры были подключены к центральному, главному, компьютеру.

В сетях с топологией "звезда" подключение кабеля и управление конфигурацией сети централизованны. Но есть и недостаток: так как все компьютеры подключены к центральной точке, для больших сетей значительно увеличивается расход кабеля. К тому же, если центральный компонент выйдет из строя, нарушится работа всей сети. А если выйдет из строя только один компьютер (или кабель, соединяющий его с концентратором), то лишь этот компьютер не сможет передавать или принимать данные по сети. На остальные компьютеры в сети это не повлияет.



### 1.4.3. Кольцо

При топологии "кольцо" компьютеры подключаются к кабелю, замкнутому в кольцо. Поэтому у кабеля просто не может быть свободного конца, к которому надо подключать терминатор. Сигналы передаются по кольцу в одном направлении и проходят через каждый компьютер. В отличие от пассивной топологии "шина", здесь каждый компьютер выступает в роли репитера, усиливая сигналы и передавая их следующему компьютеру. Поэтому, если выйдет из строя один компьютер, прекращает функционировать вся сеть.

Один из принципов передачи данных в кольцевой сети носит название передачи маркера. Суть его такова. Маркер последовательно, от одного компьютера к другому, передается до тех пор, пока его не получит тот, который "хочет" передать данные. Передающий компьютер изменяет маркер, помещает электронный адрес в данные и посылает их по кольцу. Данные проходят через каждый компьютер, пока не окажутся у того, чей адрес совпадает с адресом получателя, указанным в данных. После этого принимающий компьютер посылает передающему сообщение, где подтверждает факт приема данных. Получив подтверждение, передающий компьютер создает новый маркер и возвращает его в сеть (рис.1.7). На первый взгляд кажется, что передача маркера отнимает много времени, однако на самом деле маркер передвигается практически со скоростью света. В кольце диаметром 200 м маркер может циркулировать с частотой 10 000 оборотов в секунду.

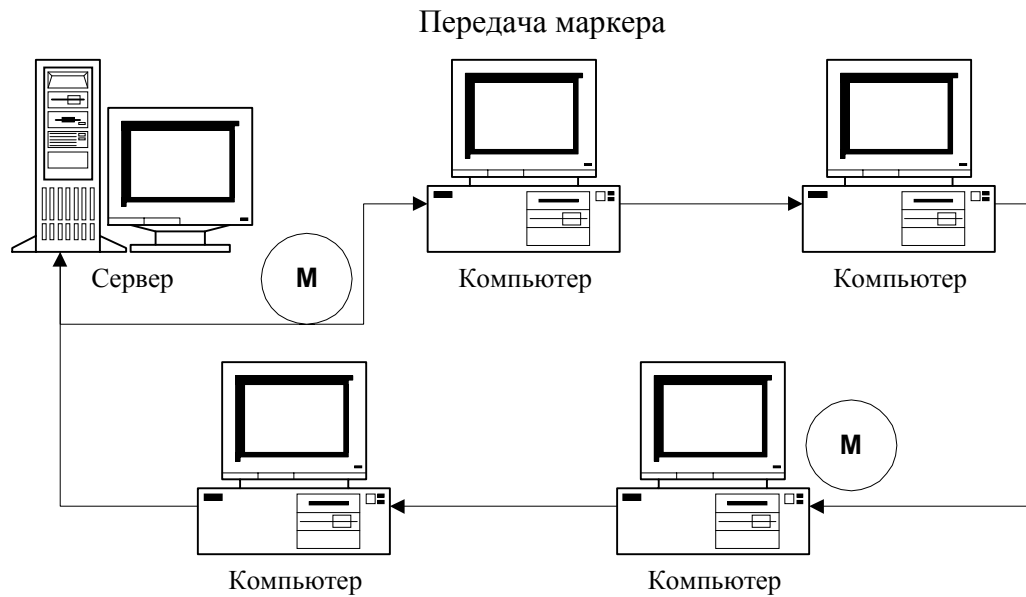


Рис. 1.7

## 1.5. Концентраторы

В настоящее время одним из стандартных компонентов сетей становится концентратор (рис.1.8). А в сетях с топологией "звезда" он служит центральным узлом.

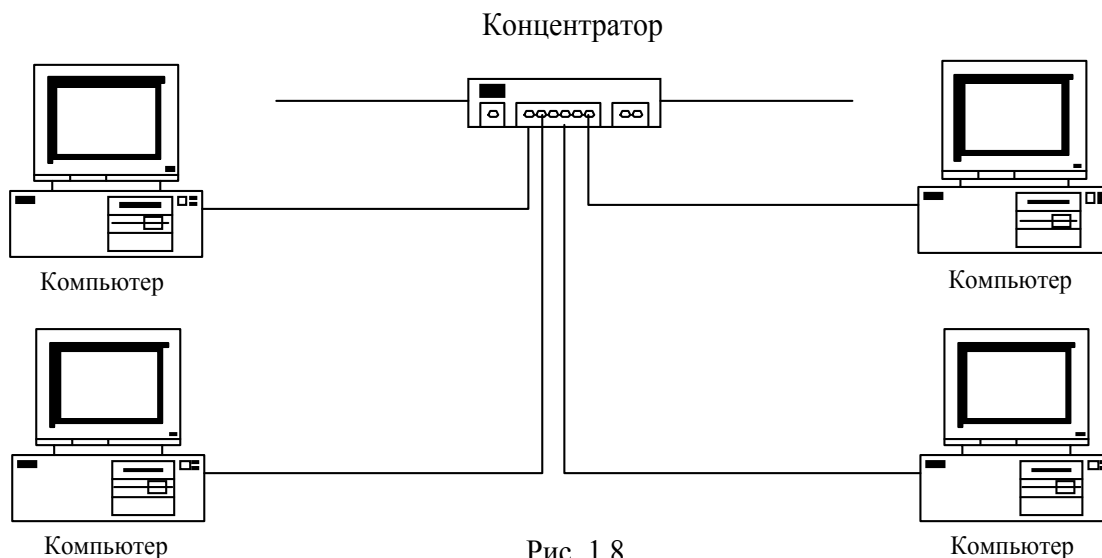


Рис. 1.8

Среди концентраторов выделяются активные (active) и пассивные (passive). Активные концентраторы регенерируют и передают сигналы так же, как это делают репитеры. Иногда их называют многопортовыми репитерами — они имеют от 5 до 24 портов для подключения компьютеров.

Некоторые типы концентраторов являются пассивными, например монтажные панели или коммутирующие блоки. Они просто пропускают через себя сигнал как узлы коммутации, не усиливая и не восстанавливая его. Пассивные концентраторы не надо подключать к источнику питания.

Гибридными (hybrid) называются концентраторы, к которым можно подключать кабели различных типов. Сети, построенные на концентраторах, легко расширить, если подключить дополнительные концентраторы.

## Выводы

Использование концентраторов дает ряд преимуществ. Разрыв кабеля в сети с обычной топологией "линейная шина" приведет к "падению" всей сети. Между тем разрыв кабеля, подключенного к концентратору, нарушает работу только данного сегмента. Остальные сегменты останутся работоспособными.

К числу других преимуществ использования концентраторов относятся:

1. простота изменения или расширения сети: достаточно просто подключить еще один компьютер или концентратор;
2. использование различных портов для подключения кабелей разных типов;
3. централизованный контроль за работой сети и сетевым трафиком: во многих сетях v активные концентраторы наделены диагностическими возможностями, позволяющими определить работоспособность соединения.

## 1.6. Комбинированные топологии

В настоящее время часто используются топологии, которые комбинируют компоновку сети по принципу шины, звезды и кольца.

### Звезда-шина

Звезда-шина (star-bus) — это комбинация топологий "шина" и "звезда". Чаще всего это выглядит так: несколько сетей с топологией "звезда" объединяются при помощи магистральной линейной шины (рис.1.9). В этом случае выход из строя одного компьютера не оказывает никакого влияния на сеть — остальные компьютеры по-прежнему взаимодействуют друг с другом. А выход из строя концентратора повлечет за собой остановку подключенных к нему компьютеров и концентраторов.

Сеть с топологией "звезда-шина"

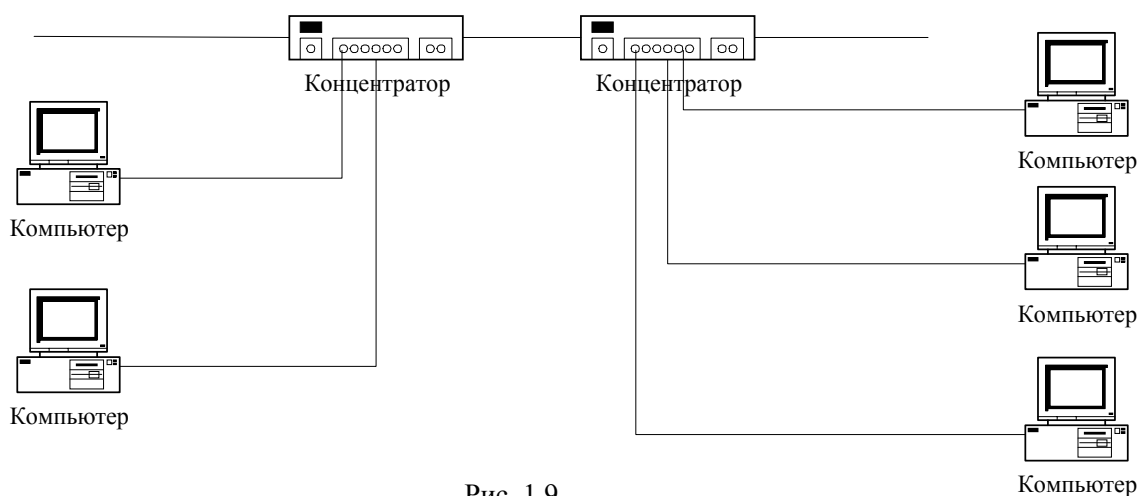


Рис. 1.9

## Звезда-кольцо

Звезда-кольцо (star-ring) кажется несколько похожей на звезду-шину. И в той, и в другой топологии компьютеры подключены к концентратору, который фактически и формирует кольцо или шину. Отличие в том, что концентраторы в звезде-шине соединены магистральной линейной шиной, а в звезде-кольце на основе главного концентратора они образуют звезду (рис.1.10).

Сеть с топологией "звезда-кольцо"

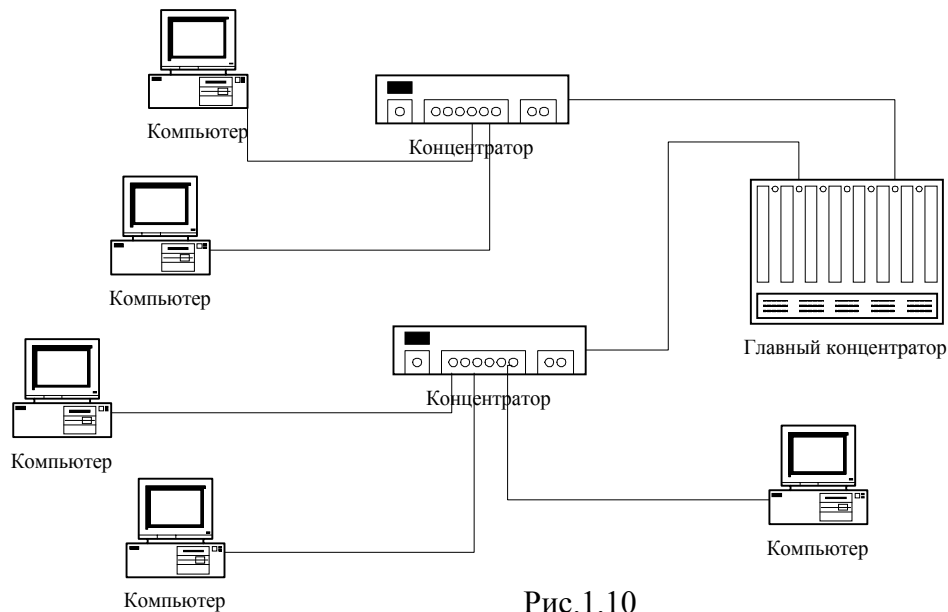


Рис.1.10

## 1.7. Выбор топологии

Существует множество факторов, которые необходимо учитывать при выборе наиболее подходящей к данной ситуации топологии. В таблице 2 приведены обобщенные данные по всем топологиям сетей.

Особенности различных топологий сетей

Таблица 2

Топология	Преимущества	Недостатки
Шина	Экономный расход кабеля. Сравнительно недорогая и несложная в использовании среда передачи. Простота, надежность. Легко расширяется.	При значительных объемах трафика уменьшается пропускная способность сети. Трудно локализовать проблемы. Выход из строя кабеля останавливает работу многих пользователей.
Кольцо	Все компьютеры имеют равный доступ. Количество пользователей не оказывает сколько-нибудь значительного влияния на производительность.	Выход из строя одного компьютера может вывести из строя всю сеть. Трудно локализовать проблемы. Изменение конфигурации сети требует остановки работы всей сети.
Звезда	Легко модифицировать сеть, добавляя новые компьютеры. Централизованный контроль и управление. Выход из строя одного компьютера не влияет на работоспособность сети.	Выход из строя центрального узла выводит из строя всю сеть.

Выбор топологии локальной сети зависит от конкретных условий, при которых учитывается количество пользователей, тип решаемых задач, условия помещения, трафик между отдельными группами пользователей.

## 2. Сетевые кабели

На сегодняшний день подавляющая часть компьютерных сетей использует для соединения провода или кабели. Они выступают в качестве среды передачи сигналов между компьютерами. Существуют различные типы кабелей, которые удовлетворяют потребности всевозможных сетей, от малых до больших. В широком ассортименте кабелей нетрудно запутаться. Но в большинстве сетей применяются только три основные группы кабелей:

- коаксиальный кабель (coaxial cable);
- витая пара (twisted pair):
  - неэкранированная (unshielded);
  - экранированная (shielded);
- оптоволоконный кабель (fiber optic).

### 2.1. Коаксиальный кабель

Не так давно коаксиальный кабель был самым распространенным типом кабеля. Это объяснялось двумя причинами. Во-первых, он был относительно недорогим, легким, гибким и удобным в применении. А во-вторых, широкая популярность коаксиального кабеля привела к тому, что он стал безопасным и простым в установке. Самый простой коаксиальный кабель состоит из медной жилы (core), изоляции окружающей ее, экрана в виде металлической оплетки и внешней оболочки (рис. 2.1). Если кабель, кроме металлической оплетки, имеет и слой фольги, он называется кабелем двойной экранизацией. При наличии сильных помех можно воспользоваться кабелем с учетверенной экранизацией. Он состоит из двойного слоя фольги и двойного или металлической оплетки.

Некоторые типы кабелей покрывает металлическая сетка — экран (shield). Он защищает передаваемые по кабелю данные, поглощая внешние электромагнитные сигналы, называемые помехами или шумом. Таким образом, экран не позволяет помехам исказить данные.

Структура коаксиального кабеля

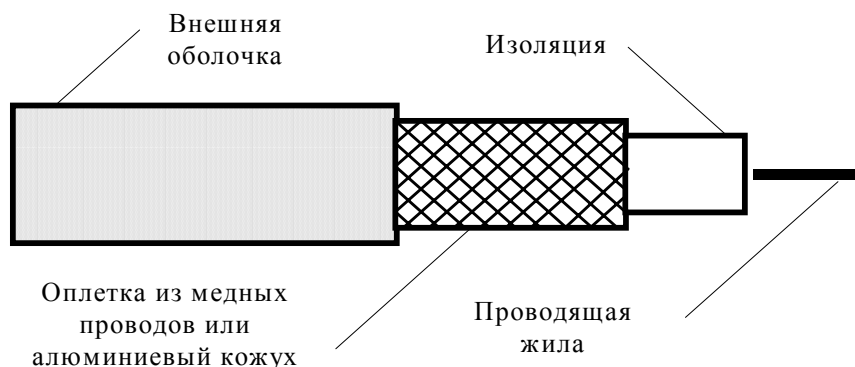


Рис. 2.1



Электрические сигналы, кодирующие данные, передаются по жиле. Жила — это один провод (сплошная) или пучок проводов. Сплошная жила изготавливается, как правило, из меди. Жила окружена изоляционным слоем, который отделяет ее от металлической оплетки. Оплетка играет роль заземления и защищает жилу от электрических шум (noise) и перекрестных помех (crosstalk). Перекрестные помехи — это электрические наводки, вызванные сигналами в соседних проводах.

Проводящая жила и металлическая оплетка не должны соприкасаться, иначе произойдет короткое замыкание, помехи проникнут в жилу, и данные разрушатся. Снаружи кабель покрыт непроводящим слоем — из резины, тефлона или пластика. Коаксиальный кабель более помехоустойчив, затухание сигнала в нем меньше чем в витой паре. Затухание (attenuation) — это уменьшение величины сигнала при его перемещении по кабелю.

Как уже говорилось, плетеная защитная оболочка поглощает внешние электромагнитные сигналы, не позволяя им влиять на передаваемые по жиле данные, поэтому коаксиальный кабель можно использовать при передаче на большие расстояния и в тех случаях, когда высокоскоростная передача данных осуществляется на несложном оборудовании.

Существует два типа коаксиальных кабелей:

- тонкий коаксиальный кабель;
- толстый коаксиальный кабель.

Выбор того или иного типа кабеля зависит от потребностей конкретной сети.

### 2.1.1. Тонкий коаксиальный кабель

Тонкий коаксиальный кабель — гибкий кабель диаметром около 0,5 см. Он прост в применении и годится практически для любого типа сети. Подключается непосредственно к платам сетевого адаптера компьютеров. Тонкий (thin) коаксиальный кабель способен передавать сигнал на расстояние до 185 м без его заметного искажения, вызванного затуханием.

Производители оборудования выработали специальную маркировку для различных типов кабелей. Тонкий коаксиальный кабель относится к группе, которая называется семейством RG-58, его волновое сопротивление равно 50 Ом. Волновое сопротивление (impedance) — это сопротивление переменному току, выраженное в омах. Основная отличительная особенность этого семейства — медная жила. Она может быть сплошной или состоять из нескольких переплетенных проводов. Расшифровка типов кабелей приведена в таблице 3

Коаксиальные кабели

Таблица 3

Кабель	Описание
RG-58 /U	Сплошная медная жила
RG-58 A/U	Переплетенные провода
RG-58 C/U	Военный стандарт для RG-58 A/U
RG-59	Используется для широкополосной передачи (например, в кабельном телевидении)
RG-6	Имеет больший диаметр по сравнению с RG-59, предназначен для более высоких частот, но может применяться и для широкополосной передачи
RG-62	Используется в сетях ArcNet®

### 2.1.2. Толстый коаксиальный кабель

Толстый (thick) коаксиальный кабель — относительно жесткий кабель с диаметром около 1 см. Иногда его называют "стандартный Ethernet", поскольку он был первым типом кабеля, применяемым в Ethernet — популярной сетевой архитектуре. Медная жила этого кабеля толще, чем у тонкого коаксиального кабеля.

Чем толще жила у кабеля, тем большее расстояние способен преодолеть сигнал. Следовательно, толстый коаксиальный кабель передает сигналы дальше, чем тонкий, — до 500 м. Поэтому толстый коаксиальный кабель иногда используют в качестве основного кабеля [магистральной (backbone)], который соединяет несколько небольших сетей, построенных на тонком коаксиальном кабеле.

Для подключения к толстому коаксиальному кабелю применяют специальное устройство — трансивер (transceiver). Трансивер снабжен специальным коннектором, который назван — "зуб вампира" (vampire tap) или "пронзающий ответвитель" (piercing tap). Этот "зуб" проникает через изоляционный слой и вступает в непосредственный физический контакт с проводящей жилой. Чтобы подключить трансивер к сетевому адаптеру, надо кабель трансивера подключить к коннектору AUI-порта сетевой платы. Этот коннектор известен также как DIX-коннектор (Digital Intel Xerox®), в соответствии с названиями фирм-разработчиков, или коннектор DB-15.

### 2.1.3. Компоненты кабельной системы на базе коаксиальных кабелей

Как правило, чем толще кабель, тем сложнее с ним работать. Тонкий коаксиальный кабель гибок, прост в установке и относительно недорог. Толстый кабель трудно гнуть, и, следовательно, его сложнее устанавливать. Это очень существенный недостаток, особенно если необходимо проложить кабель по трубам или желобам. Толстый коаксиальный кабель дороже тонкого, но при этом он передает сигналы на большие расстояния.

Для подключения тонкого коаксиального кабеля к компьютерам используются так называемые BNC-коннектор (British Naval Connector, BNC). В семействе BNC несколько основных компонентов:

- BNC-коннектор. BNC-коннектор либо припаивается, либо обжимается на конце кабеля.
- BNC T-коннектор. T-коннектор соединяет сетевой кабель с сетевой платой компьютера.
- BNC баррел-коннектор. Баррел-коннектор применяется для сращивания двух отрезков тонкого коаксиального кабеля.
- BNC-коннектор. В сети с топологией "шина" для поглощения "свободных" сигналов терминаторы устанавливаются на каждом конце кабеля. Иначе сеть не будет работать.

Выбор того или иного класса коаксиальных кабелей зависит от того, где этот кабель будет прокладываться. Существует два класса коаксиальных кабелей:

- поливинилхлоридные;
- пленумные — для прокладки в области пленума.

Поливинилхлорид (PVC) — это пластик, который применяется в качестве изолятора или внешней оболочки у большинства коаксиальных кабелей. Кабель PVC достаточно гибок, его можно прокладывать на открытых участках помещений. Однако при горении он выделяет ядовитые газы.

Пленум (plenum) — это небольшое пространство между фальш-потолком и перекрытием, обычно его используют для вентиляции. Требования пожарной

безопасности строго ограничивают типы кабелей, которые могут быть здесь проложены, поскольку в случае пожара выделяемые ими дым или газы распространятся по всему зданию.

## 2.2. Витая пара

Самая простая витая пара (twisted pair) — это два перевитых вокруг друг друга изолированных медных провода. Существует два типа тонкого кабеля: неэкранированная (unshielded) витая пара (UTP) и экранированная (shielded) витая пара (STP). Несколько витых пар часто помещают в одну защитную оболочку. Их количество в таком кабеле может быть разным. Завивка проводов позволяет избавиться от электрических помех, наводимых соседними парами и другими источниками, например двигателями, реле и трансформаторами.

### 2.2.1. Неэкранированная витая пара

Неэкранированная витая пара (спецификация 10BaseT) широко используется в ЛВС, максимальная длина сегмента составляет 100 м. Неэкранированная витая пара состоит из двух изолированных медных проводов (рис. 2.2). Существует несколько спецификаций, которые регулируют количество витков на единицу длины — в зависимости от назначения кабеля.

Неэкранированная витая пара определена в особом стандарте — Electronic Industries Association and the Telecommunications Industries Association (EIA/TIA) 568 Commercial Building Wiring Standard. EIA/TIA 568 на основе UTP — устанавливает стандарты для различных случаев, гарантируя единообразие продукции.

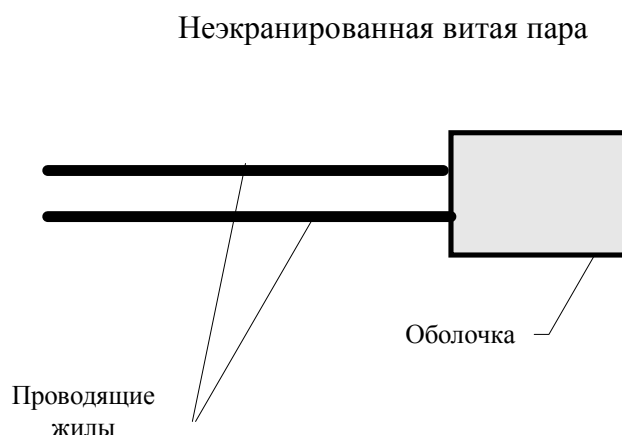


Рис. 2.2

Эти стандарты включают пять категорий UTP.

- *Категория 1.* Традиционный телефонный кабель, по которому можно передавать только речь, но не данные. Большинство телефонных кабелей, произведенных до 1983 года, относится к категории 1.
- *Категория 2.* Кабель, способный передавать данные со скоростью до 4 Мбит/с. Состоит из четырех витых пар.
- *Категория 3.* Кабель, способный передавать данные со скоростью до 10 Мбит/с. Состоит из четырех витых пар с девятью витками на метр.

- *Категория 4.* Кабель, способный передавать данные со скоростью до 16 Мбит/с. Состоит из четырех витых пар.
- *Категория 5.* Кабель, способный передавать данные со скоростью до 100 Мбит/с. Состоит из четырех витых пар медного провода.

Большинство телефонных систем использует неэкранированную витую пару. Это одна из причин ее широкой популярности. Причем во многих зданиях, при строительстве, UTP прокладывают не только для сегодняшних нужд телефонизации, но и, предусматривая запас кабеля, в расчете на будущие потребности. Если установленные во время строительства провода рассчитаны на передачу данных, их можно использовать и в компьютерной сети. Однако надо быть осторожным, так как обычный телефонный провод не имеет витков, и его электрические характеристики могут не соответствовать тем, какие требуются для надежной и безопасной передачи данных между компьютерами.

Одной из потенциальных проблем для всех типов кабелей являются перекрестные помехи — это электрические наводки, вызванные сигналами в смежных проводах. Неэкранированная витая пара особенно страдает от перекрестных помех. Для уменьшения их влияния используют экран.

### 2.2.2. Экранированная витая пара

Кабель экранированной витой пары (STP) имеет медную оплетку, которая обеспечивает большую защиту, чем неэкранированная витая пара (рис.2.3). Кроме того, пары проводов STP обмотаны фольгой. В результате экранированная витая пара обладает прекрасной изоляцией, защищающей передаваемые данные от внешних помех. Все это означает, что STP, по сравнению с UTP, меньше подвержена воздействию электрических помех и может передавать сигналы с более высокой скоростью и на большие расстояния.

Экранированная витая пара

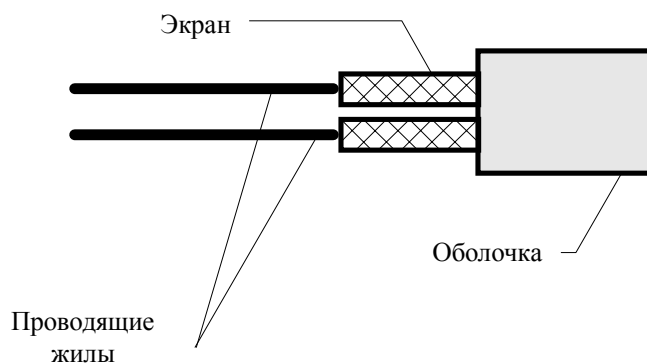


Рис. 2.3

### 2.2.3. Компоненты кабельной системы на базе витой пары

Соединители (connectors). Для подключения витой пары к компьютеру используются телефонные коннекторы RJ-45. На первый взгляд, они похожи на RJ-11, но в действительности между ними есть существенные отличия. Во-первых, вилка RJ-45 чуть больше по размерам и не подходит для гнезда RJ-11. Во-вторых, коннектор RJ-45 имеет восемь контактов, а RJ-11 — только четыре. Построить развитую кабельную

систему и в то же время упростить работу с ней поможет ряд очень полезных компонентов.

*Распределительные стойки и полки* (distribution racks, shelves). Распределительные стойки и полки предназначены для монтажа кабеля. Они позволяют централизованно организовать множество соединений и при этом занимают достаточно мало места.

*Коммутационные панели* (patch panels). Существуют разные типы панелей расширения. Они поддерживают до 96 портов и скорость передачи до 100 Мбит/с.

*Панели расширения.* Одинарные или двойные вилки RJ-45 подключаются к панелям расширения или настенным розеткам. Они обеспечивают скорость передачи до 100 Мбит/с.

## 2.3. Оптоволоконный кабель

В оптоволоконном кабеле цифровые данные распространяются по оптическим волокнам в виде модулированных световых импульсов. Это относительно надежный (защищенный) способ передачи, поскольку электрические сигналы при этом не передаются. Следовательно, оптоволоконный кабель нельзя вскрыть и перехватить данные, от чего не застрахован любой кабель, проводящий электрические сигналы. Оптоволоконные линии предназначены для перемещения больших объемов данных на очень высоких скоростях, так как сигнал в них практически не затухает и не искажается. Оптическое волокно — чрезвычайно тонкий стеклянный цилиндр, называемый жилой (core), покрытый слоем стекла, называемого оболочкой, с иным, чем у жилы, коэффициентом преломления. Иногда оптоволокно производят из пластика. Пластик проще в использовании, но он передает световые импульсы на меньшие расстояния по сравнению со стеклянным оптоволоконным.

Каждое стеклянное оптоволокно передает сигналы только в одном направлении, поэтому кабель состоит из двух волокон с отдельными коннекторами. Одно из них служит для передачи, а другое — для приема. Жесткость волокон увеличена покрытием из пластика, а прочность — волокнами из кевлара.

Передача по оптоволоконному кабелю не подвержена электрическим помехам и ведется на чрезвычайно высокой скорости (в настоящее время до 100 Мбит/с, теоретически возможная скорость — 200 000 Мбит/с). По нему можно передавать световой импульс на многие километры.

Оптоволоконный кабель

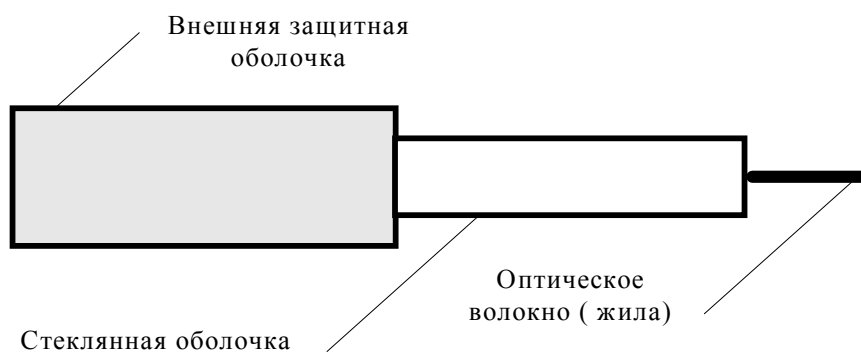


Рис. 2.4

## 2.4. Передача сигналов

Для передачи по кабелю кодированных сигналов используют две технологии — узкополосную передачу и широкополосную передачу.

### Узкополосная передача

Узкополосные (baseband) системы передают данные в виде цифрового сигнала одной частоты (рис.2.5). Сигналы представляют собой дискретные электрические или световые импульсы. При таком способе вся емкость коммуникационного канала используется для передачи одного импульса, или, другими словами, цифровой сигнал использует всю полосу пропускания кабеля. Полоса пропускания — это разница между максимальной и минимальной частотой, которая может быть передана по кабелю. Каждое устройство в сетях с узкополосной передачей посылает данные в обоих направлениях, а некоторые могут одновременно и передавать их, и принимать.

Узкополосная передача. Двухнаправленная цифровая волна.

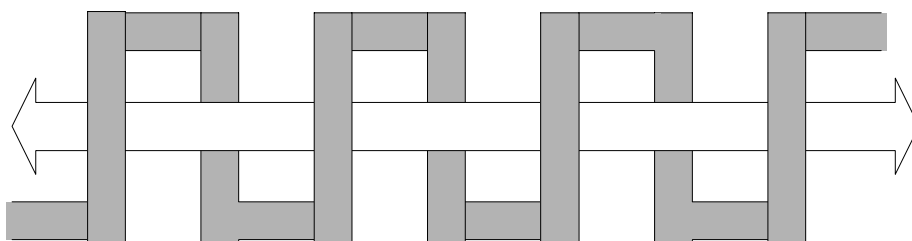


Рис.2.5

Продвигаясь по кабелю, сигнал постепенно затухает и, как следствие, может исказиться. Если кабель слишком длинный, на дальнем его конце передаваемый сигнал может исказиться до неузнаваемости или просто пропасть.

Чтобы избежать этого, в узкополосных системах используют репитеры, которые усиливают сигнал и ретранслируют его в дополнительные сегменты, позволяя тем самым увеличить общую длину кабеля.

### Широкополосная передача

Широкополосные (broadband) системы передают данные в виде аналогового сигнала, который использует некоторый интервал частот. Сигналы представляют собой непрерывные (а не дискретные) электромагнитные или оптические волны. При таком способе сигналы передаются по физической среде в одном направлении.

Если обеспечить необходимую полосу пропускания, то по одному кабелю одновременно может идти вещание нескольких систем, таких, как кабельное телевидение и передача данных.

Каждой передающей системе выделяется часть полосы пропускания. Все устройства, связанные с данной системой (например, компьютеры), должны быть настроены таким образом, чтобы работать именно с выделенной частью полосы пропускания.

Если в узкополосных системах для восстановления сигнала используют репитеры, то в широкополосных — усилители (amplifiers). В широкополосной системе

сигнал передается только в одном направлении, поэтому, чтобы все устройства могли и принимать, и передавать данные, необходимо обеспечить два пути для прохождения сигнала. Разработано два основных решения:

- разбить полосу пропускания на два канала, которые работают с различными частотами; один канал предназначен для передачи сигналов, другой — для приема;
- использовать два кабеля; один кабель предназначен для передачи сигналов, другой для приема.

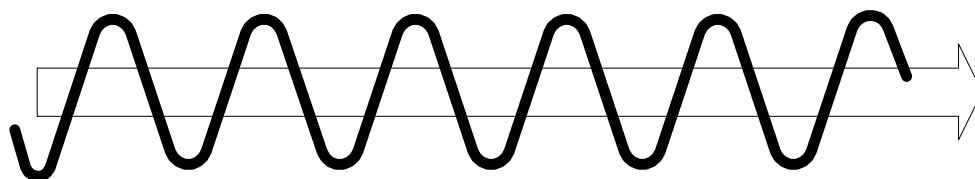


Рис.2.6

## 2.5. Сравнение кабелей

При выборе кабеля (как, впрочем, и любых других сетевых компонентов) необходимо найти некий компромисс между его стоимостью и характеристиками. Кабельная система должна соответствовать условиям ее применения. К числу факторов, влияющих на стоимость и пропускную способность кабеля относятся следующие.

*Простота установки.* Насколько прост кабель в установке, насколько просто работать с ним? В небольших сетях, с небольшими расстояниями, где безопасность данных не самый главный вопрос, нет смысла прокладывать толстый, громоздкий и дорогой кабель.

*Экранирование.* Экранирование кабеля приводит к его удорожанию, тем не менее практически любая сеть использует одну из форм экранированного кабеля. Чем больше помех в месте прокладки кабеля, тем большее экранирование требуется. Прокладка пленумного кабеля существенно увеличивает стоимость проекта.

*Перекрестные помехи.* Перекрестные помехи и внешние шумы могут вызвать серьезные проблемы в больших сетях, где критическим вопросом является вопрос защиты данных. Недорогие кабели слабо защищены от внешних электрических полей, генерируемых электропроводкой двигателями, реле и радиопередатчиками.

*Скорость передачи* (часть полосы пропускания). Скорость передачи измеряется в мегабитах в секунду (Мбит/с). Для медных кабелей сегодня самым распространенным значением является 10 Мбит/с, хотя последние стандарты позволяют передавать данные со скоростью 100 Мбит/с. Толстый коаксиальный кабель передает сигналы на большие расстояния, чем тонкий. Но с ним сложнее работать. По оптоволоконному кабелю данные передаются со скоростью более 100 Мбит/с, но для его установки нужны специальные навыки, к тому же он сравнительно дорог.

*Стоимость.* Стоимость кабелей, которые обеспечивают высокую степень защиты, передавая данные на большие расстояния, гораздо выше стоимости тонкого коаксиального кабеля простого в установке и эксплуатации.

*Затухание сигнала.* Затухание сигнала — причина, которая ограничивает максимальную длину кабеля так как значительно ослабленный сигнал может быть не распознан принимающим компьютером. Кабели разных типов имеют разную максимальную длину. Большинство сетей использует системы проверки ошибок: при искажении принятого сигнала они требуют его повторной передачи. Однако на это уходит дополнительное время, и, главное, снижается общая пропускная способность сети. Обобщенные характеристики рассмотренных кабелей приведены в табл.2.2.

Характеристики кабелей				Таблица 4
Характеристика	Тонкий коаксиальный кабель (10Base2)	Толстый коаксиальный кабель (10Base5)	Витая пара (10BaseT)	Оптоволоконный кабель
Стоимость	Дороже витой пары	Дороже тонкого коаксиального кабеля	Самый дешевый	Самый дорогой
Эффективная длина	185 м	500 м	100 м	2 км
Скорость передачи	10 Мбит/с	10 Мбит/с	4-100 Мбит/с	100 Мбит/с
Гибкость	Довольно гибкий	Менее гибкий	Самый гибкий	Не гибкий
Простота установки	Прост в установке	Прост в установке	Очень прост в установке	Труден в установке
Подверженность помехам	Хорошо защищен от помех	Хорошо защищен от помех	Подвержен помехам	Не подвержен помехам
Особые свойства	Электронные компоненты дешевле чем витой пары	Электронные компоненты дешевле, чем витой пары	Возможно использование телефонного провода	Поддерживает видео, речь и данные.
Рекомендуемое применение	Средние или большие сети с высокими требованиями к защите данных	Средние или большие сети с высокими требованиями к защите данных	Самый дешевый вариант сети	Сети любого размера с высокими требованиями к скорости передачи, уровню защиты и целостности данных

## 2.6. Беспроводные сети

Беспроводная среда постепенно входит в нашу жизнь. Как только технология окончательно сформируется, производители предложат широкий выбор продукции по приемлемым ценам, что приведет и к росту спроса на нее, и к увеличению объема продаж. В свою очередь, это вызовет дальнейшее совершенствование и развитие беспроводной среды. Словосочетание "беспроводная среда" может ввести в заблуждение, поскольку означает полное отсутствие проводов в сети. В действительности же это не так. Обычно беспроводные компоненты взаимодействуют с



сетью, в которой — как среда передачи — используется кабель. Такая сеть со смешанными компонентами называется гибридной.

Идея беспроводной среды весьма привлекательна, так как ее компоненты:

- обеспечивают временное подключение к существующей кабельной сети;
- помогают организовать резервное копирование в существующую кабельную сеть;
- гарантируют определенный уровень мобильности;
- позволяют снять ограничения на максимальную протяженность сети, накладываемые медными или даже оптоволоконными кабелями.

В зависимости от технологии беспроводные сети можно разделить на три типа:

- локальные вычислительные сети;
- расширенные локальные вычислительные сети;
- мобильные сети (переносные компьютеры).

Основные различия между этими типами сетей — параметры передачи. Локальные и расширенные локальные вычислительные сети используют передатчики и приемники, принадлежащие той организации, в которой функционирует сеть.

## 2.6.1. Локальные беспроводные сети

Типичная беспроводная сеть выглядит и функционирует практически так же, как обычная, за исключением среды передачи. Беспроводной сетевой адаптер с трансивером установлен в каждом компьютере, и пользователи работают так, будто их компьютеры соединены кабелем.

Трансивер, называемый иногда точкой доступа (access point), обеспечивает обмен сигналами между компьютерами с беспроводным подключением и остальной сетью. В беспроводных ЛВС используются небольшие настенные трансиверы. Они устанавливают радиокontakt между переносными устройствами. Такую сеть нельзя назвать полностью беспроводной именно из-за использования этих трансиверов.

Беспроводные локальные сети используют четыре способа передачи данных:

- инфракрасное излучение; лазер;
- радиопередачу в узком спектре (одночастотная передача);
- радиопередачу в рассеянном спектре.

### Инфракрасное излучение

Все инфракрасные беспроводные сети используют для передачи данных инфракрасные лучи. В подобных системах необходимо генерировать очень сильный сигнал, так как в противном случае значительное влияние будут оказывать другие источники, например окна. Этот способ позволяет передавать сигналы с большой скоростью, поскольку инфракрасный свет имеет широкий диапазон частот. Инфракрасные сети способны нормально функционировать на скорости 10 Мбит/с. Существует четыре типа инфракрасных сетей.

*Сети прямой видимости.* Как говорит само название, в таких сетях передача возможна лишь в случае прямой видимости между передатчиком и приемником.

*Сети на рассеянном инфракрасном излучении.* При этой технологии сигналы, отражаясь от стен и потолка, в конце концов достигают приемника. Эффективная область ограничивается примерно 30 м, и скорость передачи невелика (так как все сигналы отраженные).

*Сети на отраженном инфракрасном излучении.* В этих сетях оптические трансиверы, расположенные рядом с компьютером, передают сигналы в определенное место, из которого они переадресуются соответствующему компьютеру.

*Широкополосные оптические сети.* Эти инфракрасные беспроводные сети предоставляют широкополосные услуги. Они соответствуют жестким требованиям мультимедийной среды и практически не уступают кабельным сетям.

Хотя скорость и удобство использования инфракрасных сетей очень привлекательны, возникают трудности при передаче сигналов на расстояние более 30 м. К тому же такие сети подвержены помехам со стороны сильных источников света, которые есть в большинстве организаций.

## **Лазер**

Лазерная технология похожа на инфракрасную тем, что требует прямой видимости между передатчиком и приемником. Если по каким-либо причинам луч будет прерван, это прервет и передачу.

## **Радиопередача в узком спектре (одночастотная передача)**

Этот способ напоминает вещание обыкновенной радиостанции. Пользователи настраивают передатчики и приемники на определенную частоту. При этом прямая видимость необязательна, площадь вещания составляет около 46 500 м<sup>2</sup>. Сигнал высокой частоты, который используется, не проникает через металлические или железобетонные преграды. Доступ к такому способу связи осуществляется через поставщика услуг. Связь относительно медленная (около 4,8 Мбит/с).

## **Радиопередача в рассеянном спектре**

При этом способе сигналы передаются в некоторой полосе частот, что позволяет избежать проблем связи, присущих одночастотной передаче. Доступные частоты разделены на каналы, или интервалы. Адаптеры в течение предопределенного промежутка времени настроены на установленный интервал, после чего переключаются на другой интервал. Переключение всех компьютеров в сети происходит синхронно. Чтобы защитить данные от несанкционированного доступа, применяют кодирование. Скорость передачи в 250 Кбит/с (килобит в секунду) относит данный способ к разряду самых медленных. Но есть сети, построенные на его основе, которые передают данные со скоростью до 11 Мбит/с на расстояние до 3,2 км—на открытом пространстве и до 120м—внутри здания.

Это тот случай, когда технология позволяет получить по-настоящему беспроводную сеть. Например, два (или более) компьютера, оснащенные адаптерами Xircom CreditCard Netwave с операционными системами типа Microsoft Windows 95/98 или Microsoft Windows NT, могут без кабеля функционировать как одноранговая сеть.

## **Передача "точка-точка"**

Данный способ передачи несколько выходит за рамки существующего определения сети. Технология передачи "точка-точка" предусматривает обмен данными только между компьютерами, в отличие от взаимодействия между несколькими компьютерами и периферийными устройствами. Однако, чтобы организовать сеть с беспроводной 1 передачей, надо использовать дополнительные компоненты, такие, как одиночные и 1 хост-трансиверы. Их можно устанавливать как на автономных компьютерах, так и на I компьютерах, подключенных к сети.

Эта технология, основанная на последовательной передаче данных, обеспечивает: высокоскоростную и безошибочную передачу, применяя радиоканал "точка-точка"; проникание сигнала через стены и перекрытия;

скорость передачи от 1,2 до 38,4 Кбит/с на расстояние до 60м — внутри здания и на 530 м — в условиях прямой видимости.

Подобные системы позволяют передавать сигналы между компьютерами, между компьютерами и другими устройствами, например принтерами или сканерами штрих-кода.

## **2.6.2. Расширенные беспроводные сети**

Некоторые типы беспроводных компонентов способны функционировать в расширенных локальных вычислительных сетях так же, как их аналоги — в кабельных сетях. Беспроводной мост, например, соединяет сети, находящиеся друг от друга на расстоянии до 25 километров.

### **Многоточечное беспроводное соединение**

Компонент, называемый беспроводным мостом (wireless bridge), помогает установить связь между зданиями без участия кабеля. Как обычный мост служит людям для перехода с одного берега реки на другой, так и беспроводной мост прокладывает для данных путь между двумя зданиями. Мост AIRLAN/Bridge Plus, например, использует технологию радиопередачи в рассеянном спектре для создания магистрали, соединяющей ЛВС. Расстояние между ними, в зависимости от условий, может достигать 25 км. Стоимость эксплуатации такого устройства не покажется чрезмерной, поскольку отпадет необходимость арендовать линии связи.

### **Беспроводные мосты дальнего действия**

Если расстояние, которое "покрывает" беспроводной мост, недостаточно, можно установить мост дальнего действия. Для работы с сетями Ethernet и Token Ring на расстояние до 40 км он также использует технологию радиопередачи в рассеянном спектре. Его стоимость (как и обыкновенного беспроводного моста) может оказаться вполне удовлетворительной, так как отпадут затраты на аренду микроволновых каналов или линий T1. Линия T1 — это стандартная цифровая линия, предназначенная для передачи данных со скоростью до 1,544 Мбит/с. По ней можно передавать и речь, и данные.

## **2.6.3. Мобильные сети**

В беспроводных мобильных сетях в качестве среды передачи выступают телефонные системы и общественные службы. При этом используются:

- пакетное радиосоединение;
- сотовые сети;
- спутниковые станции.

Работники, которые постоянно находятся в разъездах, могут воспользоваться этой технологией: имея при себе переносные компьютеры или PDA (Personal Digital Assistants), они будут обмениваться электронной почтой, файлами и другой информацией. Такая форма связи удобна, но довольно медленна. Скорость передачи — от 8 Кбит/с до 28,8 Кбит/с. А если запущена система коррекции ошибок, скорость становится еще меньше.

Для подключения переносных компьютеров к основной сети применяют беспроводные адаптеры, использующие технологию сотовой связи. Небольшие

антенны, установленные на переносных компьютерах, связывают их с окружающими радиоретрансляторами.

### **Пакетное радиосоединение**

При пакетном радиосоединении данные разбиваются на пакеты (подобные сетевым пакетам), в которых содержится следующая информация:

- адрес источника;
- адрес приемника;
- информация для коррекции ошибок.

Пакеты передаются на спутник, который транслирует их в широкоэмитательном режиме. Затем устройства с соответствующим адресом принимают эти пакеты.

### **Сотовые сети**

Сотовые цифровые пакеты данных (Cellular Digital Packet Data, CDPD) используют ту же технологию, что и сотовые телефоны. Они передают данные по существующим для передачи речи сетям в те моменты, когда эти сети не заняты. Это очень быстрая технология связи с задержкой в доли секунды, что делает ее вполне приемлемой для передачи в реальном масштабе времени. Наиболее распространенная сейчас в России сеть подобного типа – цифровая сеть GSM.

### **Микроволновые системы**

Микроволновая технология помогает организовать взаимодействие между зданиями в небольших, компактных системах, например в университетских городках. На сегодняшний день микроволновая технология — наиболее распространенный в Соединенных Штатах метод передачи данных на дальние расстояния. Он идеален при взаимодействии — в прямой видимости — двух точек, таких, как:

- спутник и наземная станция;
- два здания;
- любые объекты, которые разделяет большое открытое пространство (например, водная поверхность или пустыня).

Микроволновая система состоит из следующих компонентов.

- Двух радиотрансиверов. Один для генерации сигналов (передающая станция), а другой — для приема (приемная станция).
- Двух направленных антенн. Они нацелены друг на друга так, чтобы осуществить прием сигналов, передаваемых трансиверами. Эти антенны часто устанавливают на вышки, чтобы покрыть большие расстояния.
- 

## **3. Сетевые адаптеры**

### **3.1. Назначение сетевого адаптера**

Платы сетевого адаптера выступают в качестве физического интерфейса, или соединения, между компьютером и сетевым кабелем. Платы вставляются в слоты расширения всех сетевых компьютеров и серверов. Чтобы обеспечить физическое соединение между компьютером и сетью, к соответствующему разъему, или порту, платы (после ее установки) подключается сетевой кабель.

Назначение платы сетевого адаптера:

- подготовка данных, поступающих от компьютера, к передаче по сетевому кабелю;
- передача данных другому компьютеру;
- управление потоком данных между компьютером и кабельной системой.

Плата сетевого адаптера, кроме того, принимает данные из кабеля и переводит их в форму, понятную центральному процессору компьютера. Общий вид сетевого адаптера представлен на рис.3.1.

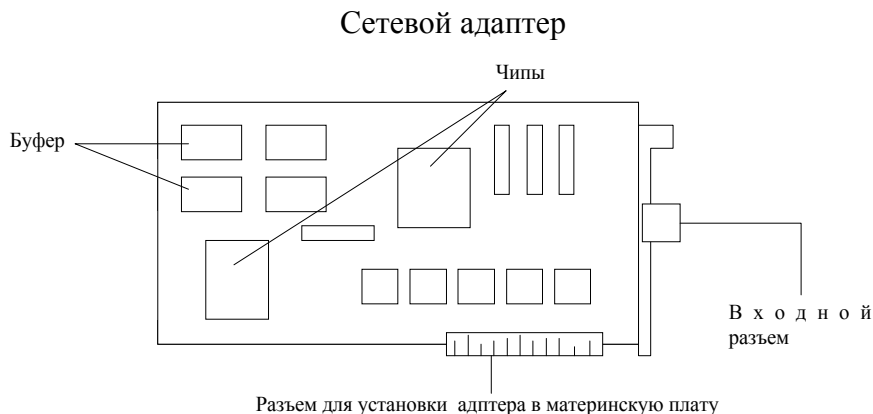


Рис.3.1

Плата сетевого адаптера состоит из аппаратной части и встроенных программ, записанных в ПЗУ. Эти программы реализуют функции подуровней *Управления логической связью* и *Управления доступом* к среде Канального уровня модели OSI. Перед тем как послать данные в сеть, плата сетевого адаптера должна перевести их из формы, понятной компьютеру, в форму, в которой они могут передаваться по сетевому кабелю. Внутри компьютера данные передаются по шинам. Как правило, это несколько проводников, расположенных близко друг к другу. Так как линий несколько, то и биты данных могут передаваться по ним группами, а не последовательно.

Шины, которые использовались в первых персональных компьютерах IBM, были известны как 8-разрядные шины: они могли передавать группы по 8 битов данных. IBM PC/AT® имеет 16-разрядную шину, это означает, что она способна передавать сразу 16 битов. Современные компьютеры оснащены уже 32-разрядной шиной. Часто говорят, что данные по шине компьютера передаются параллельно (parallel), так как 16 битов или 32 бита движутся параллельно друг другу.

В сетевом кабеле данные должны перемещаться в виде потока битов. При этом говорят, что происходит последовательная передача, потому что биты следуют друг за другом.

Плата сетевого адаптера принимает параллельные данные и организует их для последовательной (serial), побитовой, передачи. Этот процесс завершается переводом цифровых данных компьютера в электрические и оптические сигналы, которые и передаются по сетевым кабелям. Отвечает за это преобразование трансивер.

Помимо преобразования данных, плата сетевого адаптера должна указать свое мест нахождение, или адрес, — чтобы ее могли отличить от остальных плат. Сетевые адреса (network address) определены комитетом IEEE. Этот комитет закрепляет за каждым производителем плат сетевого адаптера некоторый интервал адресов. Производители "зашивают" эти адреса в микросхемы. Благодаря этому каждая плата и, следовательно, каждый компьютер имеют уникальный адрес в сети (MAC-address). При приеме данных от компьютера и подготовке их к передаче по сетевому кабелю плата сетевого адаптера участвует также в других операциях. Если плата может использовать прямой доступ к памяти, компьютер выделяет ей некоторую область своей памяти.

Перед тем как послать данные по сети, плата сетевого адаптера проводит электронный диалог с принимающей платой, во время которого они "обговаривают":

- максимальный размер блока передаваемых данных;
- объем данных, передаваемых без подтверждения о получении;
- интервалы между передачами блоков данных;
- интервал, в течение которого необходимо послать подтверждение;
- объем данных, который может принять каждая плата, не переполняясь;
- скорость передачи данных.

Если новой (более сложной и быстрой) плате необходимо взаимодействовать со старой (медленной) платой, они должны найти общую для обеих скорость передачи. Схемы некоторых современных плат сетевого адаптера позволяют им приспособиться к медленной скорости старых плат.

Каждая плата оповещает другую о своих параметрах, принимая "чужие" параметры и подстраиваясь к ним. После того как все детали определены, платы начинают обмен данными.

### 3.2. Параметры конфигурации сетевого адаптера

Параметры платы сетевого адаптера должны быть корректно установлены, чтобы ее работа протекала правильно. В их число входят:

- прерывание;
- базовый адрес порта ввода/вывода;
- базовый адрес памяти;
- используемый трансивер.

Параметры платы сетевого адаптера иногда устанавливаются в программном обеспечении, но они должны совпадать с установками, заданными на плате переключками или DIP-переключателями. Дополнительную информацию о настройке платы с помощью переключателей можно получить из ее документации.

#### Прерывание

Линии запроса прерывания — это физические линии, по которым различные устройства (например, порты ввода/вывода, клавиатура, драйверы дисков и платы сетевого адаптера) могут послать микропроцессору компьютера запросы на обслуживание, или на прерывание /3-8/.

Линии запроса прерывания встроены в аппаратуру компьютера, они имеют различные уровни приоритетов, что позволяет процессору определить наиболее важный из запросов. Посылая компьютеру запрос, плата сетевого адаптера использует прерывание (interrupt) — электрический сигнал, который направляется центральному процессору компьютера. Все устройства в компьютере должны пользоваться разными линиям запроса прерывания, или прерыванием (IRQ). Линия запроса прерывания задается при настройке устройства.

В большинстве случаев платы сетевого адаптера используют прерывание IRQ3, IRQ5, IRQ10 или IRQ11. Если есть выбор, рекомендуется отдать предпочтение IRQ5 тем более что это значение установлено по умолчанию во многих системах.

Если ни IRQ3, ни IRQ5 недоступны, необходимо другой доступный номер прерывания. Данные по прерываниям для IBM-совместимых компьютерам от 286 процессора и выше представлены в таблице 5

Прерывания, используемые в компьютере

Таблица 5

Номер прерывания	Устройство
2 (9)	видеоадаптер EGA/VGA

3	Доступен [если не занят вторым последовательным портом (COM2, COM4) или мышью]
4	COM1.COM3
5	Доступен [если не занят вторым параллельным портом (LPT2) или звуковой платой]
6	Контроллер дисководов
7	Параллельный порт (LPT1)
8	Часы
10	Доступен
11	Доступен
12	Мышь (только для компьютеров PS/2)
13	Математический сопроцессор
14	Контроллер жесткого диска
15	Контроллер жесткого диска

### Базовый порт ввода/вывода

Базовый порт ввода/вывода (base i/o port) определяет канал, по которому курсируют данные между устройством компьютера (например, платой сетевого адаптера) и его центральным процессором. Для центрального процессора порт выглядит как адрес.

Каждое устройство системы должно иметь уникальный адрес базового порта ввода/вывода. Адреса портов (в шестнадцатеричном формате), представленные в следующей таблице, если они не заняты, могут быть выделены плате сетевого адаптера. В таблице 6 перечислены адреса портов и соответствующие им устройства.

Адреса портов компьютера

Таблица 6

Порт	Устройство	Порт	Устройство
200-20F	Игровой порт	300-30F	Плата сетевого
210-21F		310-31F	адаптера
220-22F	Звуковая карта	320-32F	
230-23F		330-33F	
240-24F		340-34F	
250-25F		350-35F	
260-26F		360-36F	
270-27F	LPT2	370-37F	LPT1
280-28F		380-38F	FM-синтезатор
290-29F		390-39F	
2A0-2AF		3A0-3AF	
2B0-2BF		3B0-3BF	
2C0-2CF		3C0-3CF	EGA/VGA
2D0-2DF		3D0-3DF	CGA/MCGA
2E0-2EF	COM4	3E0-3EF	COM3
2F0-2FF	COM2	3F0-3FF	COM1 и FDD

Базовый адрес памяти (base address) указывает на ту область памяти компьютера (RAM), которая используется платой сетевого адаптера в качестве буфера для входящих и исходящих кадров данных. Этот адрес иногда называют начальным адресом RAM.

Часто базовым адресом памяти у платы сетевого адаптера является D8000. (Для некоторых плат последний нуль не указывается: вместо D8000 пишется D800.). При

этом необходимо выбирать базовый адрес памяти, не занятый другим устройством. У плат сетевого адаптера, которые не используют оперативную память системы, отсутствует такой параметр, как базовый адрес памяти.

Некоторые платы сетевого адаптера имеют параметр, позволяющий выделить определенный объем памяти для хранения кадров данных. Например, есть платы, в которых можно выделить 16 Кб или 32 Кб памяти. Чем больше памяти выделяется, тем выше скорость сети, но тем меньше памяти остается для других целей. Чтобы обеспечить совместимость компьютера и сети, плата сетевого адаптера должна отвечать следующим требованиям:

- соответствовать внутренней структуре компьютера (архитектуре шины данных);
- иметь соединитель (он должен подходить к типу кабельной системы) для подключения сетевого кабеля.

### **Архитектура шины данных**

К распространенным типам архитектуры шины данных относятся ISA, EISA, Micro Channel® и PCI. Каждая из них физически отличается от остальных.

*ISA (Industry Standard Architecture).* ISA — это архитектура, используемая в компьютерах IBM PC, XT™, AT и совместимых с ними. Чтобы дополнить систему различными адаптерами, необходимо установить платы в слоты расширения. В 1984 году (когда IBM представила IBM PC/AT) ISA была расширена с 8 разрядов до 16. ISA — это название самого слота (8- или 16-ра рядного), 8-разрядные слоты короче 16-разрядных, которые состоят из двух слотов следующих один за другим. Поэтому 8-разрядная плата может быть вставлена в 16-разрядные слоты, но не наоборот. ISA была стандартной архитектурой персональных компьютеров, пока Compaq и несколько других компаний не разработали шину EISA.

*EISA (Extended Industry Standard Architecture).* Этот стандарт шины был представлен в 1988 году консорциумом из девяти компьютерных компаний: AST Research, Inc., Compaq, Epson, Hewlett-Packard, NEC, Olivetti, Tandy, Wyse Technology и Zenith. EISA предлагает 32-разрядную шину, совместимую с ISA. Кроме того, она поддерживает дополнительные возможности, которыми обладает шина Micro Channel Architecture, разработанная IBM.

*MCA (Micro Channel Architecture).* IBM представила этот стандарт в 1988 году как часть своего проекта PS/2. Эта архитектура электрически и физически несовместима с шиной ISA. В отличие от ISA, Micro Channel работает и как 16-разрядная, и как 32-разрядная шина. Несколько процессоров контроля шины могут независимо управлять ею.

*PCI (Peripheral Component Interconnect).* Это 32-разрядная локальная шина, которая используется в большинстве компьютеров с процессором Pentium и в компьютерах Apple Power Macintosh. Современная архитектура PCI удовлетворяет большинству требований технологии Plug and Play. Plug and Play — это одновременно и философия построения персонального компьютера, и набор спецификаций его архитектуры. Цель технологии Plug and Play — возможность изменить конфигурацию персонального компьютера без вмешательства пользователя, т.е. максимально упростить подключение любого устройства. Операционными системами, поддерживающими спецификацию Plug and Play, являются Microsoft Windows95/98/2000.

### **Сетевые кабели и соединители**

Координируя взаимодействие сетевого кабеля и компьютера, плата сетевого адаптера выполняет три важные функции:



- организует физическое соединение с кабелем;
- генерирует электрические сигналы, передаваемые по кабелю;
- следует определенным правилам, регламентирующим доступ к сетевому кабелю.

Прежде чем выбрать плату сетевого адаптера, соответствующую сети, необходимо определить тип кабеля и соединителей, которые будут использоваться. Каждый тип кабеля имеет различные физические характеристики, которым должна соответствовать плата. Поэтому плата сетевого адаптера рассчитана для работы с определенным типом кабеля (коаксиальным, витой парой или оптоволоконном). Некоторые платы сетевого адаптера имеют несколько типов соединителей. Например, есть платы, разъемы которых подходят для тонкого и толстого коаксиальных кабелей или для витой пары и толстого коаксиального кабеля.

Если у платы сетевого адаптера более одного интерфейсного разъема, выбор каждого из них производится с помощью перемычек или DIP-переключателя, расположенных на самой плате, либо программно. Чтобы правильно сконфигурировать сетевую плату, обращайтесь к ее документации.

## **Производительность сети**

Поскольку плата сетевого адаптера оказывает существенное влияние на передачу данных, естественно, она влияет и на производительность всей сети. Если плата медленная, то и скорость передачи данных по сети не будет высокой. В сети с топологией "шина", где нельзя начать передачу, пока кабель занят, медленная сетевая плата увеличивает время ожидания для всех пользователей.

После определения физических требований к плате сетевого адаптера — типа разъема и типа сети, в которой она будет использоваться, — необходимо рассмотреть ряд факторов, влияющих на возможности платы.

Хотя все платы сетевого адаптера удовлетворяют определенным минимальным стандартам и спецификациям, некоторые из плат имеют дополнительные возможности, повышающие производительность сервера, клиента и всей сети.

Итак, к факторам, от которых зависит скорость передачи данных, относят следующие.

- Прямой доступ к памяти. Данные напрямую передаются из буфера платы сетевого адаптера в память компьютера, не затрагивая при этом центральный процессор. Разделяемая память адаптера. Плата сетевого адаптера имеет собственную оперативную память, которую она использует совместно с компьютером. Компьютер воспринимает эту память как часть собственной.
- Разделяемая системная память. Процессор платы сетевого адаптера использует для обработки данных часть памяти компьютера.
- Управление шиной. К плате сетевого адаптера временно переходит управление шиной компьютера, минуя центральный процессор, плата передает данные непосредственно в системную память компьютера. При этом повышается производительность компьютера, так как его процессор в это время может решать другие задачи. Подобные платы дороже стандартных, но они способны повысить производительность сети на 20—70 процентов. Архитектуры EISA, MCA и PCI поддерживают этот метод.
- Буферизация. Для большинства плат сетевого адаптера современные скорости передачи данных по сети слишком высоки. Поэтому на плате сетевого адаптера устанавливают буфер — с помощью микросхем памяти. В случае, когда плата принимает данных больше, чем способна обработать, буфер сохраняет данные до тех пор, пока они не будут обработаны адаптером. Буфер повышает производительность платы, не давая ей стать узким местом системы.
- Встроенный микропроцессор. С таким микропроцессором плате сетевого адаптера для обработки данных не требуется помощь компьютера. Большинство сетевых

плат имеет свои микропроцессоры, которые увеличивают скорость сетевых операций.

- ПЗУ удаленной загрузки
- Бывают ситуации, когда безопасность данных настолько важна, что рабочие станции не оборудуются жесткими и гибкими дисками. Эта мера гарантирует, что пользователи не смогут ни скопировать данные на какой-либо магнитный носитель, ни вынести диск с рабочего места. Однако (поскольку обычно компьютер загружается с дискеты или с жесткого диска) необходимо иметь другой источник загрузки программного обеспечения, запускающего компьютер и подключающего его к сети. В таких случаях плата сетевого адаптера снабжается специальной микросхемой ПЗУ удаленной загрузки (remote-boot FROM), которая содержит код для загрузки компьютера и для подключения его к сети (зависит от сетевой операционной системы). С такой микросхемой бездисковые рабочие станции при запуске могут подключаться к сети.

## 4. Сетевые модели OSI и IEEE Project 802

### 4.1. Модель OSI

В 1978 году International Standards Organization (ISO) выпустила набор спецификаций, описывающих архитектуру сети с неоднородными устройствами. Исходный документ относился к открытым системам, чтобы все они могли использовать одинаковые протоколы и стандарты для обмена информацией.

В 1984 году ISO выпустила новую версию своей модели, названную эталонной моделью взаимодействия открытых систем (Open System Interconnection reference model, OSI). Версия 1984 года стала международным стандартом: именно ее спецификации используют производители при разработке сетевых продуктов, именно ее придерживаются при построении сетей.

Эта модель — широко распространенный метод описания сетевых сред. Являясь многоуровневой системой, она отражает взаимодействие программного и аппаратного обеспечения при осуществлении сеанса связи, а также помогает решить разнообразные проблемы.

В модели OSI сетевые функции распределены между семью уровнями. Каждому уровню соответствуют различные сетевые операции, оборудование и протоколы. На рис. 4.1 представлена многоуровневая архитектура модели OSI. На каждом уровне выполняются определенные сетевые функции, которые взаимодействуют с функциями соседних уровней, вышележащего и нижележащего.

Например, *сеансовый уровень* должен взаимодействовать только с *представительским* и *транспортным уровнем* и т.п. Все эти функции подробно описаны. Нижние уровни — 1-й и 2-й — определяют физическую среду передачи данных и сопутствующие задачи (такие, как передача битов данных через плату сетевого адаптера и кабель). Самые верхние уровни определяют, каким способом осуществляется доступ приложений к услугам связи. Чем выше уровень, тем более сложную задачу он решает.

Каждый уровень предоставляет несколько услуг (т.е. выполняет несколько операций), подготавливающих данные для доставки по сети на другой компьютер. Уровни отделяются друг от друга границами — интерфейсами. Все запросы от одного уровня к другому передаются через интерфейс. Каждый уровень использует услуги нижележащего уровня.

## Уровни моделей OSI



Рис. 4.1

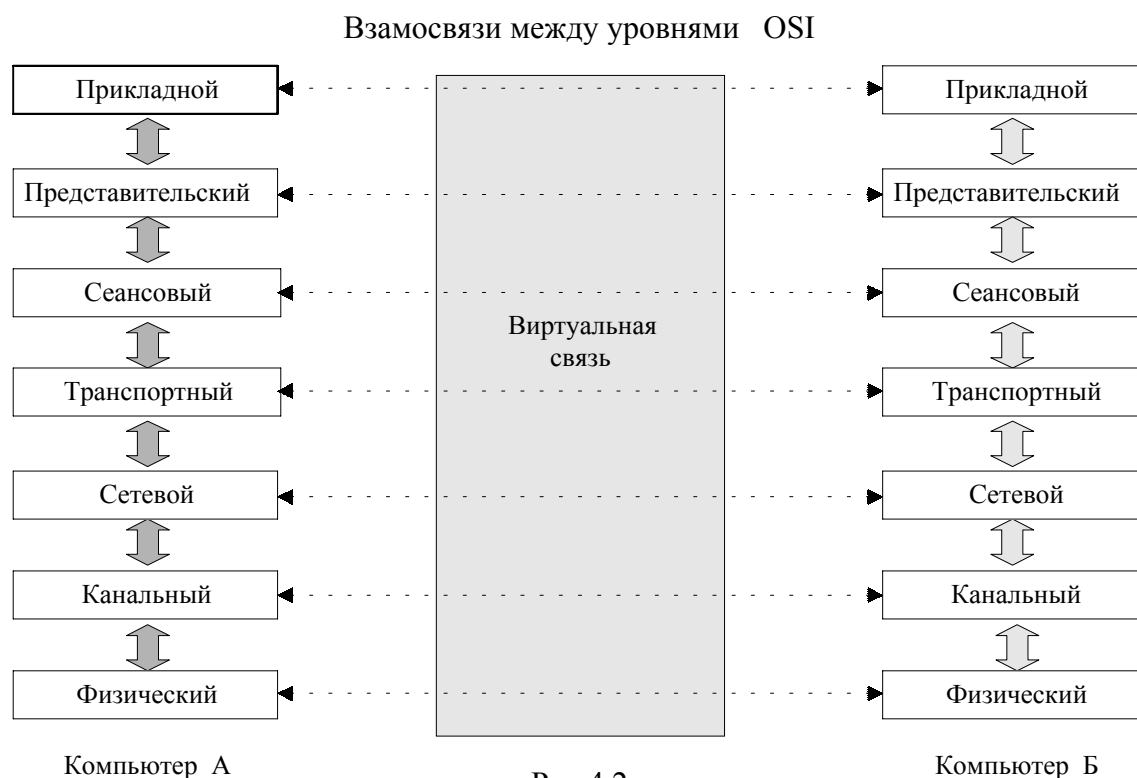
**4.1.1. Взаимодействие уровней модели OSI**

Задача каждого уровня — предоставление услуг вышележащему уровню, "маскируя" детали реализации этих услуг. При этом каждый уровень на одном компьютере работает так, будто он напрямую связан с таким же уровнем на другом компьютере. Эта логическая, или виртуальная, связь между одинаковыми уровнями показана на рисунке 4.2. Однако в действительности связь осуществляется между смежными уровнями одного компьютера — программное обеспечение, работающее на каждом уровне, реализует определенные сетевые функции в соответствии с набором протоколов.

Перед подачей в сеть данные разбиваются на пакеты. Пакет (packet) — это единица информации, передаваемая между устройствами сети как единое целое. Пакет проходит последовательно через все уровни программного обеспечения. На каждом уровне: не к пакету добавляется некоторая информация, форматирующая или адресная, которая необходима для успешной передачи данных по сети.

На принимающей стороне пакет проходит через все уровни в обратном порядке. Программное обеспечение на каждом уровне читает информацию пакета, затем удаляет информацию, добавленную к пакету на этом же уровне отправляющей стороной, передает пакет следующему уровню. Когда пакет дойдет до *прикладного уровня*, вся адресная информация будет удалена и данные примут свой первоначальный вид.

Таким образом, за исключением самого нижнего уровня сетевой модели, никакой иной уровень не может непосредственно послать информацию соответствующему уровню другого компьютера. Информация на компьютере-отправителе должна пройти через все уровни. Затем она передается по сетевому кабелю на компьютер-получатель и опять проходит сквозь все слои, пока не достигнет того же уровня, с которого она была послана на компьютере-отправителе.



Взаимодействие смежных уровней осуществляется через интерфейс. Интерфейс определяет услуги, которые нижний уровень предоставляет верхнему, и способ доступа к ним. Поэтому каждому уровню одного компьютера "кажется", что он непосредственно взаимодействует с таким же уровнем другого компьютера.

Далее описывается каждый из семи уровней модели OSI и определяются услуги, которые они предоставляют смежным уровням.

### Прикладной уровень

Уровень 7, *прикладной* (Application), — самый верхний уровень модели OSI. Он представляет собой окно для доступа прикладных процессов к сетевым услугам. Этот уровень обеспечивает услуги, напрямую поддерживающие приложения пользователя, такие, как программное обеспечение для передачи файлов, доступа к базам данных электронная почта. Нижележащие уровни поддерживают задачи, выполняемые на *прикладном уровне*. *Прикладной уровень* управляет общим доступом к сети, потоке данных и обработкой ошибок.

### Представительский уровень

Уровень 6, *представительский* (Presentation), определяет формат, используемый для обмена данными между сетевыми компьютерами. Этот уровень можно назвать переводчиком. На компьютере-отправителе данные, поступившие от *прикладного уровня* на этом этапе переводятся в общепонятный промежуточный формат. На компьютере-получателе на этом уровне происходит перевод из промежуточного формата в тот, который используется *прикладным уровнем* данного компьютера. *Представительский уровень* отвечает за преобразование протоколов, трансляцию данных, их шифрование, смену или преобразование применяемого набора символов (кодировочной таблицы) и расширение графических команд. *Представительский уровень*, кроме того, управляет сжатием данных для уменьшения передаваемых битов. На этом

уровне работает утилита, называемая редиректором (redirector). Ее назначение — переадресовать операции ввода/вывода к ресурсам сервера.

### **Сеансовый уровень**

Уровень 5, *сеансовый* (Session), позволяет двум приложениям на разных компьютерах устанавливать, использовать и завершать соединение, называемое сеансом. На этом уровне выполняются такие функции, как распознавание имен и защита, необходимые для связи двух приложений в сети. *Сеансовый уровень* обеспечивает синхронизацию между пользовательскими задачами посредством расстановки в потоке данных контрольных точек (checkpoints). Таким образом, в случае сетевой ошибки, потребуется заново передать только данные, следующие за последней контрольной точкой. На этом уровне выполняется управление диалогом между взаимодействующими процессами, т.е. регулируется, какая из сторон осуществляет передачу, когда, как долго и т.д.

### **Транспортный уровень**

Уровень 4, *транспортный* (Transport), обеспечивает дополнительный уровень соединения — ниже *сеансового уровня*. *Транспортный уровень* гарантирует доставку пакетов без ошибок, в той же последовательности, без потерь и дублирования. На этом уровне сообщения переупаковываются: длинные разбиваются на несколько пакетов, а короткие объединяются в один. Это увеличивает эффективность передачи пакетов по сети. На *транспортном уровне* компьютера-получателя сообщения распаковываются, восстанавливаются в первоначальном виде, и обычно посылается сигнал подтверждения приема. *Транспортный уровень* управляет потоком, проверяет ошибки и участвует в решении проблем, связанных с отправкой и получением пакетов.

### **Сетевой уровень**

Уровень 3, *сетевой* (Network), отвечает за адресацию сообщений и перевод логических адресов и имен в физические адреса. Одним словом, исходя из конкретных сетевых условий, приоритета услуги и других факторов здесь определяется маршрут от компьютера-отправителя к компьютеру-получателю. На этом уровне решаются также такие задачи и проблемы, связанные с сетевым трафиком, как коммутация пакетов, маршрутизация и перегрузки. Если сетевой адаптер маршрутизатора не может передавать большие блоки данных, посланные компьютером-отправителем, на *сетевом уровне* эти блоки разбиваются на меньшие. А *сетевой уровень* компьютера-получателя собирает эти данные в исходное состояние.

### **Канальный уровень**

Уровень 2, *канальный*, осуществляет передачу кадров (frames) данных от  *сетевого уровня*  к *физическому*. Кадры — это логически организованная структура, в которую можно помещать данные. Канальный уровень компьютера-получателя упаковывает "сырой" поток битов, поступающих от *физического уровня*, в кадры данных.

На рис. 4.3 представлен простой кадр данных, где идентификатор отправителя-адрес компьютера-отправителя, а идентификатор получателя — адрес компьютера получателя. Управляющая информация используется для маршрутизации, а также указывает на тип пакета и сегментацию. Данные — собственно передаваемая информация. CRC (остаток избыточной циклической суммы) — это сведения, которые

помогут выявить ошибки, что, в свою очередь, гарантирует правильный прием информации.

### Простой кадр данных

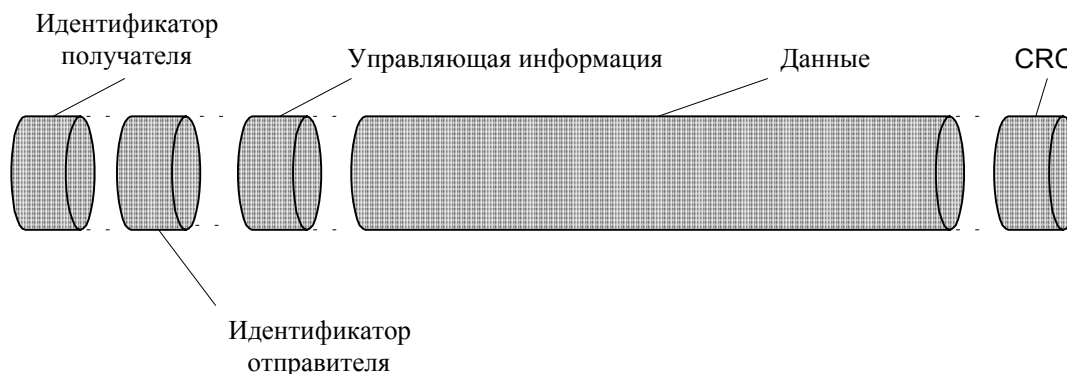


Рис.4.3

Канальный уровень (Data link) обеспечивает точность передачи кадров между компьютерами через физический уровень. Это позволяет *сетевому уровню* считать передачу данных по сетевому соединению фактически безошибочной.

Обычно, когда *канальный уровень* посылает кадр, он ожидает со стороны получателя подтверждения приема. *Канальный уровень* получателя проверяет наличие возможных ошибок передачи. Кадры, поврежденные при передаче, или кадры, получение которых не подтверждено, посылаются вторично.

### Физический уровень

Уровень 1, *физический*, — самый нижний в модели OSI. Этот уровень осуществляет передачу неструктурированного, "сырого" потока битов по физической среде (например, по сетевому кабелю). Здесь реализуются электрический, оптический, механический и функциональный интерфейсы с кабелем. Физический уровень также формирует сигналы, которые переносят данные, поступившие от всех вышележащих уровней. На этом уровне определяется способ соединения сетевого кабеля с платой сетевого адаптера, в частности, количество контактов в разъемах и их функции. Кроме того, здесь определяется способ передачи данных по сетевому кабелю.

*Физический* (Physical) уровень предназначен для передачи битов (нулей и единиц) от одного компьютера к другому. Содержание самих битов на данном уровне значения не имеет. Этот уровень отвечает за кодирование данных и синхронизацию битов, гарантируя, что переданная единица будет воспринята именно как единица, а не как ноль. Наконец, *физический уровень* устанавливает длительность каждого бита и способ перевода бита в соответствующие электрические или оптические импульсы, передаваемые по сетевому кабелю.

## 4.2. IEEE Project 802

В конце 70-х годов, когда ЛВС стали восприниматься в качестве потенциального инструмента для ведения бизнеса, IEEE пришел к выводу: необходимо определить для них стандарты. В результате был выпущен Project 802, названный в соответствии с годом и месяцем своего издания (1980 год, февраль).

Хотя публикация стандартов IEEE опередила публикацию стандартов ISO, оба проекта велись приблизительно в одно время и при полном обмене информацией, что и привело к рождению двух совместимых моделей.

Project 802 установил стандарты для физических компонентов сети — интерфейсных плат и кабельной системы, — с которыми имеют дело *физический и канальный уровни* модели OSI. Итак, эти стандарты, называемые 802-спецификациями, распространяются:

- на платы сетевых адаптеров;
- компоненты глобальных вычислительных сетей;
- компоненты сетей, при построении которых используют коаксиальный кабель и витую пару.

802-спецификации определяют способы, в соответствии с которыми платы сетевых адаптеров осуществляют доступ к физической среде и передают по ней данные. Сюда относятся соединение, поддержка и разъединение сетевых устройств. Стандарты ЛВС, определенные Project 802, делятся на 12 категорий, каждая из которых имеет свой номер.

802.1 – объединение сетей.

802.1 – управление логической связью.

802.3 – ЛВС с множественным доступом, контролем несущей и обнаружением коллизий (Ethernet).

802.4 – ЛВС топологии "шина" с передачей маркера.

802.5 – ЛВС топологии "кольцо" с передачей маркера.

802.6 – сеть масштаба города (Metropolitan Area Network, MAN).

802.7 – Консультативный совет по широкополосной технологии (Broadcast Technical Advisory Group).

802.8 – Консультативный совет по оптоволоконной технологии (Fiber-Optic Technical Advisory Group).

802.9 – Интегрированные сети с передачей речи и данных (Integrated Voice/Data Networks).

802.10 – Безопасность сетей.

802.11 – Беспроводная сеть.

802.12 – ЛВС с доступом по приоритету запроса (Demand Priority Access LAN, 100baseVG-AnyLan).

### 4.3. Драйверы

Драйверы (driver) иногда их называют драйверами устройств (device driver) — это программное обеспечение, позволяющее компьютеру работать с различными устройствами. Даже если некоторое устройство и подключено к компьютеру, операционная-система не сможет взаимодействовать с ним до тех пор, пока не будет установлен в правильно сконфигурирован драйвер этого устройства. Драйвер — программа, которая "говорит" компьютеру, как надо управлять или работать с устройством, чтобы он правильно выполняло все свои функции.

Драйверы существуют почти для каждого типа устройств компьютера и периферии, например:

- устройств ввода (мыши);
- SCSI- и IDE- контроллеров; жестких и гибких дисков;
- устройств мультимедиа (микрофонов, видеокамер, записывающих устройств);
- плат сетевого адаптера;
- принтеров, плоттеров, накопителей на магнитной ленте и т.д.

Сетевые драйверы обеспечивают связь между платами сетевого адаптера и работающими на компьютере редиректорами. Редиректор — это часть сетевого программного обеспечения, которая принимает запросы ввода/вывода, относящиеся к удаленным файлам, и переадресовывает их по сети на другой компьютер. Для установки драйвера часто используется специальная утилита.

Драйверы платы сетевого адаптера располагаются на подуровне *управление доступом к среде* (канальный уровень модели OSI). Подуровень *управление доступом к среде* отвечает за совместный доступ плат сетевого адаптера к *физическому уровню*. Другими словами, драйвер платы сетевого адаптера обеспечивает прямую связь между компьютером и самой платой. Это, в свою очередь, связывает компьютер с сетью. Производители сетевых адаптеров обычно предоставляют драйверы разработчика сетевого программного обеспечения, которые включают их в состав своих продуктов. Производители сетевых операционных систем публикуют списки совместимого оборудования (Hardware Compatibility List, HCL) — списки устройств, драйверы которых протестированы и включены в состав операционной системы. Ввод в действие и управление драйверами подразумевает их установку, настройку, обновление и удаление.

Обычно платы сетевого адаптера имеют несколько параметров, от правильной установки которых зависит корректная работа самого адаптера. Как уже говорилось ранее, настройку параметров можно осуществить перестановкой перемычек или DIP-переключателей. Однако большинство современных плат сетевого адаптера не имеет ни перемычек, ни DIP-переключатели. Они конфигурируются программно — при установке драйверов или после нее.

Время от времени производители вносят в драйверы дополнения или изменения, которые увеличивают производительность сетевых компонентов. Эти изменения распространяются или по почте (зарегистрированным пользователям), или через электронную доску объявлений, или с помощью оперативных служб, таких, как The Microsoft Network (MSN), Internet или CompuServe. Процесс обновления драйверов обычно аналогичен процессу их установки.

## 4.4. Сетевые протоколы

Среди множества протоколов наиболее популярны следующие:

- TCP/IP;
- NetBEUI;
- X.25;
- Xerox Network System (XNS™);
- IPX/SPX и NWLink;
- APP;
- AppleTalk;
- набор протоколов 0 SI;
- DECnet.

*Transmission Control Protocol/Internet Protocol (TCP/IP)* — промышленный стандартный набор протоколов, которые обеспечивают связь в гетерогенной (неоднородной) среде, т.е. обеспечивают совместимость между компьютерами разных типов. Совместимость — одно из основных преимуществ TCP/IP, поэтому большинство ЛВС поддерживает его. Кроме того, TCP/IP предоставляет доступ к ресурсам Интернета, а также маршрутизируемый протокол для сетей масштаба предприятия. Поскольку TCP/IP поддерживая маршрутизацию, он обычно используется в качестве межсетевого протокола. Благодаря своей популярности TCP/IP стал стандартом де-



факто для межсетевого взаимодействия. К другим специально созданным для набора TCP/IP протоколам относятся:

- SMTP (Simple Mail Transfer Protocol) — электронная почта;
- FTP (File Transfer Protocol) — обмен файлами между компьютерами, поддерживающими TCP/IP;
- SNMP (Simple Network Management Protocol) — управление сетью.

TCP/IP имеет два главных недостатка: размер и недостаточная скорость работы. TCP/IP — относительно большой стек протоколов, который может вызвать проблемы у MS-DOS-программ. Однако для таких операционных систем, как Windows NT или Windows 95, размер не является проблемой, а скорость работы сравнима со скоростью протокола IPX.

*NetBEUI* — расширенный интерфейс NetBIOS. Первоначально NetBIOS и NetBEUI были тесно связаны и рассматривались как один протокол. Затем некоторые производители ЛВС так обособили NetBIOS, протокол *сеансового уровня*, что он уже не мог использоваться наряду с другими маршрутизируемыми транспортными протоколами NetBIOS (Network Basic Input/Output System — сетевая базовая система ввода/вывода)-это IBM-интерфейс *сеансового уровня* с ЛВС, который выступает в качестве прикладного интерфейса с сетью. Этот протокол предоставляет программам средства для осуществления сеансов связи с другими сетевыми программами. Он очень популярен, так как поддерживается многими приложениями. NetBEUI — небольшой, быстрый и эффективный протокол *транспортного уровня*, который поставляется со всеми сетевыми продуктами фирмы Microsoft. Он появился в середине 80-х годов в первом сетевом продукте Microsoft — MS®-NET. К преимуществам NetBEUI относятся небольшой размер стека (важно для MS-DOS-приложений), высокая скорость передачи данных по сети и совместимость со всеми сетями Microsoft. Основной недостаток NetBEUI — он не поддерживает маршрутизацию. Это ограничение относится ко всем сетям Microsoft.

*X.25* — набор протоколов для сетей с коммутацией пакетов. Его использовали службы коммутации, которые должны были соединять удаленные терминалы с мейнфреймами.

*Xerox Network System (XNS)* был разработан фирмой Xerox для своих сетей Ethernet. Его широкое использование началось с 80-х годов, но постепенно он был вытеснен протоколом TCP/IP. XNS — большой и медленный протокол, к тому же он применяет значительное количество широковещательных сообщений, что увеличивает трафик сети.

*Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX)* — стек протоколов, используемый в сетях Novell. Как и NetBEUI, относительно небольшой и быстрый протокол. Но, в отличие от NetBEUI, он поддерживает маршрутизацию. IPX/SPX — "наследник" XNS. NWLink — реализация IPX/SPX фирмой Microsoft. Это транспортный маршрутизируемый протокол.

*APPC (Advanced Program-to-Program Communication)* — транспортный протокол фирмы IBM, часть Systems Network Architecture (SNA). Он позволяет приложениям, работающим на разных компьютерах, непосредственно взаимодействовать и обмениваться данными.

*AppleTalk* — собственный стек протоколов фирмы Apple Computer, позволяющий компьютерам Apple Macintosh совместно использовать файлы и принтеры в сетевой среде.

*DECnet* — собственный стек протоколов фирмы Digital Equipment Corporation. Этот набор аппаратных и программных продуктов реализует архитектуру Digital Network Architecture (DNA). Указанная архитектура определяет сети на базе локальных вычислительных сетей Ethernet, сетей FDDI MAN (Fiber Distributed Data Interface Metropolitan Area Network) и глобальных вычислительных сетей, которые используют

средства передачи конфиденциальных и общедоступных данных. DECnet может использовать как протоколы TCP/IP и OSI, так и свои собственные. Данный протокол принадлежит к числу маршрутизируемых. Несколько раз DECnet обновлялся; каждое обновление называется фазой. Текущая версия — DECnet Phase V. Используются как собственные протоколы DEC, так достаточно полная реализация набора протоколов OSI.

## 5. Сетевая архитектура Ethernet

Сетевая архитектура (network architecture) — это комбинация стандартов, топологий и протоколов, необходимых для создания работоспособной сети. Данное занятие, представляющее сетевую архитектуру Ethernet, является первым в серии занятий, посвященных сетевым архитектурам.

Первоначальная версия Ethernet представляла собой систему со скоростью передачи 2,94 Мбит/с и объединяла более 100 компьютеров с помощью кабеля длиной в 1 км. Сеть Ethernet фирмы Xerox имела такой успех, что компании Xerox, Intel Corporation и Digital Equipment Corporation разработали стандарт для Ethernet со скоростью передачи 10 Мбит/с. Сегодня ее рассматривают как спецификацию, описывающую метод кабельного соединения и совместного использования компьютеров и информационных систем.

Спецификация Ethernet выполняет те же функции, что *физический* и *канальный* уровни модели OSI. Эта разработка лежит в основе спецификации IEEE 802.3.

Ethernet — самая популярная в настоящее время сетевая архитектура. Она использует узкополосную передачу со скоростью 10 Мбит/с, топологию "шина", а для регулирования трафика в основном сегменте кабеля — CSMA/CD (рис.5.1).

Среда (кабель) Ethernet является пассивной, т. е. получает питание от компьютера. Следовательно, она прекратит работу из-за физического повреждения или неправильного подключения терминатора.

Сеть Ethernet с топологией "шина"

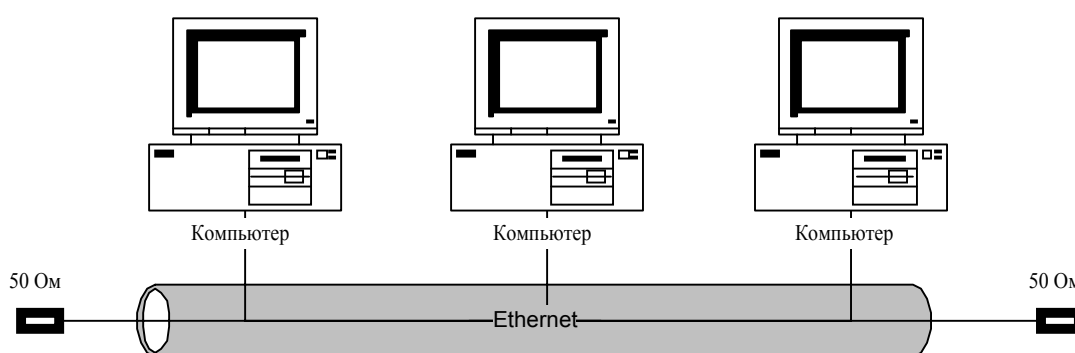


Рис. 5.1

Сеть Ethernet имеет следующие характеристики:

- |                        |                  |
|------------------------|------------------|
| традиционная топология | - линейная шина; |
| другие топологии       | - звезда-шина;   |
| тип передачи           | - узкополосная;  |
| метод доступа          | - CSMA/CD;       |

спецификации - IEEE 802.3;  
 скорость передачи данных - 10 и 100 Мбит/с;  
 кабельная система - толстый и тонкий коаксиальный, UTP.

Ethernet разбивает данные на пакеты (кадры), формат которых отличается от формата пакетов, используемого в других сетях. Кадры представляют собой блоки информации, передаваемые как единое целое. Кадр Ethernet может иметь длину от 64 до 1518 байтов, но сама структура кадра Ethernet использует, по крайней мере, 18 байтов, поэтому размер блока данных в Ethernet —от 46 до 1500 байтов. Каждый кадр содержит управляющую информацию и имеет общую с другими кадрами организацию. Например, передаваемый по сети кадр Ethernet II используется для протокола TCP/IP (рис.5.2). Кадр состоит из частей, которые перечислены в таблице 7.

Кадр данных Ethernet II

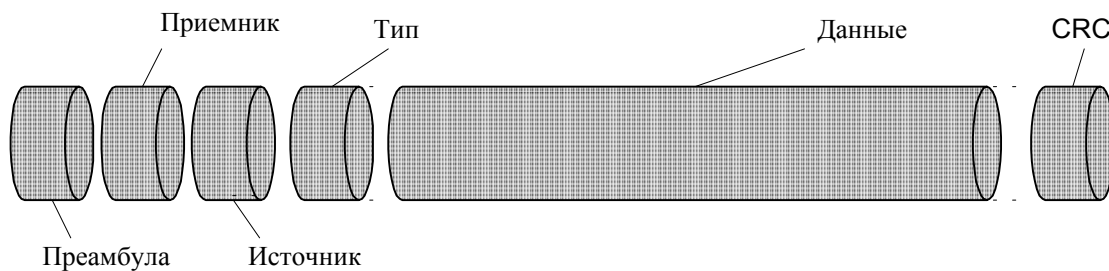


Рис.5.2

Кадр Ethernet II

Таблица 7

Поле кадра	Описание
Преамбула	Отмечает начало кадра
Местоназначение и источник	Указывает адрес источника и адрес приемника
Тип	Используется для идентификации протокола Сетевого уровня (IP или IPX)
Циклический избыточный код (CRC)	Поле информации для проверки ошибок

Сети Ethernet используют различные варианты кабелей и топологий. Далее будут представлены варианты, основанные на спецификации IEEE.

## 5.1. Стандарты IEEE на 10 Мбит/с

В данной главе будут рассмотрены четыре топологии Ethernet со скоростью передачи 10 Мбит/с:

- 10BaseT;
- 10Base2;
- 10Base5
- 10BaseFL.
- 10BaseT

## 10BaseT

В 1990 году IEEE опубликовал спецификацию 802.3 для построения сети Ethernet на основе витой пары. 10BaseT (10 — скорость передачи 10 Мбит/с, Base — узкополосная, T — витая пара) — сеть Ethernet, которая для соединения компьютеров обычно использует неэкранированную витую пару (UTP). Тем не менее и экранированная витая пара (STP) также может применяться в топологии 10BaseT без изменения каких-либо ее параметров.

Большинство сетей этого типа строятся в виде звезды, но по системе передачи сигналов представляют собой шину, как и другие конфигурации Ethernet. Обычно концентратор сети 10BaseT выступает как многопортовый (multiport) репитер и часто располагается в распределительной стойке здания. Каждый компьютер подключается к другому концу кабеля, соединенного с концентратором, и использует две пары проводов: одну — для приема, другую — для передачи.

Максимальная длина сегмента 10BaseT — 100 м. Минимальная длина кабеля — 2,5 м. ЛВС 10BaseT может обслуживать до 1024 компьютеров.

Кабель UTP обеспечивает скорость передачи данных 10 Мбит/с. Изменение конфигурации производится на коммутационных панелях — простым переключением шнура из одного гнезда в другое. Эти изменения не затрагивают другие сетевые устройства (в отличие от сети Ethernet традиционной топологии "шина").

При скорости передачи выше 10 Мбит/с коммутационные панели перед использованием необходимо тестировать. Новейшие концентраторы обеспечивают соединение как для толстого, так и для тонкого коаксиального кабеля Ethernet. При такой реализации сети, присоединив мини-трансивер 10BaseT к порту AUI платы сетевого адаптера, несложно перейти от толстого Ethernet к витой паре (10BaseT).

## 10Base2

В соответствии со спецификацией IEEE 802.3 эта топология называется 10Base2 [10 — скорость передачи 10 Мбит/с, Base — узкополосная передача, 2 — передача на расстояние, примерно в два раза превышающее 100 м (фактическое расстояние 185 м)]. Сеть такого типа ориентирована на тонкий коаксиальный кабель, или тонкий Ethernet, с максимальной длиной сегмента 185 м. Минимальная длина кабеля 0,5 м. Кроме того, существует ограничение на максимальное количество компьютеров, которое может быть размещено на 185-метровом сегменте кабеля, — 30 штук. Компоненты кабеля "тонкий Ethernet": BNC баррел-коннекторы; BNC T-коннекторы; BNC-терминаторы. Сети на тонком Ethernet обычно имеют топологию "шина". Стандарты IEEE для тонкого Ethernet не предусматривают использования кабеля трансивера между T-коннектором и компьютером. Вместо этого T-коннектор располагают непосредственно на плате сетевого адаптера.

BNC баррел-коннектор, соединяя сегменты кабеля, позволяет увеличить его общую длину. Однако использование баррел-коннекторов желательно свести к минимуму, поскольку они ухудшают качество сигнала.

Сеть на тонком Ethernet — экономичный способ реализации сетей для небольших отделений и рабочих групп. Используемый в такого типа сетях кабель: относительно недорогой; прост в установке; легко конфигурируется.

По спецификации IEEE 802.3, сеть на тонком Ethernet может поддерживать до 30 узлов (компьютеров и репитеров) на один кабельный сегмент.

## Правило 5-4-3

Сеть на тонком Ethernet может состоять максимум из пяти сегментов кабеля, соединенных четырьмя репитерами, но только к трем сегментам при этом могут быть подключены рабочие станции. Таким образом, два сегмента остаются зарезервированными для репитеров, их называют межрепитерными связями. Такая конфигурация известна как правило 5-4-3 (рис.5.3).

Правило 5 - 4 - 3

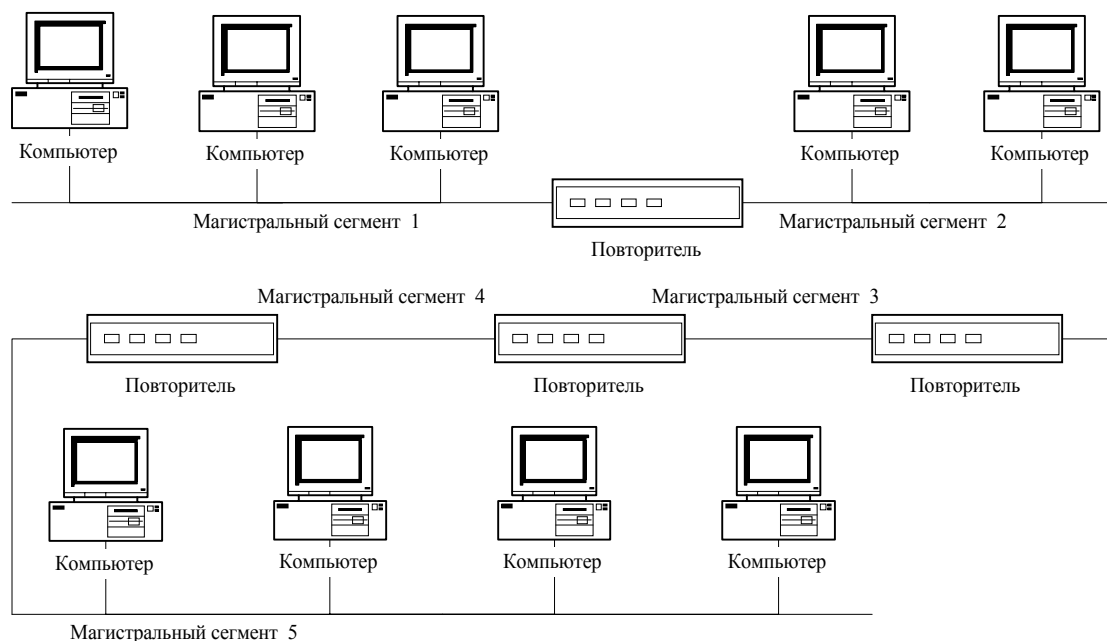


Рис. 5.3

## 10Base5

В соответствии со спецификацией IEEE эта топология называется 10Base5 [10 — скорость передачи 10 Мбит/с, Base — узкополосная передача, 5 — сегменты по 500 м (5 раз по 100 м)]. Известно и другое ее название — стандартный Ethernet. Сети на толстом коаксиальном кабеле (толстый Ethernet) обычно используют топологию "шина". Толстый Ethernet может поддерживать до 100 узлов (рабочих станций, репитеров и т.д.) на магистральный сегмент. Магистраль, или магистральный сегмент, — главный кабель, к которому присоединяются трансиверы с подключенными к ним рабочими станциями и репитерами. Сегмент толстого Ethernet может иметь длину 500 м при общей длине сети 2500 м. Расстояния и допуски для толстого Ethernet больше, чем для тонкого Ethernet.

Компоненты кабельной системы:

- Трансиверы. Трансиверы, обеспечивая связь между компьютером и главным кабелем ЛВС, совмещены с "зубом вампира", соединенным с кабелем.
- Кабели трансиверов. Кабель трансивера (ответвляющийся кабель) соединяет трансивер с платой сетевого адаптера.
- DIX-коннекторы, или AUI-коннекторы. Этот коннектор расположен на кабеле трансивера.
- Коннекторы N-серии (в том числе баррел-коннекторы) и терминаторы N-серии.

Компоненты толстого Ethernet работают так же, как компоненты тонкого Ethernet. Обычно в крупных сетях совместно используют толстый и тонкий Ethernet. Толстый Ethernet хорошо подходит в качестве магистрали, а для ответвляющихся сегментов применяют тонкий Ethernet. Вероятно, Вы помните, что толстый Ethernet имеет медную жилу большего сечения и может передавать сигналы на большие

расстояния, чем тонкий Ethernet. Трансивер соединяется с кабелем "толстый Ethernet", AUI- коннектор кабеля трансивера включается в репитер. Ответвляющиеся сегменты тонкого Ethernet соединяются с репитером, а к ним уже подключаются компьютеры.

## 10BaseFL

10BaseFL (10 — скорость передачи 10 Мбит/с, Base — узкополосная передача, FL—оптоволоконный кабель) представляет собой сеть Ethernet, в которой компьютеры и репитеры соединены оптоволоконным кабелем.

Основная причина популярности 10BaseFL — возможность прокладывать кабель между репитерами на большие расстояния (например, между зданиями). Максимальная длина сегмента 10BaseFL - 2000 м.

## 5.2. Стандарты IEEE на 100 Мбит/с

Новые стандарты Ethernet позволяют преодолеть скорость передачи в 10 Мбит/с. Эти новые возможности разрабатываются для таких приложений, порождающих интенсивный трафик, как:

- CAD (системы автоматического проектирования);
- CAM (системы автоматического производства);
- видео;
- отображение и хранение документов.

Известны два стандарта Ethernet, которые могут удовлетворить возросшие требования:

- 100BaseVG-AnyLAN Ethernet;
- 100BaseX Ethernet (Fast Ethernet).

И Fast Ethernet, и 100BaseVG-AnyLAN работают примерно в пять-десять раз быстрее, чем стандартный Ethernet. Кроме того, они совместимы с существующей кабельной системой 10BaseT. Это означает, что перейти от 10BaseT к этим стандартам достаточно просто и быстро.

## 100VG-AnyLAN

100VG (Voice Grade) AnyLAN - новая сетевая технология, которая сочетает в себе элементы Ethernet и Token Ring. Эта технология, разработанная фирмой Hewlett-Packard, в настоящее время совершенствуется стандартом IEEE 802.12. Спецификация 802.12 — стандарт передачи кадров Ethernet 802.3 и пакетов Token Ring 802.5. Эта технология имеет несколько названий:

- 100VG-AnyLAN;
- 100BaseVG;
- VG;
- AnyLAN.

Перечислим возможности некоторых из существующих в настоящее время спецификаций 100VG-AnyLAN:

- минимальная скорость передачи данных 100 Мбит/с;
- поддержка каскадируемой топологии "звезда" на основе витой пары категории 3, 4 или 5 и оптоволоконного кабеля;
- метод доступа по приоритету запроса (различаются два уровня приоритета: низкий и высокий);
- поддержка средств фильтрации персонально адресованных кадров в концентраторе (для повышения степени конфиденциальности);

- поддержка передачи кадров Ethernet и Token Ring.

Сеть 100VG-AnyLAN строится по топологии "звезда", где все компьютеры соединены с концентратором. Сеть можно расширять, добавляя "дочерние" (child) концентраторы к центральному, "родительскому" (parent), который относится к ним так же, как и к компьютерам, т.е. родительские концентраторы управляют передачей компьютеров соединенных со своими "детьми".

Представленная технология требует использования специальных концентраторов и плат. Кроме того, длина кабеля 100BaseVG, по сравнению с 10BaseT и другими реализациями Ethernet, ограничена: общая длина пары кабелей от концентратора 100BaseVG до компьютеров не может превышать 250 м. Чтобы преодолеть это ограничение, надо использовать специальное оборудование. Ограничения длины кабеля приведут к тому, что для 100BaseVG потребуется больше кабельных стоек, чем для 10BaseT.

## 100BaseX Ethernet

Этот стандарт, иногда называемый Fast Ethernet, является расширением существующего стандарта Ethernet. Он строится на UTP категории 5, использует метод доступа CSMA/CD и топологию "звезда-шина" (подобно 10BaseT), где все кабели подключены к концентратору.

100BaseX включает три спецификации среды передачи:

- 100BaseT4 (UTP категории 3, 4 или 5 с четырьмя парами проводов);
- 100BaseTX (UTP или STP категории 5 с двумя парами проводов);
- 100BaseFX (двухжильный оптоволоконный кабель).

Ethernet может использовать несколько протоколов связи, в том числе и TCP/IP, который хорошо работает в операционной среде UNIX®. Поэтому Ethernet так популярен в научных и образовательных системах.

Производительность Ethernet можно повысить: разделить перегруженный сегмент на два, соединенные мостом или маршрутизатором (рис.5.4). Трафик в каждом сегменте при этом уменьшается, так как меньшее число компьютеров в сегменте пытается осуществить передачу, и время доступа к кабелю сокращается.

Сегментация сети с использованием моста

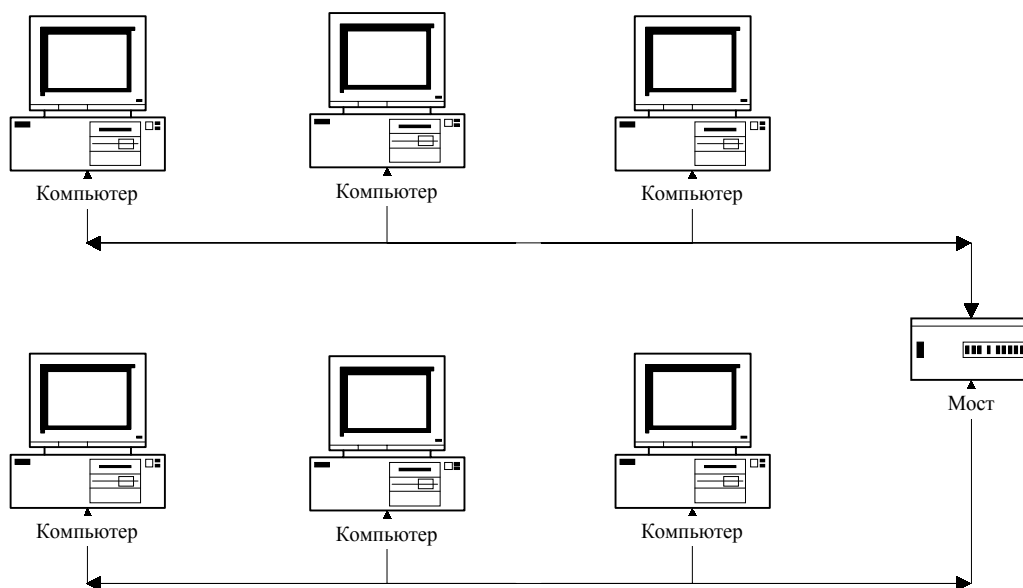


Рис.5.4

Разделение сегмента — удачный ход при подсоединении к сети новых пользователей или установке новых приложений, интенсивно работающих с сетью (например, баз данных и видеоприложений).

Ethernet работает с большинством популярных сетевых операционных систем, в числе: Microsoft Windows 95/98/2000;

Microsoft Windows NT4/5;

Microsoft Windows for Workgroups;

Novell NetWare;

IBM LAN Server;

AppleShare.

Lantastic.

В таблице 8 обобщена спецификация архитектуры Ethernet. В ней приводятся минимальные стандартные требования спецификации IEEE. (Конкретная реализация сетевой архитектуры может отличаться от требований, указанных в таблице.)

Ethernet (IEEE 802.3).

Спецификация архитектуры Ethernet

Таблица 8

	<b>10Base2</b>	<b>10Base5</b>	<b>10BaseT</b>
<b>Топология</b>	Шина	Шина	Звезда-шина
<b>Тип кабеля</b>	RG-58 (тонкий коаксиальный)	Толстый Ethernet; кабель трансивера — экранированная витая пара около 1 см	Неэкранированная витая пара категории 3,4 или 5
<b>Соединение с платой сетевого адаптера</b>	BNC T-коннектор	DIX-коннектор, или AUI- коннектор	RJ-45
<b>Сопротивление терминатора, <math>\Omega</math> (0м)</b>	50	50	Не используется
<b>Волновое сопротивление <math>\Omega</math> (0м)</b>	$50 \pm 2$	$50 \pm 2$	5-115 - для неэкранированной витой пары; 135-165 - для экранированной витой пары
<b>Расстояние (м)</b>	от 0,5 — между компьютерами	от 2,5 - между трансиверами и до 50 - между трансивером и компьютером	до 100 — между трансивером и концентратором
<b>Максимальная длина кабельного сегмента (м)</b>	185	500	100
<b>Максимальное число соединенных сегментов</b>	5 (с использованием четырех репитеров), только к трем сегментам могут быть подключены компьютеры	5 (с использованием четырех репитеров), только к трем сегментам могут быть подключены компьютеры	Не определено
<b>Максимальная общая длина сети (м)</b>	925	2460	Не используется
<b>Максимальное число компьютеров на сегмент</b>	30 (в сети может быть максимум 1024 компьютера)	100	1 (каждая рабочая станция имеет собственный кабель, соединенный с концентратором. Концентратор



			может иметь максимум 12 подсоединенных компьютеров. В сети может быть максимум 1024 компьютера)
--	--	--	---

## 6. Аппаратура для создания больших сетей

Когда организации растут, растут и их сети. В целом локальные сети имеют свойство перерастать начальные проекты. Это становится очевидным, когда:

- трафик сети достиг предела пропускной способности;
- увеличилось время ожидания очередной обработки заданий на печать;
- увеличилось время отклика интенсивно работающих с сетью приложений, таких, как базы данных.

В работе каждого администратора рано или поздно наступает момент, когда он должен увеличить размер сети или улучшить ее производительность. Сети не могут бесконечно расширяться за счет простого добавления новых компьютеров и прокладки дополнительного кабеля. Любая топология или архитектура имеет свои ограничения. Тем не менее существуют устройства, назначение которых — увеличить размер сети в действующей среде. Эти компоненты могут:

- сегментировать локальные сети так, что каждый сегмент становится самостоятельной локальной сетью;
- объединять две локальные сети в одну;
- подключать сеть к другим сетям и компьютерным средам для объединения их и большую разнородную систему.

Итак, к таким устройствам относятся:

- репитеры;
- мосты;
- маршрутизаторы;
- мосты-маршрутизаторы;
- шлюзы.

### 6.1. Репитеры

Сигнал при распространении по кабелю искажается, поскольку уменьшается его амплитуда. Причина этого явления — затухание. В результате, если кабель имеет достаточную длину, затухание может исказить сигнал до неузнаваемости. Однако благодаря репитерам сигналы способны распространяться на большие расстояния.

Репитер работает на *Физическом уровне* модели **OSI**, восстанавливая сигнал и передавая его в другие сегменты (рис.6.1).

Репитер принимает затухающий сигнал из одного сегмента, восстанавливает его и передает в следующий сегмент. Чтобы данные через репитер поступали из одного сегмента в другой, каждый сегмент должен использовать одинаковые пакеты и протоколы Logical Link Control (LLC). Это означает, например, что репитер не позволяет обмениваться данными между сетями 802.3 LAN (Ethernet) и 802.5 LAN (Token Ring).

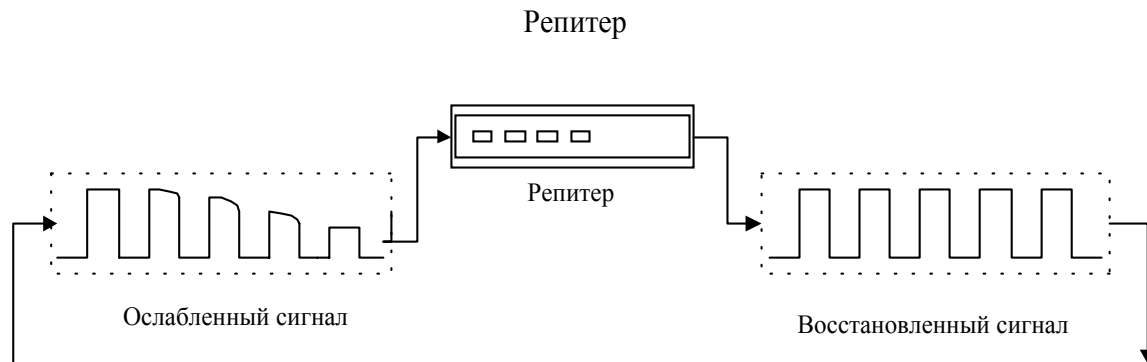


Рис. 6.1

Репитеры не выполняют функции преобразования и фильтрации. Чтобы репитер работал, оба сегмента, им соединяемые, должны иметь одинаковый метод доступа. Наиболее распространенные методы доступа — CSMA/CD и передача маркера. Таким образом, репитер не может соединять сегмент, использующий CSMA/CD, с сегментом, который использует передачу маркера. Другими словами, они не могут транслировать пакеты Ethernet в пакеты Token Ring. Однако репитеры могут передавать пакеты из одного типа физического носителя в другой (рис.6.2). Если репитер имеет соответствующие разъемы, он примет пакет Ethernet, приходящий из сегмента на тонком коаксиальном кабеле, и передаст его в сегмент на оптоволокне.

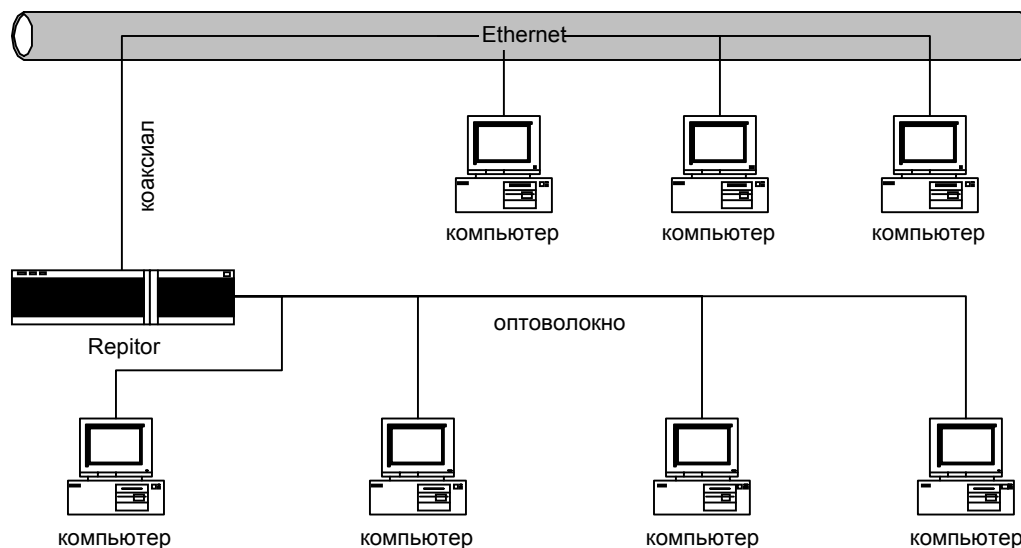


Рис.6.2

Некоторые многопортовые репитеры работают как многопортовые концентраторы, соединяющие различные типы носителя. Ограничения сегментов, в полной мере применимы и к сетям с концентраторами, однако теперь ограничения относятся к каждому отдельному сегменту, а не ко всей сети.

С одной стороны, репитеры — самый дешевый способ расширить сеть. С другой — хотя их использование и является правильным начальным шагом, они остаются

низкоуровневыми компонентами расширения сети. Применение репитеров оправдано, когда при расширении сети необходимо преодолеть ограничения по длине сегмента или по количеству узлов, причем ни один из сегментов не генерирует повышенный трафик, а стоимость — главный фактор.

Репитеры передают из сегмента в сегмент каждый бит данных, даже если данные состоят из искаженных пакетов или из пакетов, не предназначенных для этого сегмента. В результате проблемы одного сегмента могут повредить всем остальным сегментам. Как уже говорилось, репитеры не могут служить фильтром, который ограничивал бы поток пакетов, вызывающих проблемы.

Репитеры, кроме того, будут передавать из сегмента в сегмент и вал ширококестательных пакетов, распространяя их по всей сети. Переизбыток ширококестательных пакетов возникает в сети тогда, когда их количество приближается к ширине полосы пропускания сети. Если устройство отвечает на пакеты, непрерывно циркулирующие по сети, или пакеты постоянно пытаются достичь устройства, которое никогда не отзывается, то производительность сети падает.

Репитеры расширяют возможности сети, разделяя ее на сегменты, тем самым уменьшается количество компьютеров на один сегмент. Репитер:

- соединяет сегменты, использующие одинаковые или разные типы носителя;
- восстанавливает сигнал, тем самым увеличивая дальность передачи;
- функционирует на *Физическом уровне* модели OSI;
- передает весь трафик в обоих направлениях.

Необходимо использовать репитеры, чтобы с наименьшими затратами соединить два сегмента. Не применять репитеры, если:

- сетевой трафик интенсивный;
- в сегментах применяются разные методы доступа;
- необходимо реализовать какой-нибудь метод фильтрации данных.

## 6.2. Мосты

Мост (bridge), как и репитер, может соединять сегменты или локальные сети рабочих групп. Однако, в отличие от репитера, мост также служит для разбиения сети, что помогает изолировать трафик или отдельные проблемы. Например, если трафик одного-двух компьютеров или одного отдела «затопляет» сеть пакетами, уменьшая ее производительность в целом, мост изолирует эти компьютеры или этот отдел. Мосты обычно решают следующие задачи.

- Увеличивают размер сети.
- Увеличивают максимальное количество компьютеров в сети.
- Устраняют узкие места, появляющиеся в результате подключения избыточного числа компьютеров и, как следствие, возрастания графика.

Мосты разбивают перегруженную сеть на отдельные сегменты с уменьшенным трафиком. В итоге каждая подсеть будет работать более эффективно.

Соединяют разнородные физические носители, такие, как витая пара и коаксиальный кабель. Соединяют разнородные сегменты сети, например Ethernet и Token Ring, и переносят между ними пакеты (рис.6.3).

Мосты работают на *Канальном уровне* модели OSI, поэтому им недоступна информация, содержащаяся на более высоких уровнях этой модели. Мосты допускают использование в сети всех протоколов, не отличая при этом один протокол от другого.

### Мост соединяет две сети

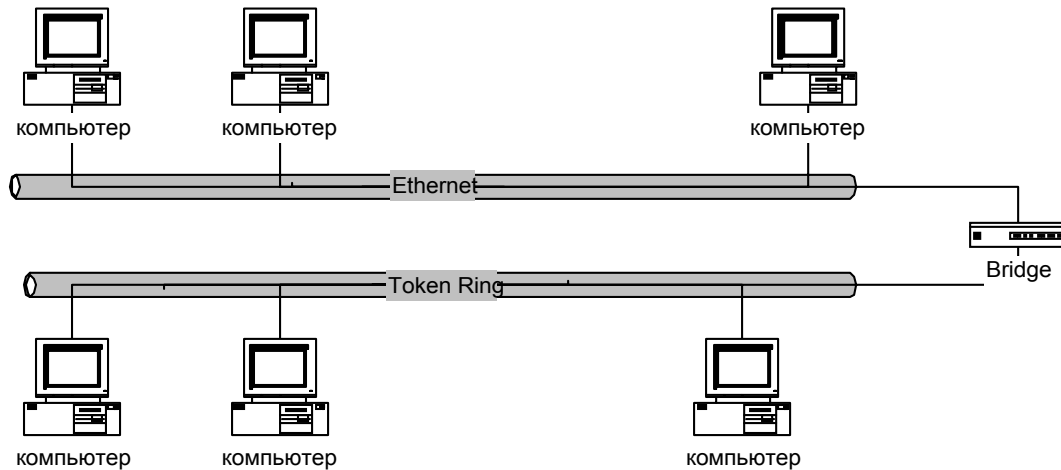


Рис.6.3

Поскольку любые протоколы могут работать через мосты, каждый компьютер должен определять, с какими протоколами он работает. Ранее говорилось, что *Канальный уровень* имеет два подуровня: *Управления логической связью* и *Управления доступом к среде*. Мосты работают на подуровне *Управления доступом к среде*, поэтому иногда называются мостами уровня *Управления доступом к среде*.

Мост уровня *Управления доступом к среде* выполняет следующие действия:

- «слушает» весь график;
- проверяет адреса источника и получателя каждого пакета;
- строит таблицу маршрутизации;
- передает пакеты.

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

Работа моста основана на принципе, согласно которому каждый узел сети имеет собственный адрес — мост передает пакеты, исходя из адреса узла назначения. Можно сказать, что мосты обладают некоторым «интеллектом», поскольку изучают, куда следует направить данные. Когда пакеты передаются через мост, данные об адресах компьютеров сохраняются в оперативной памяти моста. Он использует эти данные для построения таблицы маршрутизации.

В начале работы таблица маршрутизации моста пуста. Затем, когда узлы передают пакеты, адрес источника копируется в таблицу маршрутизации. Имея эти данные, мост изучает расположение компьютеров в сегментах сети.

### Создание таблицы маршрутизации

Итак, мосты строят таблицы маршрутизации на основе адресов компьютеров, которые передавали данные в сеть. Говоря точнее, мосты используют адреса источников — адрес устройства, инициировавшего передачу, — для создания таблицы маршрутизации. Принимая пакет, мост ищет адрес источника в таблице маршрутизации. Если адрес источника не найден, он добавляет его в таблицу. Затем мост сравнивает адреса назначения с базой данных таблицы маршрутизации.

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

Короче говоря, если мост знает о местонахождении узла-адресата, он передает пакет ему. Если адресат неизвестен, мост транслирует пакет во все сегменты.

Благодаря таблице маршрутизации мост способен сегментировать график. Например, компьютер в сегменте 1 (источник) посылает данные другому компьютеру (получателю), который также находится в сегменте 1. Если адрес назначения есть в таблице маршрутизации, мост может определить, что компьютер-получатель расположен и в сегменте 1. Так как и источник, и получатель находятся в сегменте 1, пакет не попадет в сегмент 2. Следовательно, управляя передачей пакетов в другие сегменты, мосты могут использовать таблицы маршрутизации для уменьшения сетевого трафика. Этот процесс называется сегментацией сетевого трафика.

Большая сеть не ограничивается одним мостом. Чтобы объединить несколько малых сетей в одну большую, надо использовать множество мостов. Мосты — эффективное средство для расширения и сегментирования сети, поэтому они часто используются в больших сетях (отдаленные сегменты в таких сетях соединены телефонными линиями). Для соединения двух кабельных сегментов необходим только один мост. Однако и две локальные сети, расположенные на значительном расстоянии друг от друга, можно объединить в одну сеть. С этой целью используют два удаленных моста, которые подключают через синхронные модемы к выделенной телефонной линии.

Так как удаленные сегменты локальных сетей можно объединить через телефонные линии, возникают ситуации, когда несколько локальных сетей объединены более чем по одному маршруту. В этом случае существует вероятность входа пакетов и длительный цикл. Для обработки таких ситуаций служит алгоритм Spanning Tree Algorithm (STA), разработанный IEEE 802.1 Network Management Committee. Используя STA, программное обеспечение может распознать наличие нескольких маршрутов, определить самый эффективный из них, а затем сконфигурировать мост так, чтобы он работал именно с этим маршрутом. Другие маршруты программное обеспечение отключает. Однако, если основной маршрут становится недоступным, отключенные маршруты могут быть вновь активизированы.

### 6.3. Различия между мостами и репитерами

Мосты работают на более высоком уровне модели OSI, чем репитеры. Это означает, что мосты «умней» репитеров и могут учитывать больше особенностей передаваемых данных. Мосты, так же как и репитеры, способны восстанавливать форму сигнала, однако делают это на уровне пакетов, из чего следует: мосты могут передавать пакеты на большие расстояния с использованием разнообразных сред передачи.

Во-первых, мосты, имея все возможности репитеров, позволяют подключать больше узлов. Кроме того, они обеспечивают более высокую производительность сети, чем репитеры. Так как сеть делится на изолированные сегменты, в каждом из них будет меньше компьютеров, конкурирующих за доступ к ресурсам.

Во-вторых, если обширную сеть Ethernet разделить на два сегмента, соединенных мостом, в каждом сегменте сети будет распространяться меньше пакетов,

возникать меньше коллизий, и вся сеть будет работать более эффективно. Хотя каждый сегмент изолирован, мост будет передавать между ними соответствующие пакеты.

Мост может работать как автономное устройство (внешний мост), так и на сервере (внутренний мост), если сетевая операционная система допускает установку на сервере нескольких сетевых плат.

Администраторы сетей широко применяют мосты, потому что они:

- просты в установке и незаметны пользователям;
- обладают высокой гибкостью и адаптируемостью;
- относительно дешевы.

Если для расширения сети принято решение использовать мосты, необходимо учитывать следующие факты:

- мосты обладают всеми возможностями репитеров;
- соединяют два сегмента и восстанавливают сигналы на уровне пакетов;
- функционируют на *Канальном уровне* модели OSI;
- не подходят для распределенных сетей со скоростями передачи менее 56 Кбит/с;
- не могут одновременно использовать несколько маршрутов;
- пропускают все широковещательные сообщения, допуская перегрузку сети;
- считывают адреса источника и получателя каждого пакета;
- пропускают пакеты с неизвестным адресом получателя. Основное назначение мостов:
- соединить два сегмента для увеличения длины сети или количества узлов в ней;
- уменьшить трафик за счет сегментации сети;
- соединить разнородные сети.

## 6.4. Маршрутизаторы

В среде, объединяющей несколько сетевых сегментов с различными протоколами и архитектурами, мосты не всегда гарантируют быструю связь между всеми сегментами. Для такой сложной сети необходимо устройство, которое не только знает адрес каждого сегмента, но и определяет наилучший маршрут для передачи данных и фильтрует широковещательные сообщения. Такое устройство называется маршрутизатором.

Маршрутизаторы (routers) работают на *Сетевом уровне* модели OSI. Это значит, что они могут переадресовывать и маршрутизировать пакеты через множество сетей, обмениваясь информацией (которая зависит от протокола) между отдельными сетями. Маршрутизаторы считывают в пакете адресную информацию сложной сети и, поскольку они функционируют на более высоком по сравнению с мостами уровне модели OSI, имеют доступ к дополнительным данным.

Маршрутизаторы могут выполнять следующие функции мостов:

- фильтровать и изолировать трафик;
- соединять сегменты сети.

Однако маршрутизаторам доступно больше информации, чем мостам, и они используют ее для оптимизации доставки пакетов. В сложных сетях без применения маршрутизаторов обойтись трудно, так как они обеспечивают лучшее (по сравнению с мостами) управление графиком и не пропускают широковещательных сообщений. Маршрутизаторы могут совместно использовать данные о состоянии маршрутов и, основываясь на этой информации, обходить медленные или неисправные каналы связи.

Таблица маршрутизации, которая находится в маршрутизаторах, содержит сетевые адреса. Для каждого протокола, используемого в сети, строится своя таблица. Таблица помогает маршрутизатору определить адреса назначения для поступающих данных. Она включает следующую информацию:

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

Маршрутизатор выбирает наилучший маршрут для данных, сравнивая стоимость и доступность различных вариантов. При этом необходимо помнить, что таблицы маршрутизации существуют и для мостов. Таблица маршрутизации моста содержит адреса подуровня *Управления доступом к среде*, тогда как таблица маршрутизации маршрутизатора содержит номера сетей. Поэтому термин «таблица маршрутизации» имеет разный смысл для мостов и для маршрутизаторов.

Маршрутизаторы требуют специальной адресации: им понятны только номера сетей (что объясняет их обращение друг к другу) и адреса локальных плат сетевого адаптера. К удаленным компьютерам маршрутизаторы обращаться не могут (рис.6.4)

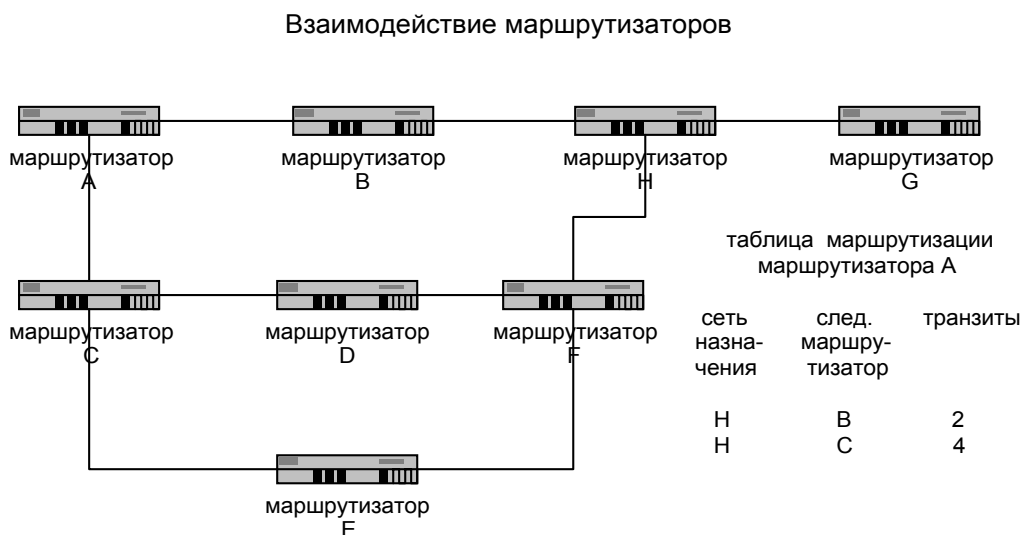


Рис. 6.4.

Маршрутизатор, принимая пакеты, предназначенные для удаленной сети, пересылает их тому маршрутизатору, который обслуживает сеть назначения. В некотором смысле это достоинство, потому что маршрутизаторы могут:

- сегментировать большие сети на меньшие;
- действовать как барьер безопасности между сегментами;
- предотвращать избыток широковещательных сообщений (такие сообщения не передаются).

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

Воспринимая только адресованные сетевые пакеты, маршрутизаторы будут препятствовать проникновению в сеть некорректных пакетов. Таким образом,

благодаря фильтрации некорректных данных и широковещательных пакетов, маршрутизаторы уменьшают нагрузку на сеть. Адрес узла назначения маршрутизаторы не проверяют; они «смотрят» только на адрес сети. Маршрутизаторы будут пропускать информацию только в том случае, если известен адрес сети. Эта возможность — контролировать данные, передаваемые через маршрутизатор, — позволяет уменьшить трафик между сетями и использовать ли связи эффективнее, чем это делают мосты.

Ориентируясь на схему адресации маршрутизаторов, администраторы всегда могут разбить одну большую сеть на множество отдельных сетей, между которыми как барьер будут действовать маршрутизаторы: не пропуская все пакеты подряд и обрабатывая далеко не каждый пакет. Благодаря этому может быть значительно уменьшен трафик в сети и время ожидания пользователей.

## Маршрутизируемые протоколы

С маршрутизаторами работают не все протоколы. Протоколы, работающие с маршрутизаторами, называются маршрутизируемыми. К ним относятся:

- DECnet;
- IP;
- IPX;
- OSI;
- XNS;
- DDP (AppleTalk).

К немаршрутизируемым протоколам относятся:

- LAT (Local Area Transport — протокол корпорации Digital Equipment Corporation);
- NetBEUI.

Существуют маршрутизаторы, которые в одной сети могут работать с несколькими протоколами (например, с IP и DECnet).

В отличие от мостов, маршрутизаторы могут не только использовать несколько активных маршрутов между сегментами сети, но и выбирать между ними. Поскольку маршрутизаторы способны соединить сегменты с абсолютно разными схемами упаковки данных и доступа к носителю, им часто будут доступны несколько путей. Это значит, что, если какой-нибудь маршрутизатор «откажется» работать, данные все равно будут передаваться по другим маршрутам.

Маршрутизатор может «прослушивать» сеть и определять, какие ее части сильнее загружены. Он устанавливает также количество транзитов между сегментами сети. Используя эту информацию, маршрутизатор выбирает маршрут передачи данных. Если один путь перегружен, он укажет альтернативный. Подобно мостам, маршрутизаторы строят таблицы маршрутизации и используют их в алгоритмах маршрутизации (routing algorithm). В качестве примера можно предложить следующие алгоритмы,

OSPF (Open Shortest Path First) — алгоритм маршрутизации на основе состояния канала. Алгоритмы состояния канала управляют процессом маршрутизации и позволяют маршрутизаторам быстро реагировать на изменения в сети. Маршрутизация на основе состояния канала использует алгоритм Dijkstra для вычисления маршрутов с учетом количества транзитов, скорости линии, графика и стоимости. Алгоритмы состояния канала более эффективны и создают меньший трафик по сравнению с дистанционно-векторными алгоритмами. Этот факт может быть важен для маршрутизируемой среды большого размера с множеством связей между сегментами распределенной сети. Протокол TCP/IP поддерживает OSPF.



RIP (Routing Information Protocol) — дистанционно-векторные алгоритмы маршрутизации. Протоколы TCP/IP и IPX поддерживают RIP.

NLSP (NetWare Link Services Protocol) — алгоритм маршрутизации на основе состоянии канала. Протокол IPX поддерживает NLSP.

### Типы маршрутизаторов

Маршрутизаторы подразделяются на два основных типа (табл. 9).

- Статические (static).

Статические маршрутизаторы требуют, чтобы администратор вручную создал и сконфигурировал таблицу маршрутизации, а также указал каждый маршрут.

- Динамические (dynamic).

Динамические маршрутизаторы автоматически определяют маршруты и поэтому требуют минимальной настройки и конфигурирования. Они сложнее статических, так как анализируют информацию от других маршрутизаторов и для каждого пакета принимают отдельное решение о маршруте передачи через сеть.

Статические и динамические маршрутизаторы

Таблица 9

Статические маршрутизаторы	Динамические маршрутизаторы
Ручная установка и конфигурирование всех маршрутов	Ручное конфигурирование первого маршрута. Автоматическое определение дополнительных сетей и маршрутов.
Всегда используют один и тот же маршрут, определяемый элементом таблицы	Могут выбирать маршрут на основе таких факторов, как стоимость и величина сетевого трафика
Используемый маршрут жестко задан и не всегда является наилучшим	Могут принимать решения о передаче пакетов по альтернативным маршрутам
Считаются более безопасными, так как администратор сам указывает каждый маршрут	Защита может быть улучшена за счет ручного конфигурирования с целью фильтрации обнаруженных адресов сетей и предупреждения передачи данных через них.

## 6.5. Различия между мостами и маршрутизаторами

Мосты и маршрутизаторы путают даже опытные сетевые инженеры, поскольку, на первый взгляд, они выполняют одни и те же действия:

- передают пакеты между сетями;
- передают данные по каналам глобальных сетей.

Как определить, когда надо использовать мост, а когда — маршрутизатор? Мост, работающий на подуровне Управления доступом к среде Канального уровня модели OSI, «видит» только адрес узла. Точнее: в каждом пакете мост ищет адрес узла подуровня Управления доступом к среде. Если мост распознает адрес, он оставляет пакет в локальном сегменте или передает его в нужный сегмент. Если адрес мосту неизвестен, он пересылает пакет во все сегменты, исключая тот, из которого пакет прибыл.

Пересылка пакетов — это ключ к пониманию функций мостов и их отличий от маршрутизаторов. При использовании мостов передаваемые широковещательные пакеты следуют ко всем компьютерам всех портов моста, исключая порт, через который они прибыли. Иначе говоря, каждый компьютер во всех сетях получит широковещательный пакет. В малых сетях это, скорее всего, и не будет иметь сколько-

нибудь существенного значения, однако большая сеть может генерировать мною широковещательных сообщений, что замедлит работу сети (несмотря на фильтрацию по адресам).

Маршрутизатор, работающий на Сетевом уровне, принимает во внимание больше информации, чем мост: он определяет и то, что нужно передавать, и то, куда нужно передавать. Маршрутизатор распознает не только адрес, как это делает мост, но и `тип` протокола. Кроме того, маршрутизатор может установить адреса других маршрутизаторов и решить, какие пакеты каким маршрутизаторам переадресовать.

Мост может распознать только один путь между сетями. Маршрутизатор среди нескольких возможных путей определяет самый лучший на данный момент. Рассмотрим рис. 6.5. Маршрутизатор А должен переслать данные маршрутизатору D. Однако он может направить пакеты маршрутизатору С или В, и данные все равно будут доставлены маршрутизатору D. Маршрутизаторы способны оценить оба пути и выбрать среди них лучший.

- Необходимо запомнить главные характеристики мостов и маршрутизаторов. Они помогут различать эти устройства, а в конкретной ситуации одному из них отдавать предпочтение. Мост распознает только локальные адреса подуровня Управления

Распознавание маршрутов маршрутизаторами

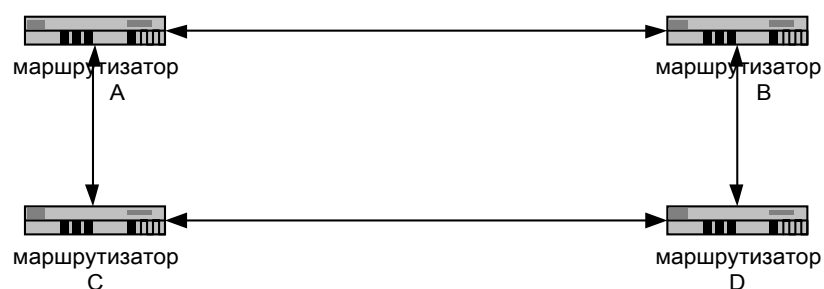


Рис.6.5

доступом к среде (адреса плат сетевого адаптера компьютеров в подключенных к нему сегментах).

- Маршрутизаторы распознают адреса сетей.
- Мост распространяет пакеты с неизвестным ему адресом получателя по всем направлениям, а все пакеты с известным адресом передает только через соответствующий порт.
- Маршрутизатор работает только с маршрутизируемыми протоколами.
- Маршрутизатор фильтрует адреса. Пакеты определенных протоколов он передает по определенным адресам (другим маршрутизаторам).

## 6.6. Мосты-маршрутизаторы

Мост-маршрутизатор (`brouter` или `switch`), о чем и говорит его название, соединил лучшие свойства моста и маршрутизатора. Мост-маршрутизатор для одних протоколов может действовать как маршрутизатор, а для других — как мост. Мосты-маршрутизаторы могут выполнять следующие функции:

- маршрутизировать отдельные маршрутизируемые протоколы;
- функционировать как мост для немаршрутизируемых протоколов;

- обеспечивать более экономичное и более управляемое взаимодействие сетей по сравнению с отдельными мостами и маршрутизаторами.

Маршрутизаторы объединяют сети и обеспечивают фильтрацию пакетов. Они также определяют наилучший маршрут для передачи данных. Маршрутизаторы работают на Сетевом уровне модели OSI.

Необходимо использовать маршрутизаторы, чтобы:

- соединить две сети и ограничить трафик;
- разделить административные участки сетей.

Если решено применять маршрутизаторы, нужно убедиться, что в сети не используются немаршрутизируемые протоколы.

## 6.7. Шлюзы

Шлюзы (gateways) обеспечивают связь между различными архитектурами и средами. Они переупаковывают и преобразуют данные, передаваемые из одной среды в другую, чтобы каждая среда могла понимать данные других сред. В частности, шлюз переупаковывает информацию в соответствии с требованиями системы назначения; изменяет формат сообщения, чтобы прикладная программа на принимающей стороне могла распознать данные. Например, шлюзы электронной почты (такие, как X.400) принимают сообщение в одном формате, транслируют его и пересылают в формате X.400, используемом получателем, и наоборот. Шлюз связывает две системы, которые используют разные:

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

Шлюзы связывают гетерогенные сети, например Microsoft Windows NT Server с SNA (Systems Network Architecture фирмы IBM). Они изменяют формат данных, чтобы сделать их понятными прикладной программе на принимающей стороне.

Шлюзы создаются для выполнения конкретного типа задач, т. е. для конкретного типа преобразования данных. Часто они и называются в соответствии с типом специализации (например, Windows NT Server To SNA Gateway).

Шлюз принимает данные из одной среды, удаляет старый протокольный стек и переупаковывает их в протокольный стек системы назначения. Обработав данные, шлюз выполняет следующие операции:

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

Некоторые шлюзы используют все семь уровней модели OSI, однако обычно шлюзы выполняют преобразование протоколов на Прикладном уровне. Впрочем, это целиком зависит от типа шлюза.

Главное назначение шлюзов — осуществлять связь между персональными компьютерами и средой мэйнфреймов или мини-компьютеров (рис. 6.6). Шлюз соединяет локальную сеть персональных компьютеров с мэйнфреймами или системами мини-компьютеров, которые не могут непосредственно взаимодействовать с персональными компьютерами.

В локальной сети один компьютер обычно выделяется на роль шлюза. Специальные прикладные программы на настольных компьютерах через компьютер-шлюз получают доступ к мэйнфрейму. Таким образом, пользователи могут работать с

ресурсами мэйнфрейма так же просто, как будто эти ресурсы принадлежат их собственным компьютерам.

Обычно роль шлюзов в сети выполняют выделенные серверы. При этом может быть задействована значительная часть мощности сервера, потому что решаются такие ресурсоемкие задачи, как преобразование протоколов. Если сервер-шлюз используется и для других целей, необходимо установить на нем адекватный объем оперативной памяти и мощный центральный процессор, в противном случае производительность сервера снизится.

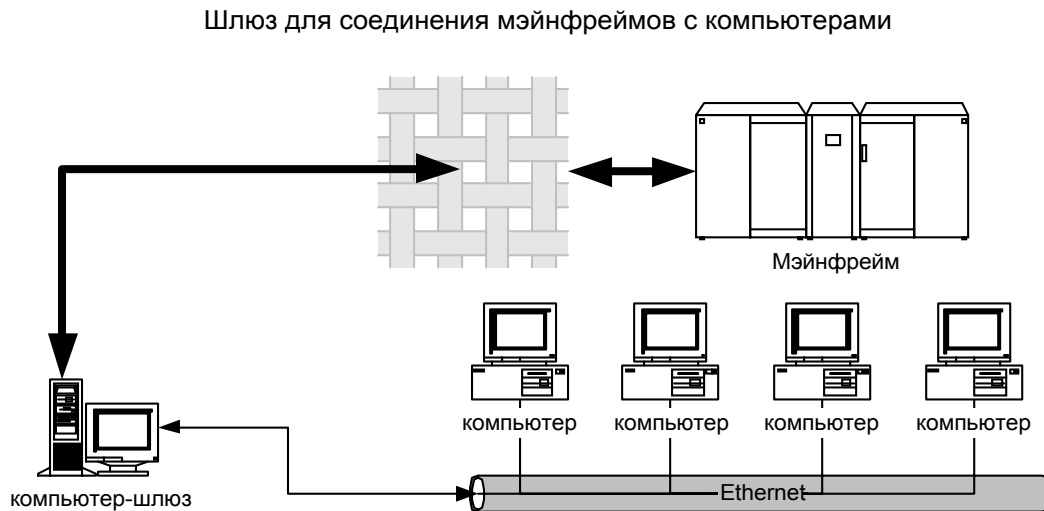


Рис. 6.6

Шлюзы имеют некоторые особенности:

- не создают высокой нагрузки для межсетевых каналов связи;
- эффективно выполняют специфичные задачи.

Шлюзы осуществляют преобразование протоколов и данных. Они имеют некоторые ограничения:

- предназначены для выполнения одной конкретной задачи;
- могут работать с низкой производительностью;
- стоимость шлюзов достаточно высока.

Используйте шлюзы, если необходимо установить связь между различными средами.

Когда возникает необходимость расширить локальную сеть, администратор должен учесть множество факторов. Вопрос заключается не только в прокладке нового кабеля, установке дополнительных компьютеров, принтеров и т. д. Каждая топология имеет свои ограничения. Существуют различные компоненты, среди которых (в зависимости от типа сети и требуемых масштабов ее расширения) надо выбрать наиболее подходящие для увеличения размеров и производительности именно Вашей сети.

Использование репитеров — самый дешевый метод расширить сеть, однако их функции ограничиваются соединением двух сегментов. Они не подходят, если велик трафик сети. Мосты могут выполнять те же функции, что и репитеры, однако они уменьшают трафик каждого сегмента. Вы можете использовать мосты для соединения сетей с разным типом среды передачи.

Маршрутизаторы соединяют сети и обеспечивают фильтрацию. Они могут определить самый целесообразный маршрут для передачи данных. Однако не все протоколы являются маршрутизируемыми. Маршрутизаторы наилучшим образом подходят для

соединения удаленных сетей, так как перелают по коммуникационному каналу только те данные, которые предназначены для этих сетей.

Мосты-маршрутизаторы соединяют в себе достоинства мостов и маршрутизаторов. Они могут действовать как маршрутизаторы для маршрутизируемых протоколов, и как мосты — для немаршрутизируемых протоколов.

Шлюзы применяются для соединения двух различных сред. Они связывают системы, которые используют различные коммуникационные протоколы, структуры и форматы данных, языки и архитектуры. Шлюзы специализированы для конкретного типа обмена данных и обычно являются выделенными серверами сети.

## **7. Стандарты передачи данных в глобальных вычислительных сетях**

Локальные сети обладают множеством достоинств, однако они имеют и физические ограничения размеров. Так как одна ЛВС не может решить всех проблем организации, имеющей несколько рабочих площадок, необходима связь между удаленными ЛВС.

Благодаря таким компонентам, как мосты и маршрутизаторы, а также услугам коммуникационных компаний, ЛВС может быть расширена от локального масштаба до сети, которая охватывает целые области, страны и даже всю планету. Такую сеть называют глобальной вычислительной сетью (ГВС).

Для конечного пользователя ГВС выглядит так же, как и локальная сеть. Фактически, если глобальная сеть должным образом реализована, не будет никаких видимых различий между ней и локальной сетью. Большинство глобальных сетей представляет собой комбинацию локальных сетей и коммуникационного оборудования, которые соединены коммуникационными каналами. Они называются каналами связи. В качестве каналов связи ГВС могут выступать:

- сети с коммутацией пакетов;
- оптоволоконный кабель;
- микроволновые передатчики;
- спутниковые каналы;
- системы кабельного телевидения на коаксиальном кабеле.

Приобретение, реализация и самостоятельное обслуживание каналов связи ГВС, так же как и глобальных телефонных сетей, — слишком дорогая и сложная задача для большинства организаций. Поэтому обычно они арендуют их у поставщиков коммуникационных услуг.

Для связи между локальными сетями может использоваться одна из следующих технологий передачи данных:

- аналоговая;
- цифровая;
- коммутация пакетов.

### **7.1. Аналоговая связь**

Всемирная сеть, которую использует телефон и которая может быть доступна компьютерам, называется общедоступной коммутируемой телефонной сетью (ОКТС). В вычислительной среде ОКТС, предлагающую коммутируемые телефонные линии для передачи речи, можно считать одним большим каналом связи ГВС.

Изначально ОКТС была создана для передачи речи, поэтому она обладает низкой скоростью, и, как уже известно, для связи по коммутируемым аналоговым линиям необходимы модемы, которые также не увеличивают скорость (рис.7.1).

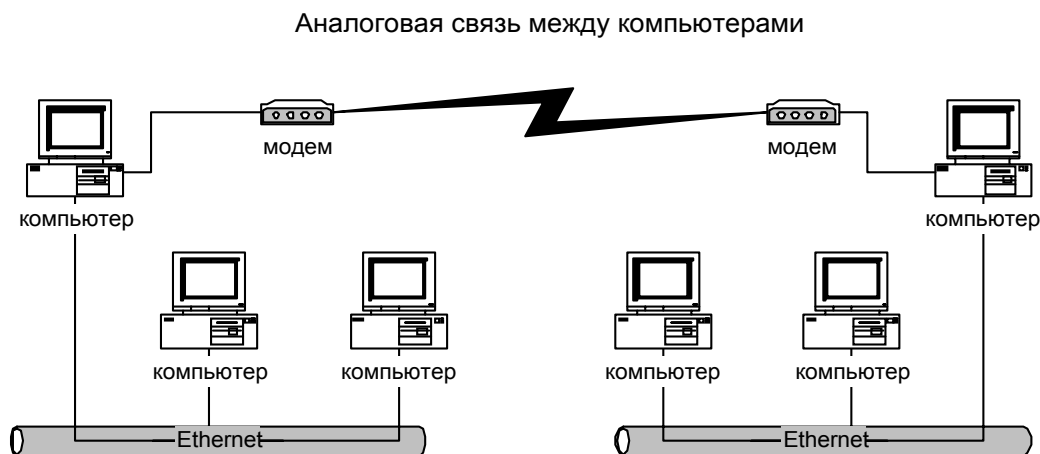


Рис.7.1

Поскольку ОКТС — сеть с коммутацией каналов, качество соединения неустойчиво. Каждый сеанс связи полностью зависит от качества каналов, скоммутированных для этого конкретного сеанса. На длинных расстояниях, например между странами, качество каналов может резко изменяться от сеанса к сеансу. Поставщики телефонных услуг предлагают телефонные линии различных типов качества (табл.10):

Линии ОКТС

Таблица 10

Тип линии	Описание
1	Передача речи (основной тип)
2	Передача речи с некоторым контролем качества
3	Передача речи/радио с подавлением помех
4	Передача данных со скоростью 1200 бит/с
5	Передача данных (основной тип)
6	Передача речи и данных по магистральным линиям
7	Передача речи и данных по частотным линиям
8	Передача речи и данных по магистралям между компьютерами
9	Передача речи и видео
10	Application relays (ретрансляция приложений)

В отличие от коммутируемых линий, которые нужно организовывать для каждого сеанса, выделенные (или арендуемые) аналоговые линии обеспечивают готовый к немедленному использованию коммуникационный канал. Арендуемая телефонная линия быстрее и надежнее, чем коммутируемое соединение. Правда, она несколько дороже, так как коммуникационная компания выделяет ресурсы этому каналу вне зависимости от того, используется линия или нет.

Выбор линии зависит от нескольких факторов:

- времени использования линии;
- стоимости услуг;
- возможности получить более высокую или более устойчивую скорость на линии с подавлением помех;
- необходимости круглосуточного непрерывного соединения.

Если канал будет использоваться редко, подойдут и коммутируемые линии. Если надежная связь нужна в течение месяцев, качество коммутируемой линии уже не сможет удовлетворять требуемым условиям передачи данных.

## 7.2. Цифровая связь

В некоторых случаях аналоговые линии обеспечивают приемлемое качество связи. Однако стоит обсудить альтернативу, если обмен данными с ГВС настолько интенсивен, что время на их передачу делает аналоговую связь неэффективной и чересчур дорогой.

Организации, которым необходим более быстрый и надежный по сравнению с аналоговыми линиями метод передачи данных, могут обратиться к линиям цифровой службы передачи данных (DDS). DDS обеспечивает синхронное соединение «точка-точка» на скоростях 2,4; 4,8; 9,6 и 56 Кбит/с. Цифровые каналы «точка-точка» — это выделенные линии, которые предоставляются некоторыми телекоммуникационными компаниями. Коммуникационная компания гарантирует полнодуплексную полосу пропускания при постоянном соединении двух точек.

Основная причина популярности цифровых линий в том, что они обеспечивают передачу данных, практически на 99 процентов свободную от ошибок. Цифровые линии доступны в различных формах, включая DDS, T1, T3, T4 и Switched 56.

Так как служба DDS использует цифровую связь, она не нуждается в модемах. Вместо этого данные от моста или маршрутизатора DDS передает через устройство, которое называется устройством обслуживания канала/устройством обработки данных (CSU/DSU). Оно преобразует стандартные цифровые сигналы, генерируемые компьютером, в биполярные цифровые сигналы, применяемые для синхронной связи. Это устройство содержит также электронные схемы для защиты сети поставщика услуг DDS.

### Цифровой канал T1

T1, вероятно, самый распространенный тип цифровой линии, применяемой для высокоскоростной связи. Эта технология «точка-точка» использует две пары проводов (одна пара — для передачи, другая — для приема), чтобы осуществлять полнодуплексную передачу данных на скорости 1,544 Мбит/с. T1 используется для передачи оцифрованной речи, данных и видеосигналов.

Линии T1 относятся к самым дорогим каналам связи ГВС. Абоненты, которым не нужна или не по карману полная полоса пропускания линии T1, могут работать с одним или несколькими каналами T1 со скоростью 64 Кбит/с, известными как Fractional T-1 (FT-1).

В некоторых странах услуги T1 пока недоступны, вместо них часто предлагаются линии E1. E1 очень похожа на T1, однако работает на скорости 2.048 Мбит/с.

T1, разработанная Bell Labs, использует технологию мультиплексирования (multiplexing) (уплотнения каналов). Несколько сигналов от различных источников накапливаются в устройстве, которое называется мультиплексор (multiplexer), и передаются по одному кабелю. На принимающей стороне происходит демультиплексирование (demultiplexing) данных в начальную форму. Этот метод появился тогда, когда стало не хватать пропускной способности телефонных кабелей, которые могли поддерживать только один сеанс связи на линию. Решение, названное

«T-Carrier network», позволило Bell Labs передавать одновременно множество разговоров по одной линии.

Канал T1 может переносить 1,544 Мбит данных в секунду. T1 делит ее на 24 канала и опрашивает каждый канал 8000 раз в секунду. Используя этот метод, T1 одновременно передает по двухпроводной паре 24 потока данных.

При каждом обращении к каналу передается 8 битов. Так как все каналы опрашиваются 8 000 раз в секунду, скорость передачи составляет 64 Кбит/с. Этот стандарт скорости называется DS-0. Скорость 1,544 Мбит/с известна как DS-1.

Канал со скоростью DS-1 может быть мультиплексирован, что обеспечит более высокие скорости передачи, обозначаемые DS-1C, DS-2, DS-3 и DS-4 (см. таблицу 11).

Каналы DS				Таблица 11
Обозначение	Система передачи	Число каналов в T-1	Число речевых каналов	Скорость передачи данных (М бит/с)
DS-0	Не применяется		1	0,064
DS-1	T1	1	24	1,544
DS-1C	T-1C	2	48	3,152
DS-2	T2	4	96	6,312
DS-3	T3	28	672	44,736
DS-4	T4	168	4032	274,760

Медные провода могут применяться для каналов T 1 и T2. Однако T3 и T4 требуют высокочастотной среды передачи, например микроволновой или оптоволоконной.

## Цифровой канал T3

Выделенные линии T3 и Fractional T-3 обеспечивают передачу речи и данных со скоростью от 6 Мбит/с до 45 Мбит/с. Они обладают наибольшей пропускной способностью среди всех общедоступных сегодня линий. T3 и FT-3 разработаны для скоростной передачи значительных массивов данных между двумя точками. Линия T3 может заменить несколько линий T1.

## Switched 56

Switched 56 — это коммутация каналов по линии DDS 56 Кбит/с. Как местные, так и междугородные телефонные компании широко предлагают эту службу коммутируемой связи локальных сетей, передающую данные со скоростью 56 Кбит/с. Преимущество Switched 56 в том, что она используется только по мере необходимости, избавляя тем самым от обязательной оплаты выделенной линии. На каждом абоненте, работающем с этой службой, надо установить устройство CSU/DSU, которое может соединиться с другим абонентом Switched 56.



### 7.2.1. Сети с коммутацией пакетов

Технология передачи пакетов очень быстрая, удобная и надежная, поэтому она используется для передачи данных на большие расстояния, например между городами, областями или странами. Сети, передающие пакеты от множества различных пользователей по многим доступным маршрутам, называются сетями с коммутацией пакетов (в соответствии с методом упаковки и пересылки данных).

Исходный блок данных разбивается на пакеты, и каждый пакет снабжается адресом получателя и другой служебной информацией. Этот принцип обеспечивает независимую передачу каждого пакета по сети. При коммутации пакетов каждый пакет передается промежуточными станциями по оптимальному на текущий момент маршруту между источником и получателем.

Каждый пакет передается совершенно независимо. Два пакета из одного исходного блока данных могут следовать до адресата по различным маршрутам. Хотя каждый пакет продвигается собственным путем, а пакеты, составляющие сообщение, могут достигать адресата в разное время или с измененной очередностью, принимающий компьютер все равно точно восстановит исходное сообщение.

Коммутаторы (switches) направляют пакеты по доступным соединениям и маршрутам. Иногда такие сети называют «связью каждого с каждым». Промежуточные станции сети анализируют каждый пакет и передают его по оптимальному маршруту, доступному в данный момент.

Пакеты имеют небольшой размер. Если при передаче возникает ошибка, то передать еще раз маленький пакет проще, чем большой. Кроме того, маленькие пакеты занимают коммутаторы в течение очень короткого промежутка времени. Сети с коммутацией пакетов высокопроизводительны и эффективны. Чтобы управлять процессом маршрутизации, а также сборкой и разборкой пакетов, такие сети должны обладать некоторой «интеллектуальностью» компьютеров и программного обеспечения, которые контролируют доставку. Сети с коммутацией пакетов дешевле, так как предлагают высокоскоростную связь с оплатой только передачи пакета, а не времени соединения.

### Виртуальные каналы связи

Большая часть сетей с коммутацией пакетов использует виртуальные (virtual) каналы. Это каналы, состоящие из цепочки логических связей между передающим и принимающим компьютером. В отличие от постоянного физического соединения между двумя станциями, полоса пропускания в виртуальных каналах предоставляется истребованию. Соединение устанавливается после того, как оба компьютера обменялись информацией и «договорились» о параметрах связи, с которыми будет работать канал. В эти параметры входят максимальный размер сообщения и путь пересылки данных.

Надежность будет гарантирована, если для виртуальных каналов установить следующие параметры связи:

- наличие подтверждений;
- управление потоком данных;
- контроль ошибок.

Виртуальные каналы могут существовать как в течение короткого диалога (временные), так и всего времени работы компьютеров, которые обмениваются данными (постоянные).

При использовании коммутируемых виртуальных каналов (SVC) передача данных по сети между конечными компьютерами осуществляется по конкретному маршруту. Пока не прервано соединение, канал будет получать сетевые ресурсы, а маршрут-право на существование. Иногда такие каналы называют «связью одного со многими»,

Постоянный виртуальный канал (PVC) подобен выделенной линии: существует всегда, однако пользователь платит только за время работы с ним.

### 7.2.2. Беспроводной канал связи

Одним из возможных вариантов реализации высокоскоростного канала связи между удаленными пользователями могут являться радиомодемы. В качестве практической реализации можно предложить радиоадаптеры ARLAN и узконаправленные антенны канадской фирмы Aironet Wireless Communications, Inc.

Краткая характеристика:

- диапазон рабочих частот 902 – 928 и 2412 - 2483 MHz
- скорости приема/передачи: 2048 Kbps
- мощность сигнала 100 mW
- максимальная дальность связи 85км.
- сертифицировано Министерством Связи России
- кодирует передаваемую информацию по методу растянутого спектра (spread spectrum)

Уникальность этого оборудования заключается еще и в высокой помехоустойчивости и живучести (широкополосной помехо-защищенный сигнал низкой амплитуды, DSSS), высокой избыточности (11-кратный) и защищенности передаваемого сигнала. Высокая защищенность сотовой радиосети достигается двумя степенями защиты:

1-я степень. Ключ доступа, используемый для алгоритма формирования сигнала. Без знания этого ключа расшифровать информацию невозможно.

2-я степень. Маркерное кольцо - специально разработанная технология сотовой архитектуры радиосети. Доступ к соте может получить только легальный пользователь

Применяемые радиоадаптеры ARLAN 655 вставляются в свободный разъем ISA любого персонального компьютера. Полностью совместимы с кабельными сетями. Поддерживают сотовую и "все-со-всеми" конфигурации вычислительных сетей. Обеспечивает интеллектуальную фильтрацию пакетов по сетевым адресам, протоколам и содержимому. Радиотехнические параметры, дальность связи и пропускная способность совпадают с соответствующими параметрами [ARLAN 630-900 и 630-2400](#). Поставляется с драйверами NDIS, ODI, Packet, TCP/IP.

## 8. Передовые технологии связи в глобальных вычислительных сетях

Рассмотрим основные особенности каждой из следующих технологий высокоскоростной передачи информации, обеспечивающих широкую полосу пропускания данных:

- X.25;
- Frame relay (ретрансляция кадров);
- ATM (Asynchronous Transfer Mode – режим асинхронной передачи данных);
- ISDN (Integrated Services Digital Network — цифровая сеть комплексных услуг);

- FDDI (Fiber Distributed Data Interface – волоконно-оптический интерфейс передачи данных );
- SONET (Synchronous Optical Network – синхронная оптоволоконная сеть);
- SMDS (Switched Multimegabit Data Service – коммутируемая служба для передачи мультимегабитных данных).

## 8.1. X.25

X.25 — это набор протоколов для сетей с коммутацией пакетов. Сети с коммутацией пакетов были созданы на основе служб коммутации, первоначальное назначение которых — подключить удаленные терминалы к мейнфреймам и хост-системам. Чтобы обеспечить оптимальную маршрутизацию сети с коммутацией пакетов, X.25 использует доступные в данный момент коммутаторы, линии связи и маршруты. Поскольку эти компоненты (коммутаторы, линии связи и маршруты) часто меняются (они зависят от текущих сетевых условий), на схемах их иногда обозначают в виде облаков. Облака указывают на изменчивую ситуацию, на то, что в сети нет стандартного набора линий связи.

Первые сети X.25 осуществляли передачу данных по телефонным линиям. При передаче по этой ненадежной среде возникало большое количество ошибок, поэтому в X.25 были введены мощные средства их контроля. Из-за повторных передач (при наличии ошибок) сеть работала довольно медленно.

Современный набор протоколов X.25 определяет интерфейс между хост-компьютером синхронного пакетного режима или другим устройством и общедоступной сетью передачи данных (PDN) через выделенный, или арендуемый, канал связи. Этот интерфейс в действительности является интерфейсом терминального оборудования- коммуникационного оборудования (DTE/DCE).

Примерами терминального оборудования (DTE) могут быть:

- хост-компьютер с интерфейсом X.25;
- устройство сборки/разборки пакетов (PAD), которое принимает асинхронный поток символов от низкоскоростного терминала и собирает их в пакеты для передачи по сети. PAD также разбирает пакеты, принятые из сети, чтобы посимвольно передать данные на терминал;
- мост между PDN и ЛВС или ГВС.

Для всех этих примеров компонентом DCE интерфейса DTE/DCE служит общедоступная сеть передачи данных (PDN). На рисунке 7.24 Вы видите примеры DTE.

## 8.2. Frame relay

С переходом межсетевых коммуникаций к цифровым и оптоволоконным средам появляются новые технологии, которые требуют меньшего уровня контроля ошибок (по сравнению с ранними аналоговыми средами).

Frame relay — это усовершенствованная быстрая технология коммутации пакетов переменной длины. Разработчики этой технологии отбросили многие функции учета и контроля X.25, которые уже не нужны в надежной, защищенной оптоволоконной среде.

Frame relay — система «точка-точка», использующая PVC для передачи кадров переменной длины Канального уровня OSI. Данные из локальной сети передаются по цифровой арендуемой линии к коммутатору данных сети frame relay. Далее они проходят по сети frame relay до сети назначения.

Сети frame relay пользуются широкой популярностью, поскольку намного быстрее других коммутирующих систем выполняют базовые действия по коммутации пакетов. Высокую скорость в frame relay обеспечивает использование PVC, благодаря чему известен весь маршрут между конечными точками. Поэтому устройства frame relay избавлены от некоторых постоянных процедур: фрагментации, восстановления, выбора оптимального маршрута.

Кроме того, сети frame relay могут выделять абонентам необходимую полосу пропускания, что позволяет им передавать данные практически любой типа.

Для передачи данных по сети с использованием технологии frame relay необходим совместимый с frame relay маршрутизатор или мост. Маршрутизатор frame relay должен иметь как минимум один ГВС-порт для подключения к сети frame relay и еще один порт — для локальной сети.

### 8.3. Асинхронный режим передачи (АТМ)

Асинхронный режим передачи (АТМ) — это усовершенствованная технология коммутации пакетов, которая обеспечивает высокоскоростную передачу пакетов фиксированной длины через широкополосные и узкополосные локальные или глобальные сети. АТМ способна передавать:

- речь;
- данные;
- факсимильные сообщения;
- видео реального времени;
- аудиосигналы качества CD;
- мультимегабитные потоки данных.

В 1988 году комитет ССИТТ определил АТМ как часть широкополосной цифровой сети комплексных услуг (BISDN). Благодаря хорошей производительности и гибкости технология АТМ в ближайшие годы окажет непосредственное влияние на развитие сетевой связи. Она одинаково пригодна как для локальных, так и для глобальных сетей и может передавать данные с очень высокой скоростью (от 66 Мбит/с до 622 Мбит/с и даже выше).

АТМ — это широкополосный метод ретрансляции ячеек, при котором данные передаются ячейками фиксированной длины (по 53 байта) (рис.8.1). Ячейки содержат 48 байтов — собственно передаваемые данные и 5 дополнительных байтов — заголовок АТМ. Например, передавая 1000-байтный пакет, АТМ разобьет его на 21 кадр и поместит каждый кадр в ячейку. Результат — передача стандартных, единообразных пакетов.

## Пакет и ячейка АТМ

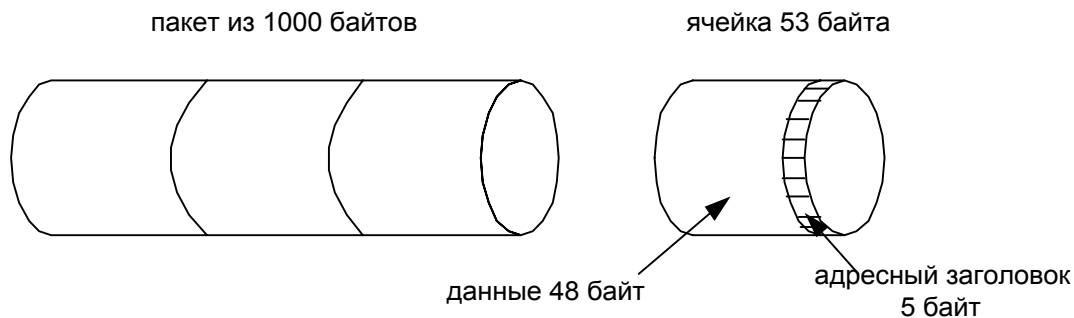


Рис. 8.1

Сетевое оборудование может коммутировать, маршрутизировать и перемещать пакеты фиксированного размера быстрее, чем пакеты произвольного размера. А ячейки стандартного размера позволяют более эффективно использовать буферы и сокращают время на свою обработку. Одинаковый размер ячеек, кроме того, упрощает планирование необходимой полосы пропускания.

Теоретически пропускная способность АТМ может достичь 1,2 Гбита в секунду. В настоящее время, однако, скорость АТМ ограничивается скоростью оптоволоконного кабеля, которая не превышает 622 Мбит/с. Большинство серийных плат АТМ будет передавать данные со скоростью около 155 Мбит/с.

Например, АТМ со скоростью 622 Мбит/с передает полное собрание Британской энциклопедии (The Encyclopedia Britannica), включая иллюстрации, меньше чем за одну секунду. Если передавать эти же данные, используя модем на 2400 бод, операция займет больше двух дней.

Примерно с одинаковой скоростью АТМ может работать как в ЛВС, так и в глобальных сетях. Для реализации АТМ на больших пространствах обычно прибегают к услугам коммуникационных компаний, в частности AT&T и US Sprint™. При этом создается однородная среда, которая сводит «на нет» концепцию медленных ГВС и различие технологий в локальных и глобальных сетях.

В настоящее время компоненты АТМ производятся узким кругом поставщиков. Вся аппаратура в сети АТМ должна быть АТМ-совместимой. Поэтому реализация АТМ в существующих условиях требует массовой замены оборудования. Это одна из причин сравнительно медленного распространения АТМ.

Однако, по мере развития рынка АТМ, многие производители будут предлагать:

- маршрутизаторы и коммутаторы для построения глобальной среды передачи данных;
- магистральные устройства для объединения всех ЛВС крупных предприятий;
- коммутаторы и адаптеры для подключения настольных компьютеров, где выполняются мультимедиа-приложения, к высокоскоростным сетям АТМ.

Технология АТМ не ограничена конкретным типом среды передачи. Она может использовать существующие среды передачи, разработанные для других коммуникационных систем, в том числе:

- коаксиальный кабель;
- витую пару;
- оптоволоконный кабель.

Однако эти традиционные среды передачи в своей настоящей форме не поддерживают всех возможностей ATM. Организация, которая называется ATM Forum, рекомендует следующие физические интерфейсы для ATM:

- FDDI (100 Мбит/с);
- Fiber Channel (155 Мбит/с);
- OC3 SONET (155 Мбит/с);
- T3 (45 Мбит/с).

К другим интерфейсам относятся frame relay и X.25.

Коммутаторы ATM — это многопортовые устройства, которые могут функционировать как любой из следующих компонентов:

- концентратор для передачи данных между компьютерами внутри сети;
- маршрутизатор, предназначенный для высокоскоростной передачи данных в удаленные сети.

В некоторых сетевых архитектурах (таких, как Ethernet и Token Ring) одномоментно может вести передачу только один компьютер. ATM использует коммутаторы в качестве мультиплексоров, позволяя нескольким компьютерам одновременно передавать данные. ATM — это относительно новая технология, требующая специального оборудования и исключительно широкой полосы пропускания. Современная технология глобальных сетей не обеспечивает полосы пропускания, необходимой для поддержки ATM в реальном времени. Приложения, работающие с речью или видео, быстро перегрузили бы самые современные среды передачи и привели бы в отчаяние пользователей, пытающихся наладить нормальную деятельность. Кроме того, реализация и поддержка ATM требуют определенного уровня знаний и опыта, которых пока еще не хватает у большинства пользователей.

## 8.4. Цифровая сеть комплексных услуг (ISDN)

Цифровая сеть комплексных услуг (ISDN) — это спецификация межсетевой цифровой связи, предназначенная для передачи:

- речи;
- данных;
- графики.

Разработчики ISDN ставили целью соединить дома и предприятия по медным телефонным проводам. Согласно первоначальному плану, реализация ISDN предусматривала преобразование существующих телефонных каналов связи из аналоговых в цифровые.

Служба Basic Rate ISDN (BRI) разделяет полную полосу пропускания на три канала передачи данных. Два из них имеют скорость 64 Кбит/с, а третий — 16 Кбит/с,

Каналы на 64 Кбит/с известны под названием В-каналов. Они могут передавать речь, данные и изображения. Медленный канал, на 16 Кбит/с, называется D-каналом. D-канал предназначен для передачи управляющих сигналов и служебной информации. Служба BRI называется 2B+D.

Компьютер, подключенный к службе ISDN, может совместно использовать оба В-канала для пересылки данных с общей скоростью 128 Кбит/с. Если обе конечные станции поддерживают сжатие данных, может быть достигнута и значительно большая пропускная способность.

Служба Primary Rate ISDN (PRI) использует всю полосу пропускания линии T1, обеспечивая 23 В-канала на 64 Кбит/с и один D-канал также со скоростью 64 Кбит/с. D-канал используется только для управления и передачи служебной информации.

Если Вы планируете использовать ISDN, прежде всего (в зависимости от необходимой пропускной способности) выберите подходящую службу: Basic Rate или Primary Rate. Сегодня ISDN повсеместно вытесняет общедоступную коммутируемую телефонную сеть и, по существу, является коммутируемой службой. Она не предназначена для круглосуточной непрерывной связи двух точек (как T1) или для предоставления полосы пропускания по требованию (как Frame relay).

## 8.5. Оптический интерфейс передачи данных (FDDI)

Fiber Distributed Data Interlace (FDDI) — это спецификация, которая описывает высокоскоростную (100 Мбит/с) сеть с передачей маркера топологии «кольцо» на основе оптоволоконка. Она была разработана комитетом ANSI X3T9.5 и опубликована в 1986 году. Спецификация FDDI предназначалась для высокопроизводительных компьютеров, которым не хватало полосы пропускания существующих архитектур — 10 Мбит/с Ethernet или 4 Мбит/с Token Ring.

FDDI обеспечивает высокоскоростную связь между соями различных типов. Она может применяться в сетях городского масштаба (MAN): соединяет сети в черте города высокоскоростным оптоволоконным кабелем. Однако длина кольца имеет ограничения до 100 км (62 мили), так что, по сути, FDDI не может претендовать на роль технологии построения ГВС.

Сети в высокопроизводительных средах используют FDDI для соединения больших компьютеров и мини-компьютеров в традиционных компьютерных залах. Иногда их называют «back-end» сетями. Такие сети обслуживают очень интенсивную (по сравнению с интерактивной связью) передачу файлов. При связи с мэйнфреймом мини-компьютеру или персональному компьютеру часто необходимо постоянное использование носителя в реальном времени. Более того, иногда им необходим исключительный доступ к носителю в течение продолжительного времени.

FDDI выступает в качестве магистральной сети, к которой можно подключить другие ЛВС малой производительности. Подключать все оборудование фирмы, обрабатывающее информацию, к одной ЛВС — не самое мудрое решение. Это может перегрузить сеть, а сбой какого-либо компонента может полностью остановить обработку данных на предприятии.

Локальные сети, которым необходима высокая скорость передачи данных и относительно большая полоса пропускания, часто используют каналы связи FDDI. Это сети, состоящие из инженерных рабочих станций и компьютеров, на которых выполняются интенсивно использующие сеть приложения (такие, как видеообработка, системы автоматизированного проектирования и системы управления производством).

Любое учреждение, нуждающееся в высокоскоростной сетевой обработке, может установить FDDI. Ведь даже в офисах коммерческих фирм производство графики для презентаций и других документов нередко вызывает перегрузку сети.

Хотя FDDI использует стандартную систему передачи маркера, существуют некоторые различия между этим процессом в сети FDDI и в сети 802.5. В сети FDDI компьютер может захватить маркер на определенное (ограниченное) время и за этот промежуток передать столько кадров, сколько успеет. Завершив передачу, компьютер освобождает маркер.

Поскольку компьютер, завершив передачу, сразу же освобождает маркер, могут остаться несколько кадров, одновременно циркулирующих по кольцу. Это объясняет, почему сеть FDDI обеспечивает более высокую производительность, чем сеть Token Ring, которая позволяет циркулировать только одному кадру.

При топологии «двойное кольцо», которая поддерживает 500 компьютеров при общей длине кольца в 100 км, FDDI функционирует со скоростью 100 Мбит/с.

FDDI основана на технологии совместного использования сети. Это означает, что одновременно могут передавать данные несколько компьютеров. Хотя FDDI работает со скоростью 100 Мбит/с, технология совместного использования сети может стать причиной ее перегрузки. Например, если 10 компьютеров начнут передавать данные со скоростью 10 Мбит/с каждый, общий поток будет равен 100 Мбит/с. А при передаче видеoinформации или данных мультимедиа среда передачи (даже со скоростью 100 Мбит/с) тем более окажется потенциальным узким местом системы.

FDDI использует систему передачи маркеров в двойном кольце. Трафик в сети FDDI состоит из двух похожих потоков, движущихся в противоположных направлениях по двум кольцам (рис. 8.2). Одно кольцо называется основным, а другое — дополнительным.

FDDI топологии «двойное кольцо» Обычно данные передаются только по основному кольцу. Если в основном кольце происходит сбой, сеть автоматически переконфигурируется, и данные начинают передаваться по дополнительному кольцу в противоположном направлении.

Одно из достоинств топологии двойного кольца — избыточность. Одно кольцо используется для передачи данных, а второе является резервным. Если возникает проблема, например отказ кольца или разрыв кабеля, сеть автоматически переконфигурируется и продолжает передачу.

Существуют и ограничения: общая длина кабеля объединенных колец не должна превышать 200 км; к нему не может быть подключено более 1000 компьютеров. К тому же, поскольку второе кольцо предназначено для защиты от сбоев, эти показатели должны быть поделены на два. Следовательно, каждая сеть FDDI должна быть ограничена 500 компьютерами и 100 км кабеля. И наконец, как минимум через каждые 2 км должен быть установлен репитер.

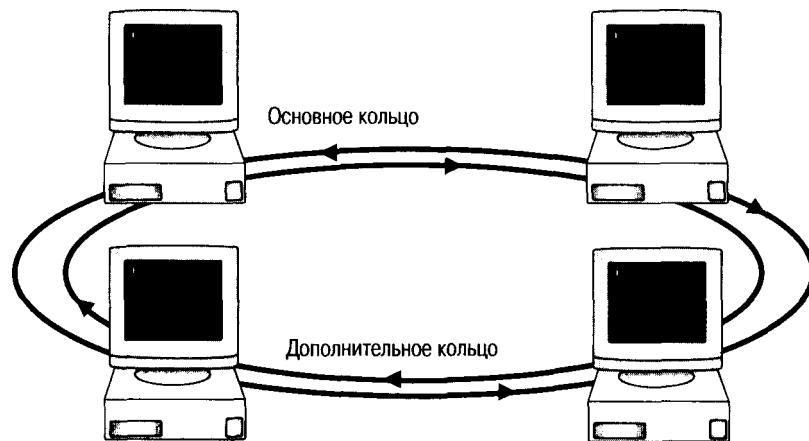


Рис. 8.2

Компьютеры могут подключаться к одному или к обоим кольцам FDDI. Компьютеры, подключенные к обоим кольцам, называются станциями Класа А, а компьютеры, подключенные только к одному кольцу, — станциями Класа В (рис 8.3).

Если происходит сбой в сети, станции Класа А участвуют в переконфигурировании сети, а станции Класа В—не участвуют.

В сети FDDI компьютеры могут иметь соединение «точка-точка» с концентратором. Это означает, что сеть FDDI реализована с топологией «звезда-кольцо». Такое решение имеет свои достоинства:

- упрощается решение проблем;
- используются возможности интеллектуальных концентраторов для сетевого управления и поиска неисправностей.



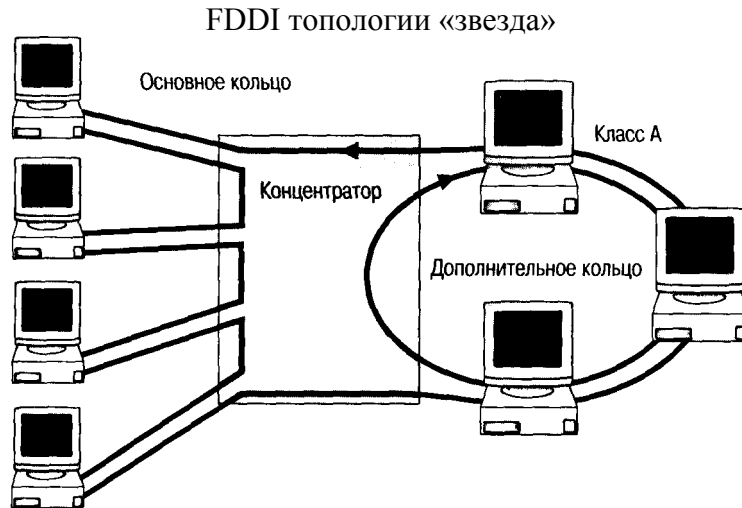


Рис. 8.3

Все компьютеры в сети FDDI отвечают за мониторинг передачи маркера. Чтобы изолировать серьезные сбои в кольце, FDDI использует метод, который называется «испускание маяка» (beaconing). Суть его такова. Компьютер, обнаруживший сбой, начинает посылать в сеть сигнал — маяк. Он будет посылать маяк до тех пор, пока не примет сигнал (маяк) от соседнего компьютера, предшествующего ему в кольце. Этот процесс продолжается до тех пор, пока в кольце не останется единственного компьютера (того, что находится непосредственно за неисправным участком), который все еще посылает маяк.

Когда посылающий маяк компьютер в конце концов примет свой собственный маяк, он «догадается», что неисправность была устранена, восстановит маркер, и сеть вернется к нормальному функционированию.

Основная среда передачи для FDDI — оптоволоконный кабель. Это означает, что сеть FDDI:

- нечувствительна к электромагнитным помехам;
- обладает повышенной защищенностью (оптоволоконный кабель не излучает сигнал, который может быть перехвачен, и к нему очень трудно незаметно подключиться);
- передает данные на большие расстояния без использования репитера.

FDDI может также работать на медных проводах, этот вариант называют CDDI, однако такое решение имеет серьезные ограничения по дальности.

## 8.6. Синхронная оптическая сеть (SONET)

Synchronous Optical Network (SONET) — представитель современных систем, которые реализуют преимущества оптоволоконной технологии. Она обеспечивает передачу данных со скоростью более гигабита в секунду. Сети, основанные на этой технологии, могут передавать речь, данные и видео.

SONET — это стандарт оптического транспорта, сформулированный ассоциацией Exchange Carriers Standards Association (ECSA) института American National Standard Institute (ANSI). Кроме того, стандарт SONET был включен в рекомендации Synchronous Digital Hierarchy комитета CCITT, известного также под названием International Telecommunications Union (ITU). Этот комитет устанавливает стандарты для международных телекоммуникационных систем.

Выстраивая иерархию передачи, основанной на волоконной оптике, SONET определяет уровни оптической несущей (OC) и сигналы синхронного транспорта (STS), эквивалентные электрическим.

SONET использует основную скорость передачи данных STS-1, эквивалентную 51,84 Мбит/с. Однако достижимы и более высокие уровни, соответствующие произведению базовой скорости на целое число. Например, STS-3 — это утроенный STS-1 ( $3 \times 51,84 = 155,52$  Мбит/с). STS-12 имел бы скорость  $12 \times 51,84 = 622,08$  Мбит/с.

SONET отличается достаточно гибкой нагрузочной способностью, благодаря чему он может использоваться как нижележащий транспортный уровень для ATM-ячеек, передаваемых по BISDN. BISDN — это отдельная сеть ISDN, которая обслуживает передачу речи, данных и видео. ATM — это стандарт комитета CCITT, поддерживающий передачу — на основе ячеек — речи, данных, видео и мультимедиа и общедоступной сети на базе BISDN. ATM Forum позиционирует SONET как транспортный уровень для трафика на основе ячеек.

## 8.7. Коммутируемая мультимегабитная цифровая служба (SMDS)

Switched Multimegabit Data Service (SMDS) — коммутируемая служба, которую предлагают некоторые локальные коммуникационные компании. Передача данных осуществляется в диапазоне скоростей: от 1 Мбит/с до 34 Мбит/с при связи «многие со многими». В отличие от выделенной ячеистой сети (сети с множеством активных маршрутов), эта служба может обеспечить широкую полосу пропускания при меньших затратах.

SMDS использует такую же технологию ретрансляции ячеек фиксированной длины, как и ATM. Одна линия SMDS с соответствующей полосой пропускания подключается к локальной несущей и обеспечивает связь между всеми абонентами (без необходимости установки и разрыва соединений). SMDS не занимается проверкой ошибок или управлением потоком данных; эти задачи возлагаются на абонентов.

SMDS совместима со стандартом сети городского масштаба IEEE 802.6, а также с BISDN. Однако SMDS работает на службы управления и объявлений, не определенные в спецификации IEEE 802.6.

Как интерфейс и метод доступа для сети служба SMDS использует Distributed Queue Dual Bus (DQDB). SMDS — это топология «двойная шина», формирующая незамкнутое кольцо.

Существует несколько новых технологий передачи данных, которые могут увеличить производительность глобальных сетей.

X.25 — это набор протоколов для сетей с коммутацией пакетов. Чтобы обеспечить оптимальную маршрутизацию в конкретный момент времени, сеть с коммутацией пакетов X.25 использует любые доступные коммутаторы, каналы связи и маршруты.

Frame relay — это технология коммутации пакетов, разработанная на основе X.25. За счет уменьшенных накладных расходов работает значительно быстрее X.25. Требуется применения совместимых с frame relay маршрутизаторов.

ATM — это широкополосный метод передачи данных ячейками фиксированной длины, равной 53 байта. Еще одна усовершенствованная форма коммутации пакетов. Единообразные кадры маршрутизируются и передаются сетевым оборудованием гораздо быстрее, чем кадры произвольного размера. При наличии необходимых физических интерфейсов ATM может использоваться с любой средой передачи.

Basic Rate ISDN — служба, которая использует цифровой метод передачи. Делит доступную полосу пропускания на два В-канала по 64 Кбит/с и один D-канал на 16 Кбит/с. Служба Primary Rate ISDN имеет 23 В-канала по 64 Кбит/с и один D-канал по 64 Кбит/с.

FDDI — это высокоскоростная сеть с передачей маркера топологии «кольцо», которая использует оптоволоконную среду передачи. Была разработана для высокопроизводительных компьютеров. Используется в средах, которые соединяют такие компоненты, как большие компьютеры и мини-компьютеры в традиционных компьютерных залах; для построения магистральных сетей; для сетей, требующих высокой скорости передачи данных и относительно широкой полосы пропускания; иногда - в высокоскоростных офисных сетях.

SONET — это новая оптоволоконная технология, которая может передавать данные со скоростью, превышающей гигабит в секунду.

SMDS — это коммутируемая служба, которую предлагают некоторые местные коммуникационные компании. Использует такую же технологию ретрансляции кадров фиксированной длины, как и ATM.

## 9. Аппаратные мероприятия по защите данных

К числу бедствий можно отнести все, что влечет за собой потерю данных в сети. Причины бедствий самые разнообразные: от дел рук человеческих до природных катаклизмов, в том числе:

- воровство или вандализм;
- пожар;
- отказы источников питания и скачки напряжения;
- отказы компонентов;
- природные явления, такие, как молнии, наводнения, бури и землетрясения.

### Предупреждение потери данных

Остановка сети, вызванная чрезвычайными причинами, всегда бедствие, всегда серьезное уменьшение производительности. Требуется время на восстановление данных из хранилища резервных копий (если есть резервные копии). Без них последствия будут самыми непредсказуемыми, с огромными финансовыми потерями. Существуют методы и системы, предупреждающие катастрофическую потерю данных:

- резервное копирование на магнитную ленту;
- источники бесперебойного питания (UPS);
- отказоустойчивые системы.

Могут использоваться все эти системы или любая из них, в зависимости от ценности данных и бюджета организации.

### Резервное копирование на магнитную ленту

Наиболее простой и недорогой метод предупредить катастрофическую потерю данных периодическое резервное копирование с последующим хранением копий за пределами организации. Это один из немногих способов гарантировать, что данные остаются в безопасности и пригодны для использования.

Опытные сетевые инженеры знают, что система резервного копирования — первая линия обороны. Надежная стратегия резервирования сводит к минимуму риск потери данных, поддерживая текущую резервную копию в таком состоянии, при котором файлы легко восстанавливаются в случае повреждения оригинальных данных.

Чтобы проводить резервное копирование, необходимо иметь:

- оборудование;
- расписание;
- сотрудника, чья обязанность — реализовать расписание на практике.

Под оборудованием обычно подразумевается один или несколько накопителей на магнитной ленте с комплектом лент (или другое устройство массового хранения данных). Любые расходы в этой области могут оказаться мизерными по сравнению с теми финансовыми потерями, которые вызовет разрушение данных.

## **Система резервного копирования**

Общее правило гласит: если Вы не можете в дальнейшем обойтись без чего-то, сделайте его резервную копию. Выбор объектов для резервного копирования — целые диски, отдельные каталоги или файлы — зависит от того, насколько быстро нужно продолжить работу после потери важных данных, восстановив их. Полное резервное копирование может ускорить восстановление конфигурации диска, однако, если имеются большие объемы данных, требует значительного числа дополнительных магнитных лент. Резервирование отдельных файлов и каталогов потребует меньше лент, однако администратору придется вручную восстанавливать конфигурацию диска. Критические данные должны резервироваться ежедневно, еженедельно или ежемесячно, в зависимости от степени их важности и оттого, насколько часто они обновляются. Самое лучшее время для резервного копирования — время наименьшей загрузки системы. Сообщите пользователям, когда будет выполняться резервное копирование, чтобы они не обращались к серверу в этот период.

Поскольку резервное копирование в основном выполняется с помощью накопителя на магнитной ленте, первый шаг — выбор такого накопителя. При этом администратор должен учесть следующие факты:

- объем данных, подлежащих резервному копированию;
- надежность носителя информации;
- емкость носителя информации;
- скорость работы накопителя;
- стоимость накопителя и носителей;
- аппаратная совместимость с операционной системой.

В идеале накопитель на магнитной ленте должен иметь емкость, превышающую емкость наибольшего сервера в сети. Он также должен обеспечивать поиск и коррекцию ошибок в течение всего процесса резервирования и восстановления.

Методы резервного копирования обычно применимы к накопителям на магнитной ленте. Опытные администраторы сетей обнаружили, что для резервного копирования больших объемов данных лучше всего использовать несколько отдельных лент; при циклическом расписании. Ленты можно использовать в многонедельном цикле (в зависимости от количества). В первый день цикла администратор выполняет полное резервное копирование, а в последующие дни выполняет резервирование с приращением. Когда цикл полностью завершен, процесс начинается снова. Некоторые администраторы пришли к выводу: целесообразно выполнять несколько резервирований с приращением каждый день в установленное время.

## 9.1. Тестирование и хранение

Квалифицированные администраторы всегда проверяют систему резервного копирования перед тем, как запустить ее в эксплуатацию. Они выполняют резервное копирование, удаляют информацию, восстанавливают данные, а затем пробуют их использовать. Администратор должен регулярно тестировать все процедуры резервного копирования, чтобы быть уверенным: все, что должно резервироваться, в действительности резервируется. Чтобы гарантировать быстрое восстановление важных файлов, необходимо также проверять процедуры восстановления.

В идеале администратор должен делать две копии каждой ленты. Одну он должен хранить на работе, а другую — за пределами организации в безопасном месте. Необходимо помнить: хранение лент в несгораемом сейфе может уберечь их от пламени, однако высокая температура скорее всего разрушит записанные данные.

### Журнал резервного копирования

Ведение журнала окажет существенную помощь при последующем восстановлении файлов. Копии журнала должны храниться вместе с магнитными лентами, рядом с компьютерами. В журнал вносится следующая информация:

- дата выполнения резервного копирования;
- номер ленты;
- тип выполненного резервного копирования;
- компьютер, данные которого резервировались;
- имена сохраненных файлов;
- фамилия сотрудника, выполнявшего операцию;
- местонахождение лент с резервной копией.

### Установка системы резервного копирования

Накопители на магнитной ленте могут быть подключены к серверу или к любому компьютеру, причем резервное копирование инициируется с того компьютера, к которому подсоединен накопитель. Если резервное копирование выполняется непосредственно на сервере, операции резервирования и восстановления протекают намного быстрее, так как отсутствует передача данных по сети.

Резервное копирование через сеть — наиболее удобный метод резервирования для множества систем, однако при этом создается значительный сетевой график и увеличивается время отклика сети. Сетевой трафик, кроме того, вызывает уменьшение производительности. Это одна из причин, почему так важно проводить резервное копирование во время наименьшей загрузки сервера.

Если несколько серверов расположены компактно, можно уменьшить вызванный резервным копированием, — поместите в изолированный сегмент компьютер, с которого выполняется резервирование. Этот компьютер подключают к отдельной сетевой плате каждого сервера (рис.9.1).

Резервное копирование через отдельный сегмент

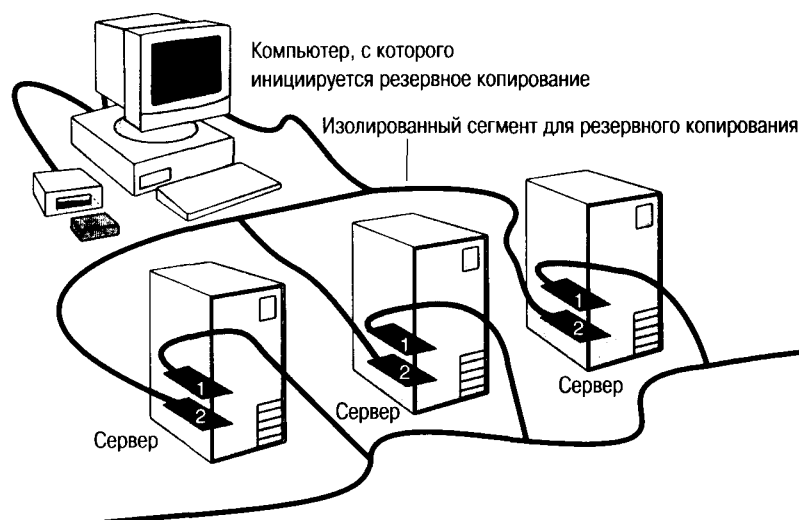


Рис. 9.1.

## 9.2. Источник бесперебойного питания

Источник бесперебойного питания (UPS) — это автоматический внешний источник энергии, который поддерживает работоспособность сервера или других устройств в случае сбоев электрической сети. Системы бесперебойного питания используют способность источников бесперебойного питания взаимодействовать с операционной системой, например с Microsoft Windows NT, через специальный интерфейс. Стандартная система бесперебойного питания обеспечивает две важнейшие для сети функции:

- питание сервера в течение некоторого времени;
- управление безопасным завершением работы системы.

Источником энергии обычно служат аккумуляторы, однако UPS может быть ротационной системой, запасаящей энергию с помощью большого маховика, и двигателем внутреннего сгорания, вращающим генератор переменного тока.

При нарушении питания UPS извещает пользователей о сбое и предупреждает о необходимости завершить работу. Затем, выждав predetermined промежуток времени, UPS организованно закрывает систему.

При этом хорошо организованная система бесперебойного питания будет предотвращать доступ к серверу дополнительных пользователей, а также пошлет администратору сети сообщение об аварии. UPS обычно размещается между сервером и источником питания. Если подача энергии будет восстановлена до полного разряда батарей источника бесперебойного питания и отключения сервера, UPS известит пользователей о возможности продолжить работу.

Лучшие системы бесперебойного питания работают в интерактивном режиме. При сбое питания во внешней сети оно начинает поступать от UPS. Процесс переключения на питание от батарей никоим образом не затрагивает пользователей. Существуют также резервные системы бесперебойного питания, которые включаются при отсутствии энергии в основной сети. Они дешевле интерактивных систем, но не так надежны.

### 9.3. Отказоустойчивые системы

Отказоустойчивые системы защищают данные, дублируя и размещая их на различных физических носителях (например, на разных дисках). Избыточность (redundancy) данных позволяет осуществлять к ним доступ даже в случае выхода из строя части системы. Избыточность — общий отличительный признак большинства отказоустойчивых систем.

Тем не менее, отказоустойчивые системы нельзя использовать как замену регулярного резервного копирования серверов и локальных жестких дисков. Тщательно спланированная стратегия резервного копирования является лучшей страховкой от потери или уничтожения данных.

Отказоустойчивые системы предлагают следующие варианты для обеспечения избыточности данных:

- чередование дисков;
- зеркализацию дисков;
- замену секторов.

#### 9.3.1. Избыточные массивы недорогих дисков

Типы отказоустойчивых систем стандартизованы и классифицируются по уровням. Эти уровни выступают как избыточные массивы недорогих дисков (RAID). Они предлагают различные комбинации производительности, надежности и стоимости. Microsoft Windows NT Server содержит программную поддержку технологии RAID (уровней 0,1 и 5). Microsoft решила поддерживать избыточное чередование дисков уровня 5, проигнорировав уровни 2, 3 и 4, поскольку уровень 5 эволюционировал из этих уровней и, следовательно, является самой последней и наиболее совершенной версией.

##### Уровень 0 — чередование дисков

При чередовании дисков (disk striping) данные делятся на блоки размером 64 Кб равномерно распределяются по всем дискам массива. Однако чередование дисков и обеспечивает повышенной надежности, так как не создает избыточности данных. При повреждении любого раздела будут потеряны все данные. Чередование дисков объединяет множество областей неформатированного свободного пространства в один большой логический диск, распределяя хранилище данных по всем дискам одновременно. В Windows NT для чередования дисков необходимо как минимум два физических диска (максимальное число — 32 диска). При чередовании дисков можно использовать разделы дисков нескольких типов: SCSI, ESDI и IDE.

Чередование дисков имеет ряд преимуществ. Во-первых, несколько малых разделов образуют один большой раздел, благодаря чему лучше используется дисковое пространство. Во-вторых, применяя несколько дисковых контроллеров, можно резко увеличить производительность.

##### Уровень 1 — зеркализация дисков

Зеркализация дисков (disk mirroring) — дублирование раздела и запись его копии на другом физическом диске. Поэтому всегда есть две копии данных, причем каждая — на отдельном диске. Любой раздел может быть зеркалом изолирован. Эта стратегия — простейший метод защиты одиночного диска от сбоев. Зеркализация дисков выступает как форма непрерывного резервного копирования, так как при этом поддерживается полная копия раздела с другого диска.

Дублирование диска (disk duplexing) — это пара зеркальных дисков, каждым из которых управляет отдельный контроллер. При этом уменьшается трафик через единичный контроллер (увеличивается быстродействие). Дублирование предназначено для защиты не только от сбоев носителей, но и от отказов контроллеров.

### **Уровень 2 — чередование дисков с записью кода коррекции ошибок**

Блок данных — при записи — делится на части, распределяемые по разным дискам. Одновременно генерируется код коррекции ошибок (ЕСС), который также записывается на разных дисках. Для кода коррекции ошибок требуется больше дискового пространства, чем при методе с контролем четности. Хотя последний гораздо эффективнее использует дисковое пространство, он уступает в этом отношении уровню 5.

### **Уровень 3 — код коррекции ошибок в виде четности**

Чередование дисков с использованием кода коррекции ошибок, хранящимся в виде четности, подобно уровню 2. Контролем четности называют процедуру проверки ошибок, при которой устанавливается количество единиц в каждой переданной группе битов. Оно должно быть одинаковым — четным или нечетным. В этом случае говорят: данные переданы без ошибок. При этой стратегии метод с кодами ЕСС заменяется схемой контроля четности, которой необходим только один диск для хранения информации контроля четности. Это приводит к тому, что примерно 85 процентов дискового пространства используется для хранения непосредственно данных.

### **Уровень 4 — чередование дисков большими блоками**

Эта стратегия, основанная на методе чередования дисков, обеспечивает запись цельных блоков данных на каждый диск в массиве. Отдельный контрольный диск используется для хранения информации о четности. При каждой записи соответствующая информация о четности должна быть прочитана с контрольного диска и модифицирована. Из-за высоких накладных расходов этот метод больше подходит для операций с крупными блоками, чем для обработки транзакций.

### **Уровень 5 — чередование с контролем четности**

В настоящее время чередование с контролем четности — наиболее популярный метод построения отказоустойчивых систем. Уровень 5 поддерживает от 3 до 32 дисков и распределяет информацию о четности по всем дискам массива (по всему набору чередования). Данные и информация об их четности всегда размещаются на разных дисках.

Блок информации о четности записывается в каждой полосе (ряде) чередования, распределенной по дискам. Информация о четности помогает восстановить данные с отказавшего физического диска. Если отказал один диск, для полного восстановления данных достаточно информации, распределенной по оставшимся дискам. RAID 4 хранит блок четности на одном физическом диске, тогда как RAID 5 распределяет информацию о четности равномерно по всем дискам.

## **9.3.2. Замена секторов**

Некоторые наиболее совершенные операционные системы (такие, как Windows NT Server) предлагают дополнительную возможность для обеспечения отказоустойчивости. Она называется замена секторов (sector sparing) или «горячая замена» (hot fixing). Эта возможность заключается в автоматическом восстановлении секторов во время работы компьютера.



Если при операции дискового ввода/вывода обнаружен дефектный сектор, отказоустойчивый драйвер попытается переместить данные на хороший сектор, а дефектный пометить как «bad». Если перенос данных прошел успешно, драйвер не сообщает файловой системе о сбое. Замена секторов возможна только для SCSI-устройств и невозможна для ESDI- и IDE-дисков.

Некоторые сетевые операционные системы (например, Windows NT Server) имеют утилиты, которые извещают администратора обо всех сбоях секторов, а также об угрозе потери данных, если избыточная копия также будет потеряна.

Большинство передовых сетевых операционных систем предлагает утилиты для реализации отказоустойчивости. В Windows NT Server, например, используется программа Disk Administrator. Графический интерфейс программы Disk Administrator облегчает конфигурирование, а также помогает управлять разбиением дисков на разделы и реализацией отказоустойчивости.

Программа Disk Administrator создает различные конфигурации дисков.

- Чередование дисков с контролем четности.

Несколько разделов дисков объединяются в один большой раздел, хранилище данных распределяется по всем дискам одновременно, для обеспечения отказоустойчивости добавляется информация о четности.

- Зеркализация дисков. Дубликат раздела помещается на отдельный жесткий диск.
- Объединение томов. Несколько разделов дисков объединяются в один большой раздел с последовательной записью данных.
- Чередование дисков. Несколько разделов дисков объединяются в один большой раздел с «размазыванием» данных по всем дискам одновременно.

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Компьютерные сети. Учебный курс/Пер. С англ. — М.: Издательский отдел "Русская редакция" ТОО "Channel Trading". — 1997. — 696 с.: ил.
2. Михаил Гук. Сети NetWare3.12–4.1. — СПб.: Питер, 1997. — 432 с.: ил.
3. Сопряжение датчиков и устройств ввода данных с компьютерами IBM PC: Пер. с англ./под ред. У. Томпкинса, Дж. Уэбстера. — М.: Мир, 1992. — 592 с.: ил.
4. Каган Б.М, Сташин В.В. Основы проектирования микропроцессорных устройств автоматики. — М.: Энергоатомиздат, 1987. — 304 с.: ил.
5. Бессекерский, Н.Б.Ефимов, С.И.Зиатдинов. Микропроцессорные системы автоматического управления. Л.: Машиностроение. Ленинградское отд., 188. — 355 с.
6. Б.А.Калабеков. Микропроцессоры и их применение в системах передачи и обработка сигналов: Учеб. Пособие для вузов. — М.: Радио и связь, 1988. — 368 с.: ил.
7. Кофрон Дж., Лонг В.. Расширение микропроцессорных систем. Пер. с англ., П.В.Нестерова. — М.: Машиностроение, 1987. — 230 с.: ил.