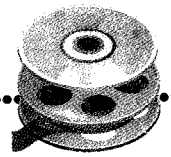


ВИДЕОСАМОУЧИТЕЛЬ

Александр Ватаманюк

Создание и обслуживание локальных сетей

ПИТЕР®

Москва · Санкт-Петербург · Нижний Новгород · Воронеж
Ростов-на-Дону · Екатеринбург · Самара · Новосибирск
Киев · Харьков · Минск
2008

ББК 32.973.202я7
УДК 004.732(075)
В21

Ватаманюк А. И.
В21 Видеосамоучитель. Создание и обслуживание локальных сетей (+CD). — СПб.: Питер, 2008. — 304 с.: ил. — (Серия «Видеосамоучитель»).

ISBN 978-5-91180-774-0

Данная книга поможет вам получить базовые теоретические знания и практические навыки по планированию, проектированию, монтажу и настройке компьютерных сетей, а также по обеспечению их безопасности и поиску неисправностей. Изложенный материал будет интересен как начинающим сетевым администраторам, так и специалистам смежных областей, которые делают первые шаги в изучении компьютерных сетей. Рассматривается настройка сетей в Windows XP и Windows Vista.

Несомненно, вы оцените бонус — прилагаемый к книге компакт-диск с видеороликами, которые иллюстрируют практические действия, касающиеся локальных сетей. На нем вы также найдете краткое описание программ для контроля сетевого трафика, антивирусной защиты и работы в Интернете, а также многие из рассмотренных программ.

ББК 32.973.202я7
УДК 004.732(075)

Краткое содержание

Введение 12
От издательства 13

Часть 1. Компьютерная сеть. Общие понятия

Глава 1. Сеть? Это что еще такое? 15
Глава 2. Типы сетей 18
Глава 3. Модель сети и сетевые протоколы 24
Глава 4. Сетевое оборудование 43
Глава 5. Стратегия выбора 63

Часть 2. Проводная сеть

Глава 6. Топология и стандарты проводной сети 71
Глава 7. Сеть на основе коаксиального кабеля 86
Глава 8. Сеть на основе витой пары 96

Часть 3. Беспроводная сеть

Глава 9. Спецификация и топология беспроводной сети 108
Глава 10. Вопросы безопасности сети 129
Глава 11. Создание сети 136

Часть 4. Нестандартные сети

Глава 12. Сеть на основе телефонной проводки 145
Глава 13. Сеть на основе электрической проводки 148
Глава 14. Сеть из двух компьютеров 151
Глава 15. Домашняя сеть 166

Часть 5. Установка оборудования и настройка программной части

Глава 16. Настройка сети в Windows 2003 Server 182
Глава 17. Установка и подключение сетевого оборудования 205

Глава 18. Настройка беспроводного оборудования 218
Глава 19. Настройка компьютера в Windows XP 249
Глава 20. Настройка компьютера в Windows Vista 263
Глава 21. Подключение сети к Интернету 276
Глава 22. Защита сети 289
Заключение 297
Приложение. Содержимое компакт-диска, который прилагается к книге ... 298

На прилагаемом компакт-диске:

Часть 6. Программное обеспечение
Глава 23. Программы контроля сетевого трафика 304
Глава 24. Программы антивирусной защиты 313
Глава 25. Программы для работы в Интернете 327

Содержание

Введение 12

От издательства 13

Часть 1. Компьютерная сеть. Общие понятия

Глава 1. Сеть? Это что еще такое? 15

1.1. Причины появления сети и перспективы ее развития 16

1.2. Как создаются сети и кто это может сделать 17

Глава 2. Типы сетей 18

2.1. Одноранговая сеть 19

2.2. Сеть на основе сервера 21

Глава 3. Модель сети и сетевые протоколы 24

3.1. Модель ISO/OSI 25

Физический уровень 26

Канальный уровень 26

Сетевой уровень 27

Транспортный уровень 28

Сеансовый уровень 29

Уровень представления данных 29

Прикладной уровень 29

3.2. Сетевой протокол 29

Протокол NetBIOS 31

Протокол NetBEUI 32

Протокол IPX/SPX 32

Протокол TCP/IP 34

3.3. Протоколы работы с электронной почтой 37

3.4. Другие протоколы 39

Глава 4. Сетевое оборудование 43
4.1. Сетевой адаптер 44
4.2. Концентратор 46
4.3. Мост 49
4.4. Коммутатор 50
4.5. Маршрутизатор 51
4.6. Модем 52
4.7. Точка доступа 53
4.8. Антенна 54
4.9. Сетевой кабель 55
Коаксиальный кабель 55
Кабель на основе витой пары 56
Оптоволоконный кабель 56
4.10. Коннекторы, розетки, инструменты 58
Все необходимое для сети на коаксиале 58
Все необходимое для сети на основе витой пары 60

Глава 5. Стратегия выбора 63
5.1. Критерии выбора класса сети 64
5.2. Определение необходимого сетевого оборудования 68

Часть 2. Проводная сеть

Глава 6. Топология и стандарты проводной сети 71
6.1. Топология «общая шина» 72
6.2. Топология «звезда» 73
6.3. Топология «кольцо» 74
6.4. Комбинированные топологии 75
6.5. Стандарты проводной сети Ethernet 76
Понятие стандарта 76
Ethernet 10Base-2 77
Ethernet 10Base-5 79
Ethernet 10Base-T 80
Ethernet 10Base-F 81
Fast Ethernet 100Base-TX 81
Fast Ethernet 100Base-FX 82
Gigabit Ethernet 82
10 Gigabit Ethernet 83
Token Ring 83
6.6. Преимущества и недостатки проводной сети 84

Глава 7. Сеть на основе коаксиального кабеля 86
7.1. Правила прокладки кабеля 87
7.2. Подготовка кабеля 90

7.3. Монтаж разъемов BNC ... 92
7.4. Установка Т-коннекторов и заглушек ... 95

Глава 8. Сеть на основе витой пары ... 96
8.1. Принципы прокладки проводки ... 97
Топологические модели ... 99
Правила прокладки кабеля ... 99
8.2. Подготовка кабеля ... 100
8.3. Монтаж сетевых розеток ... 104
8.4. Монтаж разъемов RJ-45 ... 104

Часть 3. Беспроводная сеть

Глава 9. Спецификация и топология беспроводной сети ... 108
9.1. Методы и технологии модуляции сигнала ... 109
Метод DSSS ... 111
Метод FHSS ... 111
Метод OFDM ... 111
Метод PBCC ... 112
Технология кодирования Баркера ... 113
Технология CCK ... 114
Технология CCK-OFDM ... 114
Технология QAM ... 114
9.2. Топология беспроводной сети ... 115
Независимая конфигурация ... 115
Инфраструктурная конфигурация ... 116
9.3. Стандарты беспроводной сети Ethernet ... 118
Стандарт IEEE 802.11 ... 119
Стандарт IEEE 802.11a ... 120
Стандарт IEEE 802.11b ... 120
Стандарт IEEE 802.11d ... 121
Стандарт IEEE 802.11e ... 121
Стандарт IEEE 802.11f ... 122
Стандарт IEEE 802.11g ... 122
Стандарт IEEE 802.11h ... 123
Стандарт IEEE 802.11i ... 123
Стандарт IEEE 802.11j ... 124
Стандарт IEEE 802.11n ... 124
Стандарт IEEE 802.11r ... 125
9.4. Преимущества и недостатки беспроводной сети ... 125

Глава 10. Вопросы безопасности сети ... 129
10.1. Протокол безопасности WEP ... 131
Аутентификация с открытым ключом ... 131
Аутентификация с общим ключом ... 132

10.2. Протокол безопасности WPA ... 133
10.3. Идентификатор точки доступа и MAC-фильтрация ... 134
Идентификатор точки доступа ... 134
MAC-фильтрация ... 135

Глава 11. Создание сети ... 136
11.1. Правовые вопросы ... 137
11.2. Условия использования режима Ad-Hoc ... 138
Прямая видимость между подключаемыми компьютерами ... 138
Стандарт беспроводных адаптеров ... 139
Беспроводные адаптеры ... 139
Количество подключенных компьютеров ... 140
11.3. Условия использования режима инфраструктуры ... 140
Условия использования и расположение точки доступа ... 140
Точка доступа ... 142
Мост ... 142
Маршрутизатор ... 143
Мощность передатчиков ... 143
Беспроводные адаптеры ... 143

Часть 4. Нестандартные сети

Глава 12. Сеть на основе телефонной проводки ... 145

Глава 13. Сеть на основе электрической проводки ... 148

Глава 14. Сеть из двух компьютеров ... 151
14.1. Нуль-модемное соединение ... 152
Характеристики COM-порта ... 153
Характеристики LPT-порта ... 153
Подключение компьютеров ... 155
Подготовка операционной системы ... 156
14.2. Соединение с помощью коаксиального кабеля ... 159
14.3. Соединение с помощью кабеля на основе витой пары ... 161
14.4. Соединение с помощью USB-кабеля ... 163
14.5. Соединение через FireWire-порт ... 163
14.6. Соединение через Bluetooth ... 164

Глава 15. Домашняя сеть ... 166
15.1. Проектирование сети ... 167
15.2. Выбор топологий и стандарта ... 168
15.3. Размещение оборудования ... 173
15.4. Прокладка кабеля ... 173
15.5. Использование беспроводного оборудования ... 176
15.6. Необходимое сетевое оборудование ... 177
Выбор сетевых адаптеров ... 177
Выбор маршрутизатора ... 178

Выбор концентраторов и коммутаторов ... 178
Выбор беспроводного оборудования ... 179
Управление ресурсами сети ... 180

Часть 5. Установка оборудования и настройка программной части

Глава 16. Настройка сети в Windows 2003 Server ... 182
16.1. Выбор управляющего компьютера ... 183
16.2. Создание домена ... 185
16.3. Использование DNS-сервера ... 188
16.4. Использование DHCP-сервера ... 189
Область адресов ... 190
Пул адресов ... 193
Арендованные адреса ... 193
Резервирование ... 194
Параметры области ... 195
Параметры сервера ... 195
16.5. Использование механизма Active Directory ... 195
Создание подразделений ... 196
Создание группы ... 197
Создание учетной записи пользователя ... 198
16.6. Настройка общего доступа ... 202

Глава 17. Установка и подключение сетевого оборудования ... 205
17.1. Подключение концентратора или коммутатора ... 206
17.2. Подключение точки доступа ... 208
17.3. Подключение маршрутизатора ... 209
17.4. Установка сетевого адаптера и драйверов ... 210

Глава 18. Настройка беспроводного оборудования ... 218
18.1. Настройка точки доступа ... 219
Вкладка General ... 226
Вкладка Wireless ... 227
Вкладка Security ... 231
Вкладка Filters ... 233
Вкладка AP Mode ... 235
Вкладка DHCP Server ... 237
Вкладка Client Info ... 239
Вкладка Multi-SSID ... 240
18.2. Настройка беспроводного адаптера ... 242

Глава 19. Настройка компьютера в Windows XP ... 249
19.1. Настройка параметров сети и проверка связи с сервером ... 250
Подключение к домену или рабочей группе ... 250
Настройка протокола ... 252
Проверка связи ... 255

19.2. Работа с общими ресурсами ... 257
Предоставление доступа к дискам и их содержимому ... 257
Предоставление доступа к принтерам ... 259
Подключение сетевой папки ... 261
Подключение сетевого принтера ... 262

Глава 20. Настройка компьютера в Windows Vista ... 263
20.1. Подключение к сети ... 264
Настройка протокола ... 264
Настройка сетевого обнаружения ... 266
Проверка связи ... 267
20.2. Работа с общими ресурсами ... 268
Предоставление файлового ресурса ... 268
Предоставление принтера ... 272
Подключение сетевой папки ... 275
Подключение сетевого принтера ... 275

Глава 21. Подключение сети к Интернету ... 276
21.1. Некоторые сведения об Интернете ... 277
21.2. Варианты доступа в Интернет ... 278
Подключение с помощью аналогово-цифрового модема ... 279
Подключение с помощью xDSL-модема ... 280
Подключение через выделенную линию ... 280
Подключение через Frame Relay ... 281
Подключение через беспроводной модем ... 281
Подключение через кабельное телевидение ... 282
21.3. Организация общего доступа в Интернет ... 283
Использование стандартных компонентов Windows XP ... 283
Использование программы Kerio WinRoute ... 286

Глава 22. Защита сети ... 289
22.1. Отключение трансляции SSID ... 290
22.2. Фильтрация MAC-адресов ... 291
22.3. Настройка шифрования ... 292
22.4. Снижение мощности передатчика ... 295

Заключение ... 297

Приложение. Содержимое компакт-диска, который прилагается к книге ... 298

На прилагаемом компакт-диске:

Часть 6. Программное обеспечение

Глава 23. Программы контроля сетевого трафика ... 304
23.1. DU Meter ... 306
23.2. TMeter ... 307

23.3. NetLimiter ... 308
23.4. NetStat Live ... 309
23.5. Bandwidth Monitor Pro ... 310
23.6. CommView ... 310
23.7. NetPeeker ... 311

Глава 24. Программы антивирусной защиты ... 313
24.1. Symantec AntiVirus Corporate Edition ... 314
24.2. Dr.Web ... 317
24.3. Panda Antivirus Platinum ... 319
24.4. «Антивирус Касперского» ... 322
24.5. NOD32 ... 324

Глава 25. Программы для работы в Интернете ... 327
25.1. Браузеры ... 328
Microsoft Internet Explorer ... 328
Opera ... 330
MyIE2 ... 331
Mozilla Firefox ... 332
25.2. Почтовые клиенты ... 334
The Bat! ... 336
Outlook Express ... 339
Mozilla Thunderbird ... 342
25.3. Программы для борьбы со спамом ... 344
Anti Spammer ... 345
SpamPal ... 346
Agava Spamprotexx ... 347
Anti-Spam Filter ... 348
Настройка антиспамовых фильтров ... 349
25.4. Менеджеры закачки файлов ... 355
ReGet Deluxe ... 356
FlashGet ... 357
Download Master ... 358
Teleport Pro ... 359
25.5. Интернет-пейджеры ... 360
ICQ ... 361
QIP ... 363
Trillian ... 364
25.6. Программы для борьбы со SpyWare ... 365
Ad-Aware SE ... 365
Arovax Shield ... 367

Введение

Компьютерные сети оплели весь земной шар, и вы, хотите того или нет, увязли в них так же прочно, как муха в паутине. Теперь попробуйте ответить на вопрос: нужно ли пытаться разобраться с этой ситуацией или пустить все на самотек?

Принимая решение, имейте в виду: уровень компьютеризации вырос настолько, что лишь безнадежно отсталый человек может оказаться незатронутым ею, даже если техника заполняет его быт и работу.

Книга, которую вы держите в руках, приобщит вас к научно-техническому прогрессу и научит жить в современном компьютерном обществе. Из нее вы узнаете много интересной и полезной информации о том, что такое компьютерная сеть и как с ней «общаться». Люди же более любознательные получат неоценимый опыт и смогут использовать его на практике.

Книга содержит большое количество текстовой и графической информации, которая облегчит понимание самой сущности локальной сети. Мало того, к изданию прилагается диск с видеоуроками, которые в режиме реального времени познакомят вас со всем процессом, начиная с создания сети и заканчивая ее настройкой и обслуживанием. На компакт-диске вы также найдете краткое описание программного обеспечения для контроля сетевого трафика, работы в Интернете, антивирусной защиты и многие из рассмотренных программ. Коммерческие продукты представлены ознакомительными и демонстрационными версиями. Как правило, в демонстрационных версиях недоступны некоторые инструменты и функции, но пользоваться ими можно сколь угодно долго. Ознакомительные версии обычно полнофункциональны, но действуют в течение ограниченного времени (30 дней или меньше). Некоторые из рассмотренных в книге программ являются бесплатными, их возможности и срок действия неограниченны.

Только ленивый не познает и не оценит возможности компьютерных сетей! Не становитесь им!

Книга ориентирована на определенную категорию читателей, однако это совсем не означает, что любой человек не сможет разобраться с ее материалом. По подобному принципу создавался и этот видеосамоучитель. Конечно, основная его аудитория — читатели, которые хотят больше узнать о локальных сетях и способах их создания. Тем не менее осилить и понять ее сможет даже малоопытный компьютерный пользователь.

В любом случае, даже если вас не очень интересуют разные компьютерные штучки и тем более сети, прочитав книгу, вы ими заинтересуетесь. Это гарантировано. Поэтому просто расслабьтесь и просвещайтесь, и будьте уверенны в том, что вы с легкостью овладеете изложенным материалом!

От издательства

Ваши замечания, предложения и вопросы отправляйте по следующему адресу электронной почты: **dgurski@minsk.piter.com** (издательство «Питер», компьютерная редакция).

Мы будем рады узнать ваше мнение!

На сайте издательства **http://www.piter.com** вы найдете подробную информацию о наших книгах.

Часть 1

Компьютерная сеть. Общие понятия

Глава 1

Сеть? Это что еще такое?

- Причины появления сети и перспективы ее развития
- Как создаются сети и кто это может сделать

1.1. Причины появления сети и перспективы ее развития

Когда компьютер только задумывали, главной его задачей предполагалось облегчение труда человека и автоматизация и ускорение выполнения некоторых арифметических операций. Никто тогда даже думать не мог, что компьютеров через несколько десятков лет будет настолько много, что рано или поздно они будут объединены в один громадный «организм», удовлетворяющий практически все потребности человека. Тем не менее так оно и произошло, по крайней мере очень близко к этому.

Каковы же причины появления сети? Как минимум можно выделить несколько:

- несовершенство существующих компьютеров и компьютерной техники;
- недостаток мощности отдельного компьютера для выполнения сложной задачи;
- слишком большое количество людей, задействованных в достижении поставленной цели;
- новые направления в науке, требующие все больших человеческих и компьютерных ресурсов.

Этот список можно продолжать очень долго, но факт остается фактом: рано или поздно сеть должна была возникнуть и она возникла.

Таким образом, сеть — не что иное, как некоторое количество компьютеров, определенным способом подключенных друг к другу. Однако это только часть понятия. На самом деле сюда еще нужно включить сетевые операционные системы, прикладные программы, специальные программные механизмы обмена информацией и многое другое.

Можно сказать однозначно, что появление сети изменило жизнь всего человечества. Преимуществ у сети много, больше, чем можно было бы себе представить. Вот только некоторые из них:

- организация одновременной работы многих пользователей с одним источником, будь то распределенная база данных или обычный офисный документ;
- использование всех компьютеров сети для выполнения одной работы с целью осуществления сложного, требующего много ресурсов проекта;

- обмен информацией любого характера, будь то рабочие данные или фильмы и музыка;
- получение данных из любой точки земного шара с использованием для этого сети спутников;
- общение (устное, письменное, визуальное) на расстоянии;
- использование компьютерных сетей для обучения и любого другого типа образования.

Преимуществ сети много, а недостатков практически нет. Ну разве что возможность тотального наблюдения за любым подключенным к сети пользователем...

Каковы перспективы дальнейшего развития сети? Все очень просто: глобальная компьютеризация и возможность мгновенного получения любой информации с использованием для этого любого устройства с коммуникационными способностями. После этого, наверное, жизнь станет гораздо скучнее.

1.2. Как создаются сети и кто это может сделать

Сети возникают с пугающей скоростью. Порой приходишь в знакомый офис через неделю, а в нем уже функционирует современная сеть с высокой пропускной способностью. Но самое главное, что организовать сеть может практически любой человек, более или менее знакомый с принципом и правилами ее создания. Так почему бы вам не стать этим «любым»?

Конечно, сразу создать сеть с большим количеством компьютеров будет достаточно трудно, даже если вы прочтете гору книг по теме. Самый простой способ научиться — познакомиться с теорией и попроситься к кому-нибудь в ученики. И будет большим плюсом, если вы попытаетесь сами соединить хотя бы два рядом стоящих компьютера в домашних условиях. Это и станет началом вашей сетевой практики.

Однако, как обычно, все нужно начинать с теории. Необходимо познакомиться с существующими стандартами и топологиями, увидеть сетевое оборудование, пощупать кабель, коннекторы и т. д.

Данная книга призвана облегчить процесс освоения принципов сети и дать основные практические советы. Как говорится, не святые горшки лепят, все в ваших руках. Поэтому учите теорию и осваивайте практику!

Глава 2

Типы сетей

- Одноранговая сеть
- Сеть на основе сервера

Сегодня, как и 10 лет назад, существует два типа сетей: одноранговая сеть и сеть на основе сервера (выделенного компьютера). Каждая из них имеет как преимущества, так и недостатки.

Одноранговая сеть, скорее всего, придется по душе пользователям, которые хотят сначала попробовать сеть в деле или ограничены в средствах. Сеть на основе сервера организуют там, где важен полный контроль над всеми рабочими местами. Это может быть и небольшая домашняя сеть, и объемная корпоративная система сетей, объединенных в одну общую.

Эти два разных типа имеют общие корни и принципы функционирования, что в случае необходимой модернизации позволяет перейти от более простого варианта (одноранговой сети) к более сложному (сети на основе сервера).

2.1. Одноранговая сеть

Одноранговую сеть построить достаточно просто. Особенность такой сети в том, что все входящие в ее состав компьютеры работают сами по себе, то есть ими никто не управляет.

Одноранговая сеть выглядит как некоторое количество компьютеров, объединенных определенным образом в одну рабочую группу (рис. 2.1). Именно отсутствие управляющей машины (сервера) делает ее построение дешевым и эффективным мероприятием.

Любой компьютер в такой сети можно назвать как рабочим, так и сервером, поскольку нет какой-либо конкретной выделенной машины, которая осуществляла бы административный или другой контроль. За компьютером такой сети следит сам пользователь (или пользователи), который работает на нем. В этом кроется главный недостаток одноранговой сети — ее пользователь должен не просто уметь работать на компьютере, но и иметь представление об администрировании. Кроме того, ему в большинстве случаев приходится самому справляться с возникающими внештатными ситуациями и защищать себя от разнообразных неприятностей, начиная с вирусов и заканчивая программными и аппаратными неполадками.

Как и полагается, одноранговая сеть позволяет использовать общие файлы, принтеры, модемы и т. п. Однако из-за отсутствия управляющего компьютера каждый пользователь разделяемого ресурса должен самостоятельно устанавливать права доступа к нему.

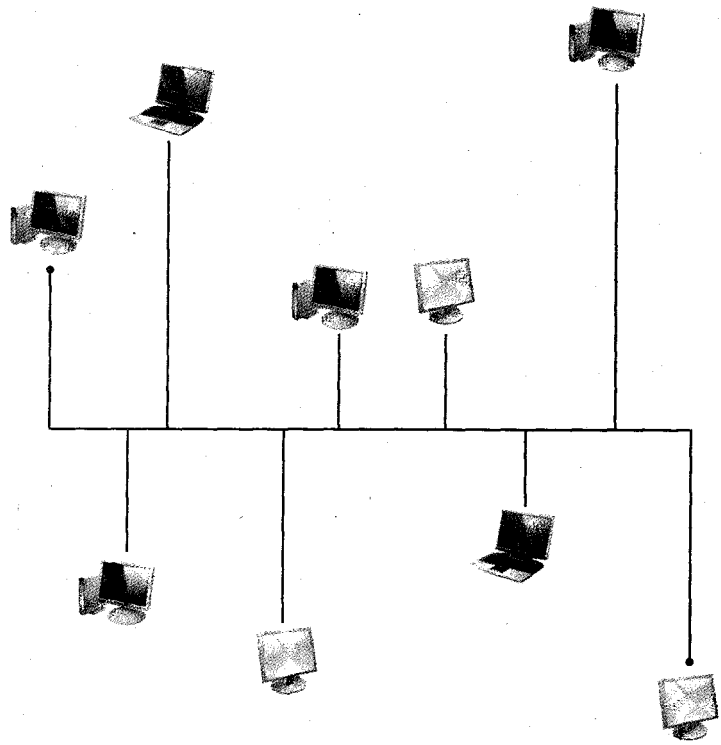


Рис. 2.1. Пример одноранговой сети

Для работы с одноранговыми сетями можно использовать любую операционную систему. Ее поддержка реализована в Windows, начиная с Windows 95, поэтому никакого дополнительного программного обеспечения для работы в локальной сети не требуется. Однако если вы хотите обезопасить себя от разных программных проблем, лучше использовать операционную систему достаточно высокого класса, например Windows XP.

Одноранговую сеть обычно применяют тогда, когда нужно связать несколько (как правило, до десяти) компьютеров и не нужно использовать строгую защиту данных. Большее количество компьютеров подключать не рекомендуется, так как отсутствие «контролирующих органов» рано или поздно приводит к возникновению различных проблем. Ведь из-за одного необразованного или ленивого пользователя под угрозу ставится безопасность и работоспособность всей сети.

Если вы заинтересованы в более защищенной и контролируемой «организации», то создавайте сеть на основе сервера.

В табл. 2.1 перечислены основные преимущества и недостатки одноранговой сети.

Таблица 2.1. Преимущества и недостатки одноранговой сети

Преимущества	Недостатки
Дешевая в создании	Недостаточный контроль над клиентскими местами
Не нужен выделенный сервер (или серверы)	Отсутствие механизма настраиваемого доступа нескольких пользователей к разным ресурсам на одном компьютере
Не требуется специальное программное обеспечение	Низкая безопасность и защищенность сети от вирусных атак
Не нужен человек, который будет поддерживать сеть и клиентские места	Отсутствие нормального механизма резервного копирования данных
	Необходимость подготовленности пользователя к разным административным мерам — обновлению антивирусной базы, архивированию данных, определению механизмов доступа к раздаваемым ресурсам и т. д.
	Для предоставления пользователям общего ресурса, который будет интенсивно использоваться, требуется достаточно мощный компьютер
	Ограниченная расширяемость сети

2.2. Сеть на основе сервера

Сеть на основе сервера — наиболее часто встречающийся тип, который используют как в полноценных домашних сетях и в офисах, так и на крупных предприятиях (рис. 2.2).

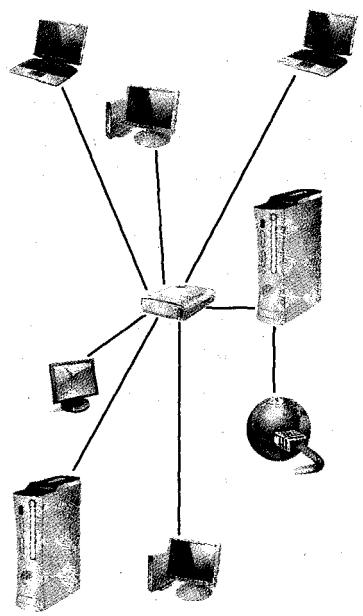


Рис. 2.2. Пример сети на основе сервера

Как ясно из названия, данная сеть использует сервер, контролирующий работу всех подключенных клиентских компьютеров. Главная его задача — создание, настройка и обслуживание учетных записей пользователей, настройка прав доступа к общим ресурсам, механизма авторизации и смены паролей доступа и многое другое.

Как правило, сервер характеризуется большой мощностью и быстродействием, необходимым

для выполнения поставленных задач: будь то работа с базой данных или обслуживание других запросов пользователей. Сервер оптимизирован для быстрой обработки запросов пользователей, обладает специальными механизмами программной защиты и контроля. Достаточная мощность сервера позволяет снизить требования к мощности клиентской машины.

За работой сети на основе сервера обычно следит специалист — системный администратор. Он отвечает за регулярное обновление антивирусных баз, устраняет возникшие неполадки, разделяет общие ресурсы и т. п.

Количество рабочих мест в такой сети может быть разным — от нескольких до сотен или тысяч компьютеров. С целью поддержки производительности сети на необходимом уровне при возрастании количества подключенных пользователей устанавливают дополнительное или более скоростное сетевое оборудование, серверы и т. д.

Не все серверы выполняют одинаковую работу. Существуют следующие специализированные машины, позволяющие автоматизировать или просто облегчить выполнение тех или иных задач.

- **Файл-сервер.** Используется в основном для хранения разнообразных данных, начиная с офисных документов и заканчивая музыкой и видео. Обычно на таком сервере создаются личные папки пользователей, обращаться к которым могут только они (или другие пользователи, получившие право доступа). Для управления таким сервером используют любую сетевую операционную систему, например Windows 2000 или Windows 2003. Благодаря кэшированию файлов доступ к ним значительно ускоряется.
- **Принт-сервер.** Главная его задача — обслуживание очереди печати сетевых принтеров и обеспечение доступа к ним. Очень часто с целью экономии средств файл-сервер и принт-сервер совмещают.
- **Сервер базы данных.** Основная его задача — обеспечить максимальную скорость поиска и записи нужных данных в базу данных или получения информации из нее с последующей передачей конечному пользователю сети. Это самые мощные из всех серверов. Они обладают максимальной производительностью, так как от этого зависит комфортность работы всех пользователей.
- **Сервер приложений.** Промежуточный сервер между пользователем и сервером базы данных. Как правило, на нем выполняются те из запросов, которые требуют максимальной производительности и должны быть переданы

пользователю, не затрагивая ни сервер базы данных, ни пользовательский компьютер. Это могут быть как часто запрашиваемые из базы данные, так и любые программные модули.

Кроме перечисленных выше, существуют другие серверы, например почтовые, коммуникационные, серверы-шлюзы и т. д.

Достаточно часто в целях экономии средств на один из серверов «вешают» обслуживание нехарактерных для него заданий. В этом случае следует понимать, что скорость выполнения им тех или иных задач может значительно понижаться.

Сеть на основе сервера предоставляет широкий спектр услуг и возможностей, которых трудно или невозможно добиться от одноранговой сети. Кроме того, последняя уступает в плане защищенности и администрирования. Имея выделенный сервер или серверы, легко обеспечить резервное копирование, что является первоочередной задачей, если в сети присутствует сервер базы данных.

В табл. 2.2 перечислены основные преимущества и недостатки сети на основе сервера.

Таблица 2.2. Преимущества и недостатки сети на основе сервера

Преимущества	Недостатки
Практически неограниченная расширяемость	Достаточно дорогая в создании и обслуживании
Контроль над клиентскими местами	Необходимо специальное программное обеспечение, способное работать в сети
Наличие четкого механизма доступа к общим ресурсам	Нужен постоянный системный администратор, который будет поддерживать сеть и клиентские места
Единая антивирусная база	Сложный процесс расширения сети (прокладка кабеля)
Высокая производительность	
Централизованное резервное копирование всей информации	
Низкие требования к мощности клиентских машин	

Глава 3

Модель сети и сетевые протоколы

- Модель ISO/OSI
- Сетевой протокол
- Протоколы работы с электронной почтой
- Другие протоколы

Какой бы ни была сеть, она должна подчиняться определенным законам. Не забывайте, что сеть — это не только кусок провода, но и все устройства, которые в нее входят, в том числе и компьютеры. Представьте себе на минуту, что нет никаких правил работы сети. Какие функции должны выполнять сетевая карта или маршрутизатор, как должен реагировать на это компьютер?

Чтобы избежать хаоса и упорядочить «взаимоотношения» в сети, используется специальная система правил и стандартов. Их представителями являются сетевая модель взаимодействий ISO/OSI и протоколы передачи данных.

3.1. Модель ISO/OSI

Пожалуй, ключевым понятием в стандартизации сетей и всего, что к ним относится, является *модель взаимодействия открытых систем* (Open System Interconnection, OSI), разработанная Международной организацией по стандартизации (International Standards Organization, ISO). На практике применяется короткое название «модель ISO/OSI».

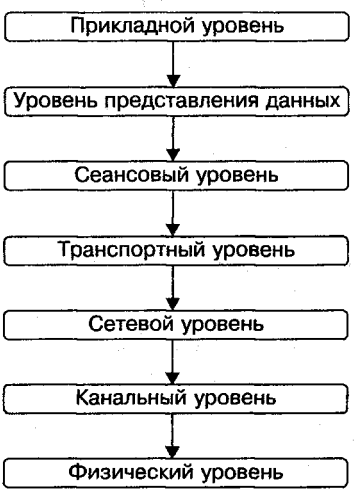


Рис. 3.1. Уровни модели ISO/OSI

Описываемая модель состоит из семи уровней (рис. 3.1), каждый из которых отвечает за определенный круг задач, осуществляя их с помощью заложенных в этот уровень алгоритмов — стандартов и протоколов. Для связи между уровнями используются процедуры взаимодействия. Таким образом, выполнив свою часть задачи, нижестоящий уровень передает готовые данные вышестоящему. Вот и получается, что, пройдя всю цепочку из семи уровней, на выходе получаются готовые к «употреблению» данные. При этом они успевают должным образом закодироваться или раскодироваться, пройти проверку целостности и многое другое.

Основное различие между проводными (Ethernet 802.3) и беспроводными (IEEE 802.11) сетями кроется только в двух крайних уровнях — физическом и канальном. Остальные же работают абсолютно одинаково и не имеют никаких различий.

Рассмотрим все уровни модели ISO/OSI подробнее.

Физический уровень

Физический уровень — самый первый, «нижний» уровень. Фактически он представляет собой аппаратную часть сети и описывает способ передачи данных, используя для этого любой имеющийся канал — проводной или беспроводной. Исходя из выбранного канала передачи данных должно использоваться соответствующее сетевое оборудование с определенными параметрами передачи данных, учитывающими всевозможные особенности канала, такие как полосы пропускания, защита от помех, уровень сигнала, кодирование, скорость передачи данных в физической среде и т. п.

Таким образом, всю описанную работу вынуждено выполнять сетевое оборудование: сетевая карта, мост, маршрутизатор и т. д.

Физический уровень — один из уровней, который отличает беспроводные сети от их «собратьев» — проводных сетей. Разница между ними заключается в канале передачи данных: в первом случае это радиоволны определенной частоты или инфракрасное излучение, в другом — любая физическая линия, например коаксиал, витая пара или оптоволокно.

Канальный уровень

Главная его задача — удостовериться, что канал свободен и ничто не станет угрожать надежности передачи и целостности пакетов. В идеале протоколы канального уровня в паре с сетевым оборудованием должны проверить, является ли канал свободным для передачи данных, не имеется ли коллизий и т. п.

Такую проверку необходимо проводить каждый раз, поскольку локальная сеть редко состоит всего из двух компьютеров, хотя даже в этом случае канал может быть занят. Обнаружив, что канал свободен, данные, которые необходимо передать другому компьютеру, делятся на более мелкие части — кадры. Каждый такой кадр снабжается контрольной суммой и отсылается. Приняв этот кадр, получатель проверяет контрольные суммы и, если они совпадают, принимает его и отправляет подтверждение о доставке. В противном случае кадр игнорируется, фиксируется ошибка, которая отправляется получателю, и кадр передается заново. Так, кадр за кадром, происходит передача всего объема данных.

Канальный уровень также описывает алгоритмы работы в конкретной физической среде, например при использовании витой пары или оптоволокна. Сюда же включаются и правила прокладки кабеля.

Как и в случае с физическим уровнем, канальный также имеет различия для проводных и беспроводных сетей. Связано это со спецификой сетевого оборудования. Так, беспроводное оборудование на данный момент работает только в полудуплексном режиме, а это означает, что одновременно может вестись только прием или только передача. Этот факт резко снижает эффективность обнаружения коллизий и, соответственно, скорость передачи данных в беспроводных сетях.

Поскольку модель ISO/OSI жестко регламентирует действия каждого уровня, то разработчикам пришлось немного модернизировать протоколы канального уровня для работы в беспроводных сетях. В частности, в случае беспроводной передачи данных используются протоколы CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) или DCF (Distributed Coordination Function).

Протокол CSMA/CA характеризуется тем, что избегает коллизий при передаче данных, используя явное подтверждение доставки, которое говорит о том, что пакет доставлен и он не поврежден.

Работает это следующим образом. Когда один компьютер собирается передать данные другому, то всем станциям сети посылается короткое сообщение (ready to send, RTS), содержащее в себе информацию о получателе и времени, необходимом для передачи данных. Получив такой пакет, все компьютеры прекращают передачу данных на указанное время. Получатель отсылает отправителю сообщение о готовности приема данных (clear to send, CTS). Получив его, компьютер-отправитель высылает первую порцию данных и ждет подтверждения доставки пакета. После подтверждения доставки передача данных продолжается. Если же подтверждение не пришло, компьютер-отправитель повторно передает конкретный пакет.

Это гарантирует доставку пакетов данных, но в то же время заметно снижает скорость передачи данных. Именно поэтому беспроводные сети всегда были медленнее проводных и таковыми останутся надолго, если не навсегда. Чтобы хоть как-то повысить скорость, один из протоколов канального уровня производит фрагментацию (разделение на фрагменты) пакетов, что увеличивает шанс их передачи с удачным исходом, исключая повторную пересылку.

Сетевой уровень

Как и канальный, сетевой уровень занимается передачей информации. Однако между ними есть существенная разница: канальный уровень может передавать

данные между компьютерами, которые подключены с использованием одной топологии. Если сеть является комбинированной, за работу принимается сетевой уровень.

Данные в сетевом уровне делятся на порции, которые называются пакетами. Перед тем как начать передачу данных другому компьютеру, происходит преждевременная настройка связи, заключающаяся в выборе пути, по которому будут передаваться данные. Этот процесс называется *маршрутизацией*. Выбор нужного маршрута — одна из основных функций сетевого уровня. Невозможно выбрать идеальный путь, поскольку рано или поздно на одном из отрезков может повыситься трафик, что приведет к увеличению времени передачи пакетов. Поэтому нужный путь выбирается по среднему значению всех необходимых параметров: пропускной способности, интенсивности трафика, дальности и скорости передачи, ее надежности и т. п.

Как правило, при выборе маршрута используются маршрутизаторы. В их таблицах хранится информация о скорости передачи между отдельными отрезками сети, трафике, среднем времени передачи и т. д., основываясь на которой протоколы сетевого уровня могут выбрать оптимальный путь прохождения данных.

Организация сетевого уровня может осуществляться как программно, так и аппаратно.

Транспортный уровень

Идеальную сеть создать невозможно — хоть где-то, но произойдет отклонение от требований ее построения. Если сеть достаточно большая и включает несколько маршрутизаторов, то это не только усложняет ее, но и приводит к ее ненадежности.

Основная задача транспортного уровня — обеспечить требуемую степень надежности при передаче информации между выбранными компьютерами. Транспортный уровень может делать это пятью способами. Каждый из них отличается не только защищенностью данных при пересылке, но и временем их доставки или возможностью исправления возникающих ошибок. Поэтому, начиная с данного уровня, выбор варианта доставки может производить программа, то есть непосредственно пользователь. Зачем назначать максимальные предосторожности перед отправкой и во время передачи данных, если сеть характеризуется хорошим качеством и низкой вероятностью появления ошибок? Логично

выбрать наиболее простой способ из пяти существующих. И наоборот, если в сети часто происходят коллизии, которые приводят к потере информации, следует использовать способ, который гарантирует вам доставку данных в любом случае.

Транспортным уровнем можно управлять программно, а не только аппаратными средствами.

Сеансовый уровень

Сеансовый уровень контролирует передачу пакетов между компьютерами. Осуществляя синхронизацию принятых и отправленных пакетов, протоколы сеансового уровня отслеживают недостающие и передают их заново. За счет того что передаются только недостающие пакеты, достигается повышение скорости.

Уровень представления данных

Чтобы урегулировать процессы отправки и получения информации между двумя компьютерами, существует уровень представления, который приводит ее к единому синтаксическому стандарту, поэтому именно здесь эффективно использовать разнообразные методы шифрования данных, чем и занимаются многие протоколы.

Прикладной уровень

Этот уровень отвечает за связь с прикладными программами. Он представляет собой обычный набор протоколов, с помощью которых можно осуществлять доступ к любым ресурсам сети.

Таким образом, пройдя все семь уровней, сообщение пользователя пополняется служебной информацией (заголовками) каждого из них. Аналогично, попав к нужному получателю и опять пройдя все семь уровней, информация очищается от всей служебной информации.

3.2. Сетевой протокол

В предыдущем разделе была кратко рассмотрена модель ISO/OSI, которая описывает работу любого сетевого оборудования и сети в целом. Однако это

всего лишь модель, рисунок на бумаге. Чтобы все это начало работать, необходим механизм, ее реализующий. Таким механизмом является протокол передачи данных, а если точнее, множество протоколов.

Таким образом, *протокол* — набор правил, использование которых делает возможной передачу данных между компьютерами. Все эти правила работают в рамках модели ISO/OSI и не могут отступать от нее ни на шаг, поскольку это может повлечь за собой несовместимость оборудования и программного обеспечения.

Поскольку каждый из уровней модели ISO/OSI обладает своими особенностями, то реализация всех этих особенностей невозможна в рамках одного протокола. Мало того, она даже невыгодна, поскольку значительную часть логики можно разрабатывать на уровне аппаратного обеспечения, что приводит к максимально быстрой обработке данных. Исходя из этих соображений было разработано множество узконаправленных протоколов, каждый из которых выполняет свою задачу и делает это с максимальной отдачей и быстродействием.

Все протоколы можно разделить на низкоуровневые и высокоуровневые.

Низкоуровневые реализованы давно, и никаких кардинальных изменений в них не вносится, что за длительное время их использования позволило найти и устранить все возможные дыры и ошибки в их работе.

ПРИМЕЧАНИЕ

Низкоуровневые протоколы реализуются на аппаратном уровне, что позволяет добиться максимального быстродействия и безошибочности.

Что касается *высокоуровневых* протоколов, то их разрабатывают и совершенствуют постоянно. В этом нет ничего плохого, даже наоборот: всегда существует возможность придумать новый, более эффективный способ передачи данных.

ПРИМЕЧАНИЕ

Как правило, высокоуровневые протоколы реализуются в виде драйверов к сетевому оборудованию для разных операционных систем.

Существует множество разных протоколов, каждый из которых имеет свои особенности. Одни из них узконаправленные, другие имеют более широкое применение. Разрабатываются несколькими фирмами, поэтому неудивительно,

что каждая из них создает свой собственный стек (набор) протоколов. Хотя эти стеки по умолчанию между собой несовместимы, существуют дополнительные протоколы, являющиеся мостами между ними, что позволяет использовать в одной операционной системе несколько несовместимых между собой протоколов.

Следует также упомянуть тот факт, что не все протоколы могут применяться в одинаковых условиях. Бывает, применение одного из них выгодно для небольшой группы компьютеров одноранговой сети и крайне невыгодно для большого количества машин сети на основе сервера с несколькими маршрутизаторами и общим выходом в Интернет.

Наибольшую популярность приобрели такие стеки протоколов, как NetBIOS/NetBEUI, IPX/SPX, TCP/IP и др. Более подробно познакомиться с их возможностями вы сможете ниже.

Протокол NetBIOS

NetBIOS (Network Basic Input/Output System) — один из первых сетевых протоколов, разработанный в 1984 году с целью создания интерфейса передачи сообщений по локальной сети, как одноранговой, так и на основе сервера.

Для передачи сообщений по сети NetBIOS используются логические имена компьютеров. Когда компьютер заходит в сеть, он не только сообщает об этом всем остальным, но и заносит имена всех подключенных к сети компьютеров в свою динамическую таблицу.

В силу своей простоты NetBIOS является одним из самых быстрых протоколов, и это его сильная сторона.

На самом деле NetBIOS не является полноценным протоколом, поскольку описывает только программную часть передачи данных — набор сетевых API-функций. Это означает, что, используя его, можно только подготовить данные для передачи. Физическая же передача осуществляется только с помощью любого транспортного протокола. В частности, обычно в паре с протоколом NetBIOS используется транспортный протокол NetBEUI.

Плюсом этой технологии является непривязанность к транспортному протоколу, что позволяет использовать любой другой подходящий для этих целей протокол. Кроме того, неоспоримым достоинством является его быстродействие.

Недостаток же заключается в том, что для полноценной работы NetBIOS требуется, чтобы на всех компьютерах сети стоял одинаковый транспортный протокол, иначе машины не смогут синхронизироваться. Еще один минус протокола — отсутствие поддержки маршрутизации, без которой не обходится любая сеть сложной топологии. Именно поэтому протокол NetBIOS, как правило, находит свое применение только в сетях малого размера, обычно в одноранговых.

Протокол NetBEUI

NetBEUI (NetBIOS Extended User Interface) — транспортный протокол, «брат» NetBIOS, его расширение. Однако он обладает большей надежностью доставки сообщений и устойчивостью к ошибкам. Достигается все это путем подтверждающих пакетов, каждый раз присылаемых в ответ на полученное сообщение. Кроме того, до начала передачи устанавливается логическая связь между компьютером-отправителем и компьютером-получателем, что уже гарантирует доставку пакетов.

Еще один механизм, обеспечивающий надежность передачи данных, — механизм, отслеживающий время «жизни» пакета (TTL). Если по истечении этого времени компьютер-получатель не пришлет подтверждение о доставке очередного пакета данных, компьютер-отправитель отсылает порцию данных повторно. Аналогично повторная передача происходит и в случае, если пакет оказался поврежденным и компьютер-получатель его отклоняет, о чем и сообщает компьютеру-отправителю.

Так же как и NetBIOS, NetBEUI не поддерживает маршрутизацию в сети, что не позволяет эффективно использовать его скорость и применять в глобальных сетях. Тем не менее этот протокол является одним из основных компонентов NT-систем и его установка происходит автоматически.

Протокол IPX/SPX

IPX и SPX являются представителями стека протоколов, разработанных компанией Novell, которая в свое время являлась прямым конкурентом Microsoft. Конкуренция велась в области сетевых операционных систем: с одной стороны стояла операционная система Novell Netware, с другой — Windows NT. Соответственно каждая из этих систем использовала свой набор протоколов.

К сожалению, со временем Novell сдала свои позиции и первенство завоевали сетевые версии операционных систем Windows NT. Тем не менее разработанные Novell протоколы используются до сих пор и будут использоваться еще очень долго.

IPX/SPX представляет собой набор подпротоколов, каждый из которых может выполнять возложенную на него задачу на высоком уровне (рис. 3.2). Два нижних уровня (физический и сетевой) реализуют стандартные протоколы Ethernet.

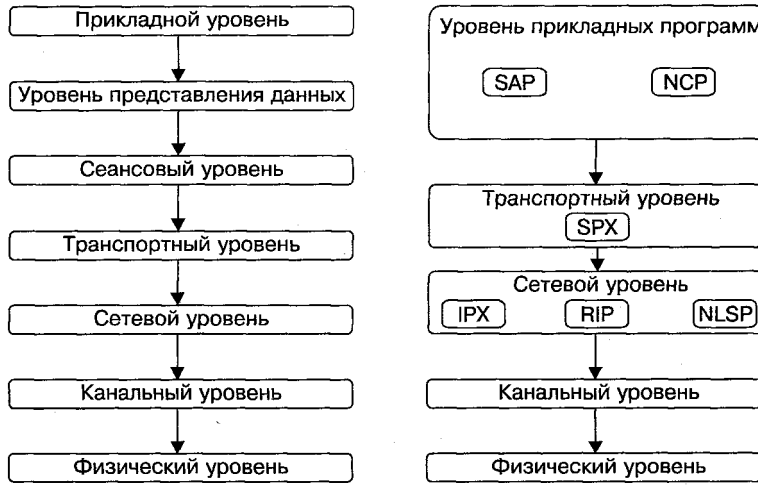


Рис. 3.2. Распределение протоколов стека IPX/SPX по уровням модели ISO/OSI

Ниже описаны только некоторые из протоколов, входящих в состав стека протоколов IPX/SPX.

IPX (Internetwork Packet Exchange) — отвечает за работу сетевого уровня. Его основные функции — вычисление адресов компьютеров сети и организация маршрутизации между двумя выбранными машинами. Анализируя данные других протоколов, IPX составляет наиболее эффективный путь маршрутизации. После этого пакет данных (датаграмма[1]) с добавленной информацией об адресе получателя и отправителя идет по выбранному маршруту. К сожалению, этот протокол самостоятельно работать не может, поскольку

[1] В работе протокол использует понятие «датаграмма» — пакет данных, снабженных служебной информацией о получателе и отправителе.

не устанавливает соединение между компьютерами. Без этого нельзя ожидать от него надежной доставки пакетов.

SPX (Sequenced Packet Exchange) — протокол транспортного уровня. Он отвечает за установку соединения между выбранными компьютерами и передает сообщения — датаграммы.

SAP (Service Advertising Protocol) — отвечает за работу сразу трех уровней: прикладного, представления и сеансового. Однако одна из основных его функций — рассылка сообщений о доступных сервисах. Благодаря этому все сетевые устройства знают об имеющихся сетевых сервисах. SAP — очень мощное средство организации службы поддержки, однако это и является его основным недостатком. Поскольку любое сетевое устройство постоянно посылает о себе информацию, это приводит к повышению трафика сети и соответственно снижению ее эффективности. Для уменьшения засорения сети используют возможности маршрутизаторов, которые позволяют фильтровать «чужие» SAP-сообщения.

NCP (NetWare Core Protocol) — протокол верхнего (прикладного) уровня. Он отвечает за взаимодействие сервера операционной системы Novell NetWare и рабочей станции. С его помощью пользователь видит любую нужную информацию о ресурсах сети, открывает, изменяет и сохраняет файлы, меняет их атрибуты, удаляет, копирует и т. д.

Протокол TCP/IP

TCP/IP — самый распространенный протокол транспортного уровня как в локальных, так и в глобальных сетях. В свое время он был разработан Министерством обороны США, что уже говорит о его надежности.

Протокол TCP/IP имеет открытый интерфейс. Это означает, что вся информация об этом протоколе открыта и любой может использовать ее по своему желанию и назначению.

На самом деле TCP/IP состоит из нескольких протоколов.

Как вы уже заметили, в его названии есть разделитель, то есть он состоит из названий двух протоколов. Первый из них — TCP (Transmission Control Protocol), второй — IP (Internet Protocol). Это говорит о том, что в нем участвует по меньшей мере два протокола (рис. 3.3).

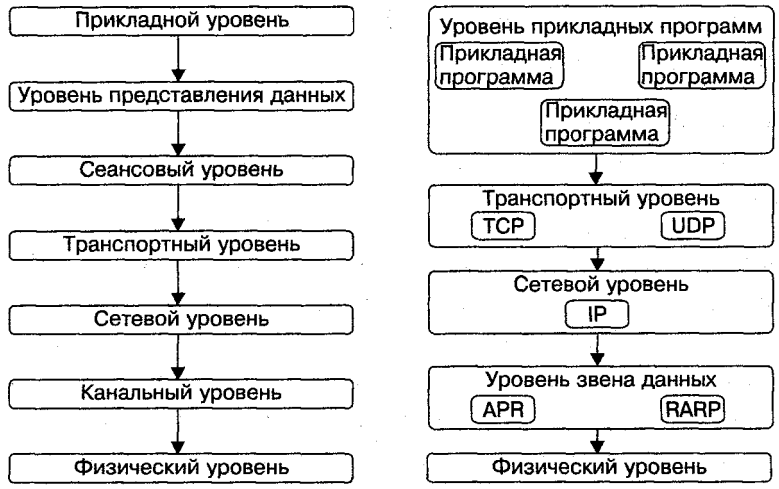


Рис. 3.3. Распределение протоколов стека TCP/IP по уровням модели ISO/OSI

На самом деле в стеке TCP/IP участвует намного больше протоколов. Это связано с тем, что каждый из них предназначен для выполнения определенных задач. Как известно, лучше иметь несколько механизмов, работа которых отлажена до мелочей, нежели один большой, но вызывающий неполадки.

Ниже описаны некоторые протоколы, входящие в стек TCP/IP.

TCP (Transmission Control Protocol) осуществляет обмен данными между двумя компьютерами с предварительно установленной логической связью. Он постоянно используется в Интернете, поскольку надежность соединения и универсальность в этом случае играют очень большую роль. Кроме того, TCP обеспечивает надежность доставки сообщений, принимая подтверждение доставки каждой его порции путем подтверждающих пакетов, каждый раз присылаемых в ответ на полученное сообщение. При этом в самом начале устанавливается логическая связь между компьютером-отправителем и компьютером-получателем, что уже гарантирует доставку пакетов.

UDP (User Datagram Protocol) — при использовании этого протокола не нужно иметь установленное логическое соединение двух компьютеров. Когда передаются данные другому компьютеру, предполагается, что он где-то есть, то есть подключен к сети. В этом случае нет никакой гарантии, что обмен данными произойдет. При этом к отсылаемому пакету просто добавляется IP-адрес машины, которой нужно отослать сообщение. Если сообщение принято, присылается подтверждение об этом, иначе отсылка данных повторяется через некоторый

промежуток времени. Как ни странно, протокол UDP применяется в сети достаточно часто. Благодарить за это нужно скорость его работы, которая достигается за счет того, что не устанавливаются соединения с другими компьютерами, а это позволяет использовать трафик в нужном направлении. Так, данный протокол часто используют в сетевых играх, для передачи звуковых данных интернет-радио и в других случаях, где надежность доставки пакетов не играет большой роли.

IP (Internet Protocol) — протокол более высокого уровня, чем TCP и UDP. Он используется непосредственно для передачи данных по ранее установленному (или не установленному) соединению и имеет механизмы маршрутизации. Пользуясь информацией о маршрутизации между выбранными компьютерами, он просто добавляет адрес отправителя и получателя к пакету и отсылает его дальше. Наиболее востребованной функцией протокола является разбивка большого пакета на более мелкие на одном компьютере и соответственно соединение всех частей на другом. Это значит, что IP не контролирует доставку сообщений конечному адресату. IP-адреса машины-отправителя и машины-получателя включаются в заголовок датаграммы и используются для ее передачи между шлюзами. При этом информация о маршрутизации, находящаяся на шлюзе, указывает, куда передавать датаграмму на каждом этапе.

ICMP (Internet Control Message Protocol) контролирует протокол IP, отслеживает любые изменения, влияющие на процесс маршрутизации. При возникновении каких-либо ошибок об этом узнают и отправитель, и получатель. При этом в сообщении указывается причина сбоя.

RIP (Routing Information Protocol) — «родной брат» протокола IP. Они оба связаны с маршрутизацией. Тем не менее протокол RIP отвечает за выбор наилучшего маршрута доставки данных.

ARP (Address Resolution Protocol) — работает с адресами компьютеров, то есть определяет фактический адрес машины, расположенной в той или иной ветке сети. Например, если нужно узнать физический адрес в сети Ethernet, имея при этом IP-адрес, ARP конвертирует 32-битный IP-адрес в 48-битный Ethernet-адрес.

DNS (Domain Name System) — важнейший протокол, который позволяет определять адрес компьютера, ориентируясь на его логическое имя.

RARP (Revere Address Resolution Protocol) — протокол, определяющий адрес компьютера в сети. Работает аналогично протоколу ARP, однако конвертирование происходит в обратном порядке, то есть 48-битный Ethernet-адрес конвертируется в 32-битный IP-адрес.

BOOTP (Boot Protocol) — относится к прикладному уровню. С его помощью можно запустить сетевой компьютер, используя данные о загрузке с сервера.

FTP (File Transfer Protocol) — протокол, который позволяет загружать файлы с одного компьютера на другой. Именно его вы используете каждый раз, когда пытаетесь выгрузить или загрузить файл с FTP-сервера в Интернет.

TELNET — используется для связи между двумя компьютерами с целью управления одним из них. Протокол очень эффективен в действии и позволяет связывать любые два компьютера, где бы они ни находились.

Кроме описанных, существует набор протоколов, отвечающих за разные аспекты функционирования сети, в частности администрирование, работу с электронной почтой и т. п.

Имея в составе мощный набор вспомогательных протоколов, TCP/IP не зря так популярен. К тому же сегодня это единственный эффективный протокол, который используется для работы в Интернете.

3.3. Протоколы работы с электронной почтой

Без этих протоколов невозможна работа электронной почты. Что такое электронная почта и как без нее плохо, объяснять, пожалуй, не нужно.

Особенностью этих протоколов является их узкая направленность — использование для других целей принципиально невозможно, да и не имеет смысла. Их задача — организация обмена электронными сообщениями.

Еще одной особенностью почтовых протоколов является однозадачность: например, протокол, умеющий отсылать сообщения, не умеет их принимать, и наоборот. Именно поэтому такие протоколы работают парами.

SMTP (Simple Message Transfer Protocol) — почтовый протокол для передачи электронных сообщений. Он накапливает письма и рассылает их по тем адресам, которые указаны в заголовках.

Благодаря своей простоте[1] и возможностям, SMTP завоевал достойное место под солнцем. Есть, конечно, и недостатки, основной из которых — отсутствие механизма аутентификации входящих соединений и шифрования передачи данных между серверами.

SMTP рассчитан на передачу только текстовой информации, поэтому для отсылки файлов разработан стандарт UUENCODE. Благодаря этому дополнению также появляется возможность использовать разную кодировку писем. Однако и UUENCODE не является полноценным дополнением, поскольку при кодировании файла в текстовый формат теряется информативность, то есть его эмоциональный характер, формат и т. п.

Поэтому вместе с SMTP работает еще одно расширение почты — MIME (Multipurpose Internet Mail Extension), выполняющее больше функций.

Достоинством протокола SMTP является возможность отправлять сообщения с любым форматом вложения, будь то простой текстовый файл или файл с любимой песней. Однако у всего есть свои недостатки — сообщение, прошедшее через кодовую обработку UUENCODE, увеличивается в размере в среднем на 30 %.

Перед тем как отправить письмо, SMTP устанавливает предварительное соединение с адресатом, что позволяет ему получить письмо в кратчайшие сроки. В случае если адресат, указанный в заголовке письма, не найден, пользователь получает об этом сообщение от почтового сервера.

POP[2] (Post Office Protocol) — один из самых распространенных почтовых протоколов. С его помощью пользователь может загружать адресованные ему письма с почтового сервера.

Данный протокол имеет простой интерфейс, который на все запросы отвечает недвусмысленно: **OK** или **ERR**. Возможно, это и не позволяет использовать некоторые желательные функции, например чтение писем без копирования их на локальный компьютер или выборочный прием писем. Для выполнения этих и других полезных функций вместе с POP используют протокол IMAP.

---

[1] Именно так переводится с английского полное название протокола — «простой протокол передачи сообщений».

[2] В настоящее время распространена третья версия протокола, поэтому он носит название POP3.

IMAP (Interactive Mail Access Protocol) — еще один почтовый протокол. Он был разработан позже протокола POP3, что позволило учесть все недостатки и добавить много новых востребованных функций.

Наиболее полезными среди них являются скачивание заголовков сообщений, анализируя которые можно эффективно настраивать фильтры, сортирующие письма или отсеивающие спам.

Еще одно немаловажное нововведение — механизм оптимизации использования каналов, по которым передаются сообщения. Эти каналы не всегда быстрые и незагруженные, поэтому наличие такой функции существенно облегчает жизнь пользователя. Также имеется возможность передачи сообщений по частям, что очень полезно, когда размер письма большой, например 5–10 Мбайт.

3.4. Другие протоколы

HTTP. О протоколе HTTP вы, скорее всего, слышали. Именно он является одним из прародителей обмена информацией в Интернете. Каждый раз, переходя с одной веб-страницы на другую или выбирая ссылку, вы тем самым приводите в действие механизм, который напрямую связан с HTTP-протоколом.

Особенностью протокола является то, что он может передавать любую информацию — текстовую и графическую. Это позволяет использовать дополнительные средства в разработке веб-страниц и веб-ресурсов, делая их оформление разнообразным, красочным и даже анимированным.

FTP (File Transfer Protocol) — «собрат» HTTP-протокола, так как они всегда работают вместе. Главное отличие заключается в том, что FTP-протокол был разработан специально для передачи файлов в Интернете. Каждый раз, скачивая, например, музыку или нужные документы, вы пользуетесь услугами механизмов FTP-протокола. Представить себе Интернет без FTP невозможно.

SLIP (Serial Line Internet Protocol) создан специально для организации постоянного подключения к Интернету с использованием имеющейся телефонной линии и обычного модема. Из-за высокой стоимости этот тип подключения могут позволить себе не многие пользователи. Как правило, такое подключение применяется в организациях, имеющих серверы, на которых находятся их веб-страницы и другие ресурсы (базы данных, файлы).

Данный протокол работает вместе с протоколом TCP/IP, находясь на более низком уровне. Перед тем как информация с модема поступит на обработку TCP/IP-протоколу, ее предварительно обрабатывает SLIP-протокол. Выполнив все необходимые действия, он создает другой пакет и передает его TCP/IP.

В другую сторону формирование пакетов происходит в обратном порядке. Получив пакет данных от TCP/IP, SLIP создает другой пакет, предварительно выбрав всю ценную информацию.

PPP (Point-to-Point Protocol) выполняет ту же работу, что и описанный выше SLIP. Однако он более приспособлен к ней, так как обладает дополнительными функциями. Кроме того, в отличие от SLIP, PPP может взаимодействовать не только с TCP/IP, но и с IPX/SPX, NetBIOS, DHCP, которые получили распространение в локальных сетях.

Протокол PPP более распространен также благодаря использованию на веб-серверах с установленной операционной системой Windows NT (SLIP применяют для соединения с серверами, работающими в операционной системе UNIX).

X.25 был создан в 1976 году и усовершенствован в 1984-м, работает на физическом, канальном и сетевом уровнях модели взаимодействия ISO/OSI. Его разработкой занимался консорциум, состоящий из представителей многих телефонных компаний, и создавали его специально для использования на существующих телефонных линиях.

Учитывая год создания протокола, а соответственно и качество тогдашних телефонных линий, можно с уверенностью сказать, что протокол X.25 — один из самых надежных. Когда создавался X.25, цифровая телефонная линия была редкостью — использовалась в основном аналоговая. По этой причине в нем присутствует система обнаружения и коррекции ошибок, что существенно повышает надежность связи. В то же время она замедляет скорость передачи данных (максимальная — 64 Кбит/с). Однако этот факт не мешает использовать его там, где прежде всего требуется высокая надежность, например в банковской системе.

Frame Relay — еще один протокол, предназначенный для передачи данных по телефонной линии, который, кроме высокой надежности X.25, обладает дополнительными полезными нововведениями. Поскольку передаваемые данные могут иметь формат видео, аудио или содержать электронную информацию, есть возможность выбирать приоритет пересылаемого содержимого.

Еще одна особенность протокола Frame Relay — его скорость, которая достигает 45 Мбит/с.

AppleTalk является собственностью компании Apple Computer, был разработан для установки связи между компьютерами Macintosh.

Так же как и TCP/IP, протокол AppleTalk представляет собой набор протоколов, каждый из которых отвечает за работу определенного уровня модели ISO/OSI.

В отличие от протоколов TCP/IP и IPX/SPX, стек протокола AppleTalk использует собственную реализацию физического и канального уровней, а не протоколы модели ISO/OSI (рис. 3.4).

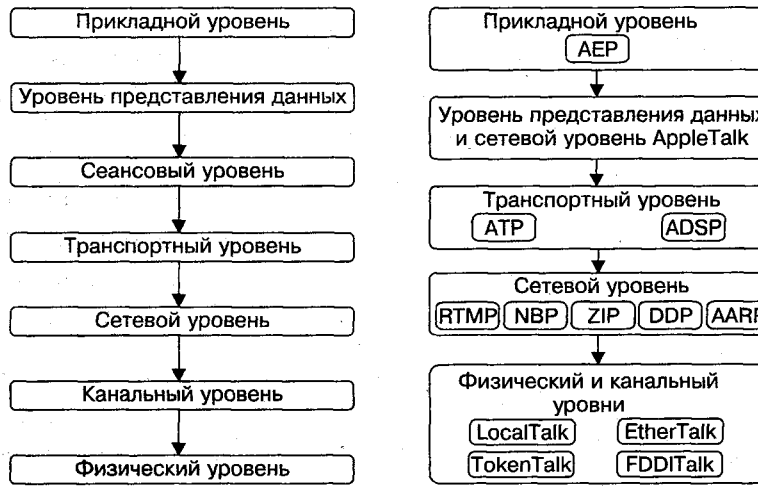


Рис. 3.4. Распределение протоколов стека AppleTalk по уровням модели ISO/OSI

Рассмотрим протоколы стека AppleTalk.

- **DDP** (Datagram Delivery Protocol) — отвечает за работу сетевого уровня. Его основное предназначение — организация и обслуживание процесса передачи данных без предварительной установки связи между компьютерами.
- **RTMP** (Routing Table Maintenance Protocol) — работает с маршрутными таблицами AppleTalk. Любая такая таблица содержит информацию о каждом сегменте, куда возможна доставка сообщений. Таблица состоит из номеров маршрутизаторов (порта), которые могут доставить сообщение

к выбранному компьютеру, количества пунктов «пересадки»[1], параметров выбранных сегментов сети — скорости, загруженности и т. п.

- **NBP** (Name Binding Protocol) — отвечает за адресацию, которая сводится к привязке логического имени компьютера к физическому адресу в сети. Кроме процесса привязки имени, он отвечает за регистрацию, подтверждение, стирание и поиск этого имени.
- **ZIP** (Zone Information Protocol) — протокол, работающий в паре с NBP, помогая ему производить поиск имени в рабочих группах, или зонах. Для этого он использует информацию ближайшего маршрутизатора, который создает запрос по всей сети, где могут находиться компьютеры, входящие в заданную рабочую группу.
- **ATP** (AppleTalk Transaction Protocol) — один из протоколов транспортного уровня, который отвечает за транзакции. Транзакция — это набор из запроса, ответа на этот запрос и идентификационного номера, который присваивается данному набору. Примером транзакции может быть сообщение о доставке данных от одного компьютера другому. Кроме того, ATP умеет делать разбивку больших пакетов на более мелкие с последующей их сборкой после подтверждения о приеме или доставке.
- **ADSP** (AppleTalk Data Stream Protocol) — протокол, аналогичный ATP, отвечающий за доставку пакетов. Однако в данном случае осуществляется не одна транзакция, а гарантированная доставка, которая может повлечь за собой несколько транзакций. Кроме того, протокол гарантирует, что данные при доставке не будут утеряны или продублированы.

---

[1] Количество других маршрутизаторов, которые будут задействованы для доставки сообщения выбранному компьютеру.

Глава 4

Сетевое оборудование

- Сетевой адаптер
- Концентратор
- Мост
- Коммутатор
- Маршрутизатор
- Модем
- Точка доступа
- Антенна
- Сетевой кабель
- Коннекторы, розетки, инструменты...

Компьютерная сеть не может существовать без сетевых устройств. Каждое из них имеет свое предназначение, что позволяет четко разделить функции поддержки работы сети. Обычный пользователь может даже не знать, какие именно устройства применяются. Единственное, с чем он сталкивается, — это сетевая карта, установленная (или встроенная) в материнскую плату его компьютера. Тем более не обязательно знать, как все это функционирует. Однако если вы любознательный человек, то знание основ работы сетевых устройств вам не помешает и даже пригодится. Кроме того, подобные знания будут совсем не лишними для человека, который будет выступать в роли администратора сети.

4.1. Сетевой адаптер

Чтобы пользователь мог подключиться к локальной сети, в его компьютере должно быть установлено специальное устройство — сетевой контроллер (адаптер, карта).

Сетевой адаптер выполняет множество заданий, самые главные из которых — кодирование информации и получение доступа к информационной среде с использованием уникального идентификатора (MAC-адреса).

Сетевые карты бывают в виде плат расширения, которые устанавливаются в соответствующий слот (рис. 4.1), или могут быть встроенными в материнские платы (рис. 4.2).

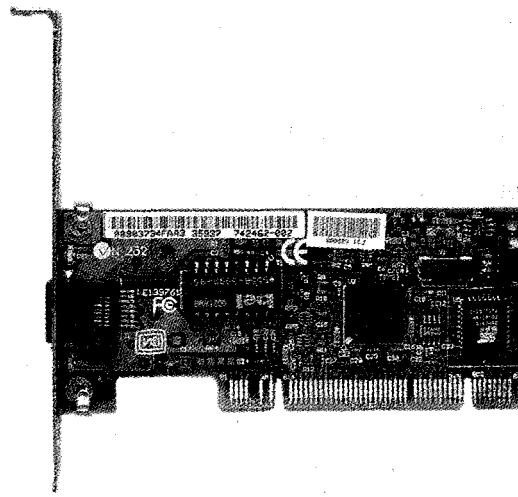


Рис. 4.1. Сетевая карта в виде платы расширения, устанавливаемой в PCI-слот

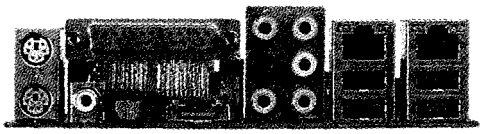


Рис. 4.2. Пример встроенной сетевой карты (два коннектора сверху в правой части)

Сетевые платы различаются по трем основным параметрам.

- **Скорость передачи данных.** Поскольку существуют сети с различными скоростями приема и передачи информации, естественно, существуют аналогичные сетевые адаптеры. Наибольшее распространение в странах СНГ получили сети Ethernet и Fast Ethernet, построенные на витой паре или коаксиальном кабеле (встречаются реже), имеющие пропускную способность 100 и 10 Мбит/с соответственно. Также в последнее время все чаще встречаются локальные сети, работающие со скоростью 1 Гбит/с. Как правило, сетевой адаптер с более высокой скоростью передачи данных также умеет работать и на более низких скоростях. К примеру, если сеть функционирует на скорости 10 Мбит/с, 100-мегабитный сетевой адаптер также будет работать на скорости 10 Мбит/с.
- **Тип коннектора.** Тип коннектора сетевой карты зависит от выбора сетевой топологии и кабеля, по которому происходит передача данных. Существует несколько типов коннекторов: RJ-45 для витой пары, BNC для коаксиального кабеля и ST, SC или FC для оптоволокна. Они существенно различаются по конструкции, поэтому использовать коннектор не по назначению невозможно. Хотя существуют комбинированные сетевые адаптеры, которые содержат, например, RJ-45- и BNC-коннекторы. Но поскольку сети на коаксиальном кабеле встречаются все реже, то и адаптеры такие попадаются нечасто. Сегодня сети на основе витой пары составляют примерно 90 %.
- **Тип подключения к компьютеру.** Сетевая карта может устанавливаться в PCI-слот или в USB-порт (рис. 4.3). Кроме этого практически любая современная материнская плата имеет интегрированный сетевой контроллер.

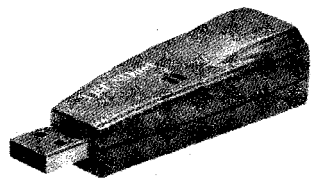


Рис. 4.3. Сетевая карта, подключаемая к USB-порту

Что касается сетевых адаптеров (рис. 4.4) для беспроводной сети, то по внешнему виду они практически не отличаются от проводных, за исключением наличия гнезда антенны — внутренней или внешней.

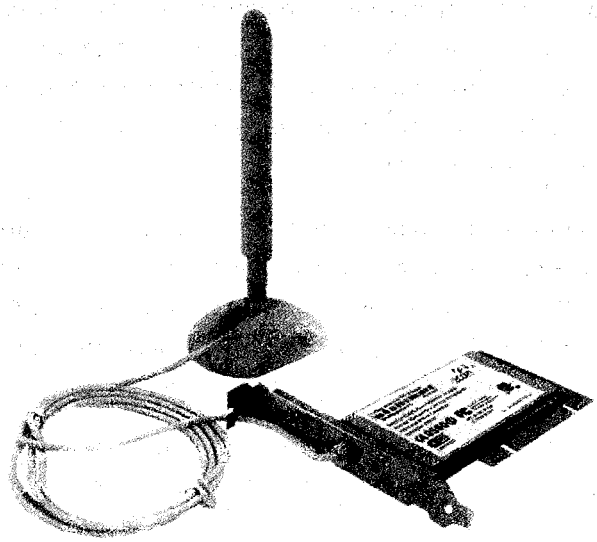


Рис. 4.4. Беспроводной сетевой адаптер

Что касается сетевых плат, которые подключают через USB-порт, они встречаются достаточно часто, особенно это касается беспроводных вариантов.

Часто на сетевой карте присутствует микросхема BIOS, с помощью которой можно даже производить загрузку компьютера или выводить его из спящего режима (функция WOL, wake up on LAN). В последнем случае сетевая карта должна быть подсоединена к материнской плате специальным кабелем.

4.2. Концентратор

Когда сеть содержит более двух компьютеров, для их объединения приходится использовать специальное устройство — концентратор. Свое применение он находит, как правило, в сетях на основе витой пары.

Концентратор (также используются названия «хаб», «повторитель», «репитер») — сетевое устройство, имеющее два и более разъема (порта), которое, кроме коммутации подключенных к нему компьютеров, выполняет и другие функции, например усиление сигнала.

Концентратор служит для расширения сети, и основное его предназначение — передача поступившей на вход информации остальным подключенным к нему устройствам сети.

Все подключенные к концентратору устройства получают абсолютно одинаковую информацию, что одновременно является и недостатком устройства — наличие нескольких концентраторов в сети засоряет эфир, поскольку концентратор не видит реального адреса, по которому нужно отослать сообщение, и вынужден передавать его всем.

В любом случае концентратор выполняет свою задачу — соединяет компьютеры, находящиеся в одной рабочей группе. Кроме того, он производит анализ ошибок, в частности, возникающих коллизий. Если одна из сетевых карт приводит к возникновению частых коллизий, порт на концентраторе, к которому она подключена, может временно отключаться.

Концентратор реализует физический уровень модели ISO/OSI, на котором работают стандартные протоколы, поэтому использовать его можно в сети любого стандарта.

Существует два основных типа концентраторов.

- **Концентраторы с фиксированным количеством портов** (рис. 4.5) — самые простые. Выглядит такой концентратор как отдельный корпус, снабженный определенным количеством портов и работающий на выбранной скорости. Как правило, один из портов служит для связи с другим концентратором или коммутатором.

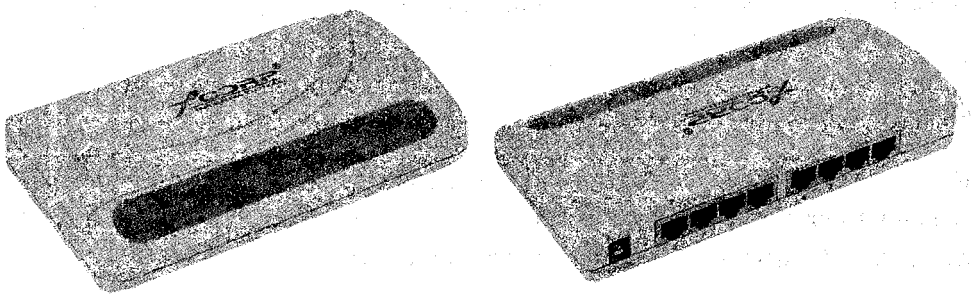


Рис. 4.5. Концентратор с фиксированным количеством портов

- **Модульные концентраторы** (рис. 4.6) состоят из блоков, которые устанавливаются в специальное шасси и объединяются общей шиной. Возможна

также установка концентраторов, которые не связаны между собой общей шиной, например, когда существуют разные локальные сети, связь между которыми не принципиальна.

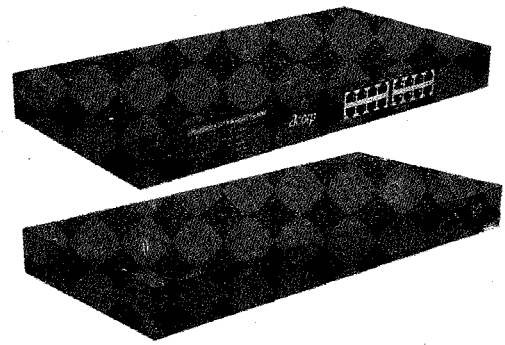


Рис. 4.6. Модульный концентратор

Модульный концентратор выглядит практически так же, как концентратор с фиксированным количеством портов. Единственное возможное отличие — пластмассовый корпус. Количество портов в таких конструкциях не обязательно должно быть одинаковым. Кроме того, каждый концентратор может работать со своей топологией сети.

Преимуществом модульного концентратора является сосредоточение всех устройств в едином центре управления. Это позволяет быстро делать соответствующие настройки в случае любых изменений в сети.

Поскольку для создания сети в основном используют коаксиальный кабель и кабель на основе витой пары, соответственно существуют и концентраторы с BNC- и RJ-45-портами.

В зависимости от сложности концентратора на нем может присутствовать консольный порт (рис. 4.7), с помощью которого, используя специальное программное обеспечение, можно изменять некоторые параметры, конфигурировать порты или считывать их статистику.

Концентраторы могут содержать разное количество портов — от 5 до 48. Чем их больше, тем дороже и функциональнее устройство. В частности, существуют конструкции, позволяющие управлять концентратором напрямую (то есть не используя консольный порт) или поддерживающие резервную линию соединения с другими устройствами.

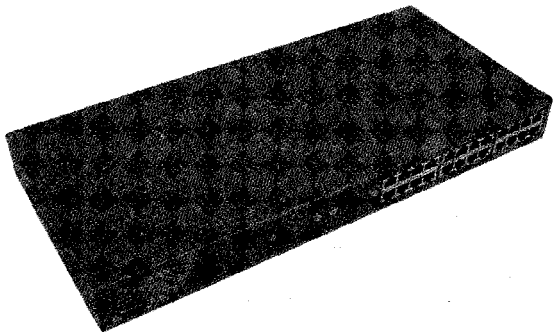


Рис. 4.7. Концентратор с консольным портом (в левой части)

Часто на концентраторе есть дополнительный порт, через который можно соединять другие сегменты сети, в частности сеть на коаксиальном кабеле, на основе витой пары или радиосеть.

4.3. Мост

Мост (также используются названия «свич», «переключатель») представляет собой довольно простое устройство (рис. 4.8), основное предназначение которого — разделение двух сегментов сети с целью увеличения ее общей длины (соответственно количеству подключенных повторителей) и преодоления при этом ограничения сетевой топологии.

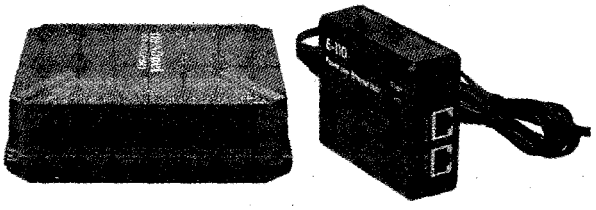


Рис. 4.8. Беспроводной мост

В отличие от концентраторов, мост умеет передавать отдельные (отфильтрованные) пакеты, что позволяет уменьшить трафик информации.

Как правило, мост имеет два или больше портов, к которым подключают сегменты сети. Анализируя адрес получателя пакета, он может фильтровать сообщения, предназначенные другому сегменту. Пакеты, предназначенные для родного сегмента, устройство попросту игнорирует, что также уменьшает трафик.

Для построения сети используют три типа мостов:

- **локальный** — работает только с сегментами одного типа, то есть имеющими одинаковую скорость передачи данных;
- **преобразующий** — предназначен для того же, что и локальный мост, также работает с разнородными сегментами, например Token Ring и 100Base;
- **удаленный** — соединяет сегменты, расположенные на значительном расстоянии друг от друга, при этом могут использоваться любые средства соединения, например модем.

Мост может использоваться как в проводных, так и в беспроводных сетях.

4.4. Коммутатор

Коммутатор (рис. 4.9) объединяет в себе возможности концентратора и моста, а также выполняет еще некоторые полезные функции.

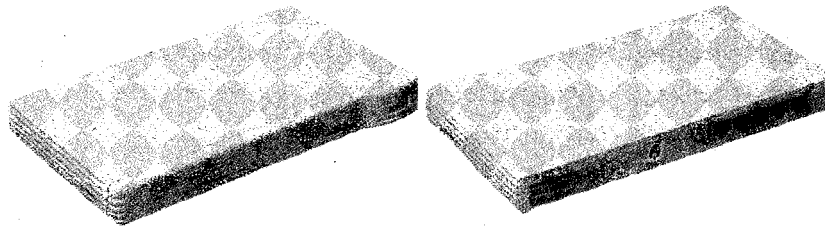


Рис. 4.9. Коммутатор

Например концентратор, получив от какой-либо сетевой карты пакет данных, не зная о том, кому он адресован, рассылает его по всем подключенным к нему сетевым устройствам. Не сложно представить, какой создается трафик, если в сети существует не один, а несколько концентраторов.

Коммутатор — более интеллектуальное устройство, которое не только фильтрует поступающие пакеты, но, имея таблицу адресов всех сетевых устройств, точно определяет, какому эти пакеты предназначены. Это позволяет ему передавать информацию сразу нескольким устройствам.

Поэтому для организации разветвленной сети концентраторы и коммутаторы используют совместно. Первые — для объединения компьютеров в одну группу, вторые — для организации эффективного обмена информацией между ними.

Коммутаторы работают на канальном уровне, что позволяет использовать их не только в разных типах сетей, но и объединять различные сети в одну.

Коммутатор может использоваться как в проводных, так и в беспроводных сетях.

4.5. Маршрутизатор

Главная задача маршрутизатора (роутера) — разделение большой сети на подсети. Он выполняет множество полезных функций и обладает большими возможностями. В нем сочетаются концентратор, мост и коммутатор. Кроме того, добавляется возможность маршрутизации пакетов. В связи с этим маршрутизатор (рис. 4.10) работает на более высоком уровне — сетевом.

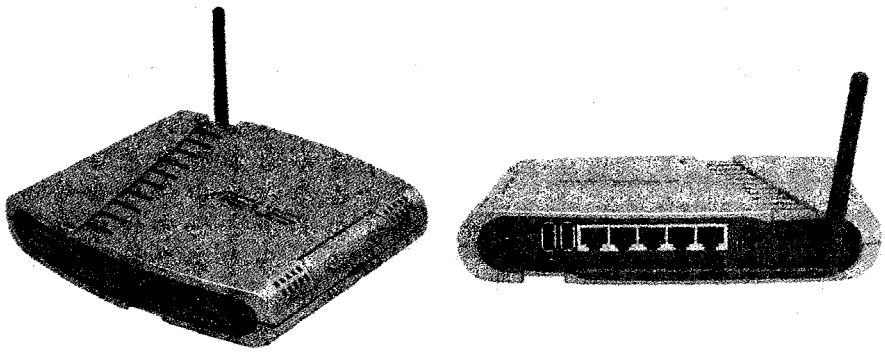


Рис. 4.10. Беспроводной маршрутизатор

Таблица возможных маршрутов движения пакетов все время обновляется, что дает маршрутизатору возможность выбирать самый короткий и самый надежный путь доставки сообщения.

Одной из ответственных задач является связь разнородных сетевых сегментов локальной сети. С помощью маршрутизатора также можно организовывать виртуальные сети, каждая из которых будет иметь доступ к тем или иным ресурсам, в частности к Интернету.

Организация фильтрования широковещательных сообщений в маршрутизаторе выполнена на более высоком уровне, чем в коммутаторе. Все протоколы, которые использует сеть, беспрепятственно принимает и обрабатывает процессор маршрутизатора. Даже если попался незнакомый протокол, устройство быстро научится с ним работать.

Маршрутизатор может использоваться в проводных и беспроводных сетях. Часто функции маршрутизации ложатся на беспроводные точки доступа.

4.6. Модем

Модем также является сетевым оборудованием, и его до сих пор часто используют для организации выхода в Интернет.

Слово «модем» — сокращение от «модулятор» и «демодулятор».

Модем представляет собой устройство, которое имеет цифровой интерфейс связи с компьютером и аналоговый интерфейс для связи с телефонной линией (цифро-аналоговые и аналогово-цифровые преобразования).

Модем состоит из процессора, памяти, аналоговой части, ответственной за сопряжение с телефонной сетью, и контролера, который всем управляет.

Обмен информацией происходит по обычной телефонной линии в диапазоне частот 300–3400 Гц. Преобразование аналогового сигнала осуществляется достаточно просто — с определенной частотой его характеристики измеряются и записываются в цифровой форме по определенному алгоритму. В обратной последовательности идет преобразование цифровой информации.

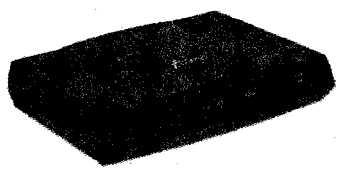


Рис. 4.11. Внешний модем

Модемы бывают двух типов: внешние (рис. 4.11) и внутренние (рис. 4.12). Внутренние представляют собой плату расширения, которую обычно устанавливают в PCI-слот. Внешний же модем может подключаться к компьютеру через LPT-, COM-, USB-порт или вход сетевой карты.

Модемы могут работать с телефонной линией, с выделенной линией и радиоволнами.

В зависимости от типа устройства и среды передачи данных отличается и скорость этой передачи. Скорость обычного цифро-аналогового модема, работающего с телефонной аналоговой линией, приблизительно 33,6–56 Кбит/с. В последнее время все чаще встречаются цифровые модемы, использующие преимущества DSL-технологии. При использовании таких модемов возможна работа на скорости до 24 Мбит/с. Еще одним неоспоримым плюсом этих модемов является то, что телефонная линия всегда остается свободной.

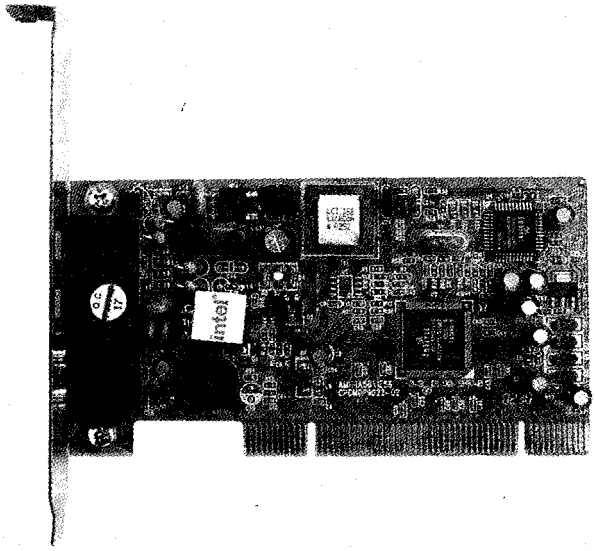


Рис. 4.12. Внутренний модем

Для связи с другим модемом используются свои протоколы и алгоритмы. Большое внимание при этом уделяется качеству обмена информацией, поскольку качество линий при этом достаточно низкое.

Модем может использоваться как в проводных, так и в беспроводных сетях.

4.7. Точка доступа

Точка доступа (рис. 4.13) — устройство, необходимое для организации беспроводной сети в инфраструктурном режиме. Она играет роль концентратора и позволяет компьютерам обмениваться нужной информацией, используя для этого таблицы маршрутизации, средства безопасности, встроенный аппаратный DNS- и DHCP-сервер и многое другое.

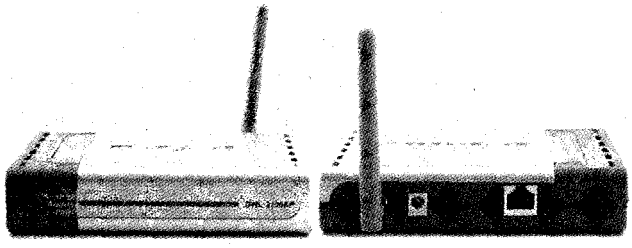


Рис. 4.13. Точка доступа

От точки доступа зависит не только качество и устойчивость связи, но и стандарт беспроводной сети. Существует большое количество разнообразнейших моделей точек доступа с разными свойствами и аппаратными технологиями. Однако на сегодняшний день наиболее оптимальными можно считать устройства, работающие со стандартом IEEE 802.11g, поскольку он совместим со стандартами IEEE 802.11a и IEEE 802.11b и позволяет работать на скорости до 108 Мбит/с.

4.8. Антенна

В беспроводной сети антенна имеет огромное значение, особенно если к ней подключено активное сетевое оборудование: точка доступа, концентратор, маршрутизатор и т. д. Хорошая антенна позволяет сети работать с максимальной отдачей, достигая при этом своих теоретических пределов дальности распространения сигнала.

Антенны бывают внутренние (встроенные) и внешние (рис. 4.14) и отличаются в основном своей направленностью и мощностью. Так, узконаправленная антенна позволяет достичь более дальней связи, что и используют, когда необходимо соединить два удаленных сегмента беспроводной сети.

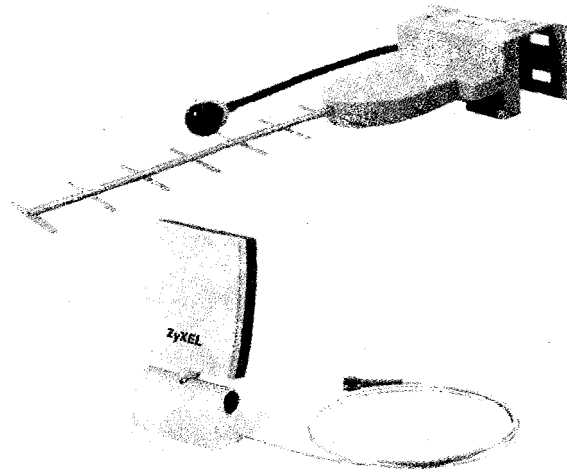


Рис. 4.14. Антенна для беспроводного оборудования

Широконаправленная антенна распространяет сигнал вокруг себя, что позволяет другим рядом установленным устройствам взаимодействовать друг с другом. Однако достичь каких-либо выдающихся результатов при этом не удается.

4.9. Сетевой кабель

Если в беспроводной сети для передачи данных используют радиоэфир, то в проводной сети, соответственно, кабель. Существует несколько типов кабелей, основными из которых являются кабель на основе витой пары, коаксиальный и оптоволоконный кабель.

Существует несколько категорий кабелей, каждая из которых имеет свои характеристики. Основными отличительными параметрами являются:

- частотная полоса пропускания;
- диаметр проводников;
- диаметр проводника с изоляцией;
- количество проводников (пар);
- наличие экрана вокруг проводника (проводников);
- диаметр кабеля;
- диапазон температур, при котором качественные показатели находятся в норме;
- минимальный радиус изгиба, который допускается при прокладке кабеля;
- максимально допустимые наводки в кабеле;
- волновое сопротивление кабеля;
- максимальное затухание сигнала в кабеле.

Все эти параметры входят в понятие категории кабеля. Например, кабель на основе витой пары бывает пяти разных категорий. В этом случае чем выше категория, тем лучше показатели кабеля, тем больше у него пропускная способность.

Коаксиальный кабель

Коаксиальный кабель (рис. 4.15) имеет отношение к таким стандартам сети, как «толстый» и «тонкий» Ethernet.

На рынке представлен достаточно широкий выбор коаксиального кабеля, однако для создания сетей используют только кабель разной толщины с волновым сопротивлением 50 Ом (телевизионный кабель имеет сопротивление 75 Ом).

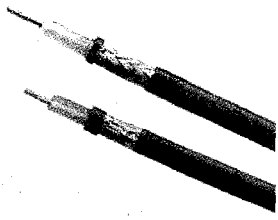


Рис. 4.15. Коаксиальный кабель

Как видно из рис. 4.15, строение коаксиального кабеля следующее:

- центральный провод (жила);
- диэлектрический изолятор центрального провода;
- металлическая оплетка — экран (как правило, медный);
- внешний изолятор.

Чаще всего при построении сети применяют коаксиальный кабель марки RJ-58, хотя есть и другие, например RJ-8, RJ-174, RJ-178, PK-50 и т. д.

Кабель на основе витой пары

Кабель на основе витой пары (рис. 4.16) популярнее коаксиального, поскольку предлагает более высокие скорости передачи данных и лучшую расширяемость сети.

Основу такого кабеля составляют пары проводников, которые не только скручены между собой, но и закручены вокруг остальных таких же пар.

Каждой паре соответствует своя цветовая гамма, например, первый из них — синий, другой — бело-синий. Кроме цветового отличия, каждая пара имеет свой номер и название.

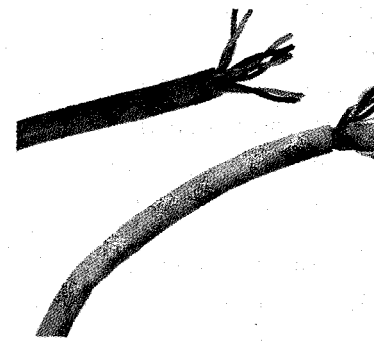


Рис. 4.16. Кабель на основе витой пары

При построении сети используют два типа кабеля — экранированный (Shielded Twisted-Pair, STP) и неэкранированный (Unshielded Twisted-Pair, UTP). Кроме того, кабели на основе витой пары делятся на шесть категорий, каждая из которых имеет определенные свойства. Чем выше категория, тем лучше характеристики кабеля. Например, для организации сети со скоростью передачи данных 100 Мбит/с используют кабель пятой категории.

Оптоволоконный кабель

Оптоволоконный кабель — кабель, строение которого коренным образом отличается от рассмотренных выше и любых других.

В качестве физической среды передачи данных по кабелю используют свет (фотоны), сформированный лазером. В этом заключается главное преимуще-

ство оптоволокна, поскольку полностью исключаются электрические наводки (помехи).

Таким образом, оптоволоконный кабель является самым защищенным, что очень важно для многих систем, например банков и государственных учреждений. Кроме того, учитывая низкое затухание сигнала, длина сегмента оптоволоконного кабеля значительно превосходит длину любого другого кабеля и может составлять более 100 км.

Однако достаточно высокая стоимость оборудования для формирования сигнала (света) и особенности прокладки (а именно обжим коннекторов) сдерживают широкое распространение этой технологии. Тем не менее там, где требуются скорость и защита, оптоволокно по праву заняло свое место.

Оптоволоконный кабель состоит из четырех частей: сердечника (сердечников), оболочки сердечника, прокладки и внешней оболочки (рис. 4.17). Главным является сердечник. Как правило, его изготавливают из кварца или специального полимера. Свет, проходя через сердечник, отражается от оболочки, что позволяет проводить кабель с изгибами любого угла.

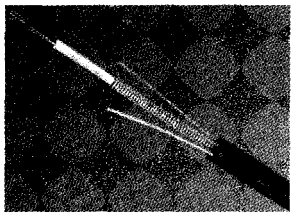


Рис. 4.17. Оптоволоконный кабель

Для механической защиты кабеля используют специальную прокладку, сделанную из пластика и кевралового волокна, придающего прочность. Дополнительную устойчивость к разрушениям обеспечивает тефлоновый слой.

Для прокладки сетей используют два вида оптоволокна — одномодовое и многомодовое, которые отличаются толщиной сердечника и оболочки. В зависимости от толщины варьируется количество сердечников. Соответственно одномодовый кабель содержит один сердечник большей толщины, а многомодовый — несколько более тонких.

Однако главное отличие этих двух типов кабелей заключается в пропускной возможности. Хотя многомодовый кабель при прокладке позволяет создавать участки с большими изгибами, его пропускная способность хуже, так как свет меньше отражается от оболочки сердечника. Кроме того, длина сегмента при этом значительно меньше (примерно в 50 раз).

Пропускная способность одномодового кабеля намного выше, он и значительно дороже многомодового.

4.10. Коннекторы, розетки, инструменты...

Одного кабеля для создания сети мало. Нужны еще различные мелочи — коннекторы, розетки, короба, панели и т. п. и, конечно, разнообразные инструменты для обрезки и обжима кабелей. Понятное дело, что в случае использования беспроводной сети без всего этого можно обойтись. Исключение составляют лишь комбинированные сети (например, беспроводная сеть с сегментами проводной).

Ниже рассмотрены практически все инструменты и материалы, необходимые для создания сетей на коаксиальном кабеле и на основе витой пары. Оптоволоконная сеть не рассматривается, поскольку она требует слишком дорогостоящего оборудования и ее создание лучше оставить профессионалам.

Все необходимое для сети на коаксиале

Коннектор BNC. Коннектор BNC (Bayonet Nut Connector) применяют при построении сети на основе коаксиального кабеля для обжима его концов, идущих к сетевой карте или порту любого сетевого оборудования, которое имеет соответствующий разъем (рис. 4.18).

Существует два типа коннекторов для обжима коаксиального кабеля. Наибольшее распространение получил коннектор, показанный рис. 4.18, для обжима которого используется специальный инструмент. Такой коннектор обеспечивает большую степень надежности, нежели другие, например использующие металлический колпачок, который накручивается на коннектор и прижимает его к кабелю.

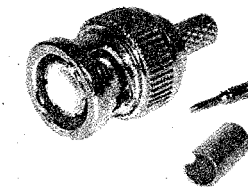


Рис. 4.18. Коннектор BNC и его составные части

Т-коннектор используют для соединения основной кабельной магистрали с сетевой картой компьютера или другого оборудования в сети, построенной на коаксиальном кабеле.

Внешне Т-коннектор (рис. 4.19) похож на обычный, но имеет отводы для вклинивания в центральную магистраль.

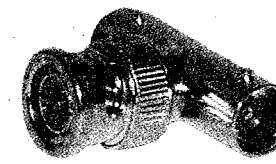


Рис. 4.19. Т-коннектор

Т-коннектор всегда используют в паре с коннектором (продлевает сегмент кабеля) или терминатором (закрывает сегмент) (рис. 4.20).

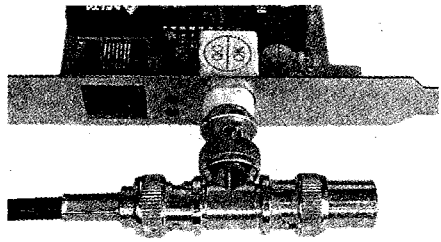


Рис. 4.20. Т-коннектор, присоединенный к сетевой карте

I-коннектор (рис. 4.21) служит соединителем сегментов кабеля без применения активного оборудования.

Данный коннектор применяют, когда нужно, например, дотянуть кабель до компьютера, но его длины не хватает.

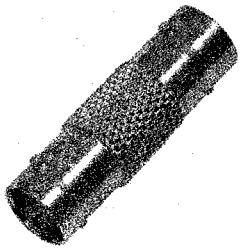


Рис. 4.21. I-коннектор

Терминатор (рис. 4.22) — устройство, которое устанавливают в конце сегмента с целью заглушить сигнал.

Если терминатор не установить, то сигнал, поступая в никуда, может привести не только к задержкам неопределенной длительности, но и к выходу сети из строя.

Рис. 4.22. Терминатор

Существуют разные **инструменты для обработки коаксиального кабеля**. При использовании коннекторов с накручивающимся колпачком достаточно иметь инструмент, показанный на рис. 4.23.

Для обжима BNC-коннекторов необходимо иметь инструмент, показанный на рис. 4.24. Он сочетает в себе функции обрезного инструмента, а также обеспечивает возможность обжима центрального сердечника и металлического обжимного кольца.

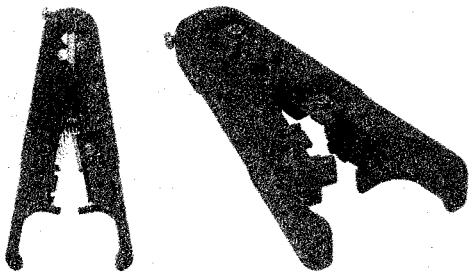


Рис. 4.23. Инструмент для обрезки кабеля и оголения его центрального проводника

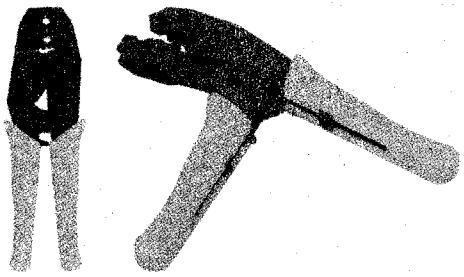


Рис. 4.24. Инструмент для обжима коннектора BNC

Все необходимое для сети на основе витой пары

Коннектор RJ-45 (рис. 4.25) используют для обжима кабеля, основанного на витой паре.

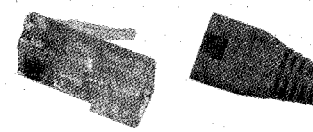


Рис. 4.25. Коннектор RJ-45 *(слева)* и защитный колпачок *(справа)*

Если в случае с коннектором BNC обжим кабеля можно произвести без инструмента, то с RJ-45 это невозможно. Чтобы хорошо обжать кабель с таким разъемом, требуется достаточно сильно сжать ручки инструмента, который оголит проводники кабеля и прижмет их к проводящим дорожкам на коннекторе. Вручную это сделать не получится.

Колпачок, надевающийся на коннектор, используется не только для скрытия лишней оголенности проводников, но и защищает их от пыли и различных атмосферных явлений.

Розетка RJ-45. Розетки являются такой же частью компьютерной сети, как бытовые электророзетки в электросети. Это некое связующее звено, служащее в качестве контактной площадки. Прокладка сети стоит достаточно дорого, поэтому она должна быть максимально защищена от повреждений. Чтобы исключить возможность порчи сегментов кабеля, их рекомендуется скрывать в специальные короба, окнами из которых и служат розетки (рис. 4.26).

ПРИМЕЧАНИЕ

При использовании коаксиального кабеля розетки не применяют.

Как и кабели, розетки делятся на категории, которые отличаются степенью защиты и другими требованиями к организации сети. На рис. 4.27 изображена розетка более низкой категории, чем розетка, показанная на рис. 4.26.

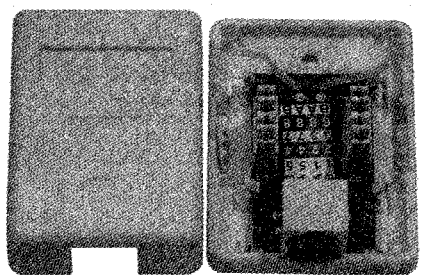


Рис. 4.26. Розетка

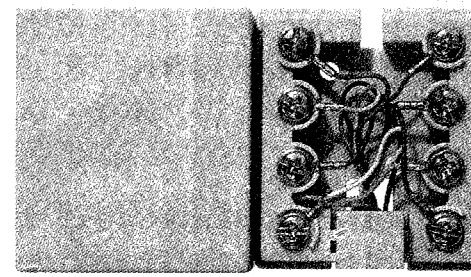


Рис. 4.27. Розетка одной из первых категорий

Одно из видимых различий между показанными розетками заключается в наличии специальных площадок для крепления проводников в первой (см. рис. 4.26), в то время как во второй (см. рис. 4.27) крепление производится с помощью обычных шурупов, что не гарантирует качества соединения.

Кросс-панель (рис. 4.28) используется в сети, построенной на кабеле, который основан на витой паре.

Кросс-панель служит в качестве связующего звена между кабельной системой и сетевым оборудованием.

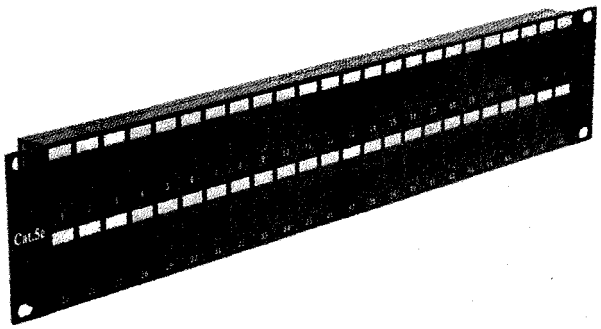


Рис. 4.28. Кросс-панель

На передней ее части находится определенное количество разъемов RJ-45, которые при необходимости соединяются с портами RJ-45 на сетевом оборудовании, например концентраторе или маршрутизаторе.

Все приходящие к соответствующим разъемам на передней панели проводники монтируются в задней части кросс-панели.

Патч-кордом (рис. 4.29) называют провод длиной до 5 м, который соединяет выход сетевой карты компьютера с разъемом на розетке. Как правило, он более мягкий, чем кабель, который идет от розетки к концентратору или другому сетевому оборудованию.

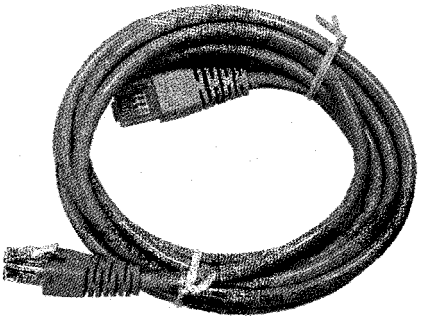


Рис. 4.29. Патч-корд

Такой кабель на обоих концах содержит коннекторы RJ-45, которые обжаты согласно принятым правилам в зависимости от выбранного стандарта и категории кабеля.

Кросс-кабель является «родным братом» патч-корда и отличается только меньшей длиной. Его применяют специально для подключения портов на концентраторе или другом сетевом оборудовании с разъемами на кросс-панели, которая физически связана с кабелем, ведущим к конкретному сетевому порту.

Инструменты для работы с витой парой. Для обжима кабеля на основе витой пары используют инструмент, подобный по принципу действия инструменту для обжима коаксиального кабеля. Данное приспособление позволяет обрезать кабель, снимать внешнюю оболочку и, конечно, обжимать коннектор, то есть втискивать жилы проводников в контакты разъема (рис. 4.30).

Часто этим инструментом можно обжимать разъемы для телефонной сети (RJ-11), более узкие и с меньшим количеством контактов.

При монтаже сетевых розеток используют специальный нож-вставку (рис. 4.31).

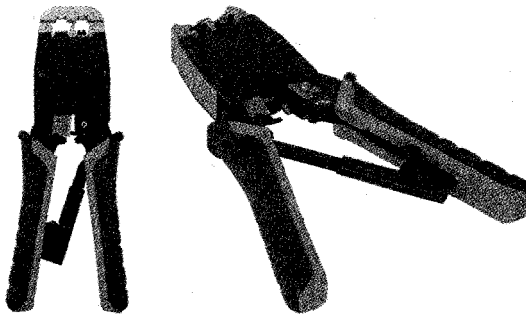


Рис. 4.30. Инструмент для обжима коннектора RJ-45

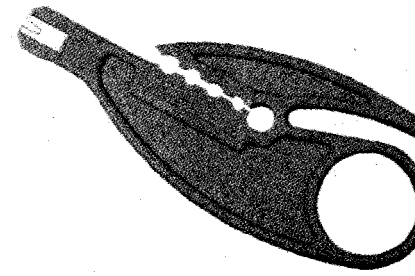


Рис. 4.31. Инструмент для зажима проводников в сетевой розетке

С помощью данного ножа можно вставлять проводники кабеля в контактные площадки сетевой розетки.

Глава 5

Стратегия выбора

- Критерии выбора класса сети
- Определение необходимого сетевого оборудования

Если вы планируете соединить два домашних компьютера, вам вполне хватит сети, построенной с применением коаксиального кабеля или кабеля на основе витой пары со скоростью передачи данных 10 Мбит/с, а в последнем случае и 100 Мбит/с. Стоимость такой сети состоит лишь из стоимости кабеля и коннекторов, поскольку сетевая карта обычно (для витой пары) уже установлена в компьютере.

Если же вы планируете соединить в сеть 40 компьютеров с выделенными серверами и сетевыми принтерами, естественно, вам придется использовать стандарт, скорости передачи которого будет достаточно для обеспечения потребностей пользователей.

5.1. Критерии выбора класса сети

Вы уже знаете, что существует два типа сетей — одноранговые и сети на основе выделенного сервера. Их аппаратная разница и возможности имеют большое значение и влияют на практическое использование (более подробные сведения смотрите в последующих главах книги). Поэтому при выборе класса сети необходимо учитывать следующие факторы.

Предназначение сети. Сеть может быть обычная (из нескольких компьютеров), домашняя и офисного или корпоративного назначения. Каждая из них несет свою функциональную нагрузку.

- Обычная сеть является разновидностью офисной и отличается только размерами и требованиями.
- Офисную или корпоративную сеть строят по строгим правилам, которые обеспечивают ей максимальную защищенность и функциональность.
- Домашняя сеть — особый тип, ориентированный на использование в квартирах, домах и районах (при ее построении применяют свои правила, что обуславливает ее уникальность и особенности).

Количество пользователей сети. Этот факт решающим образом влияет на выбор класса сети. Чем больше пользователей подключено, тем большим запасом производительности она должна обладать. Кроме того, от этого зависит количество проблем, которые будут возникать при работе сети, что рано или поздно приводит к решению выбрать администратора.

Масштабность сети. При построении сети используют определенные стандарты, диктующие правила ее использования (см. главу 11). Одним из них является максимальная протяженность сегмента сети. Естественно, что реальная оценка протяженности будущей сети повлияет на выбор класса.

Пропускная способность сети. Это величина, которую должна обеспечивать сеть при выполнении запросов пользователей. Другими словами — это скорость сети.

Предположим, в сети установлен сервер базы данных, в которой хранятся результаты деятельности крупного предприятия за несколько лет. Большое количество экономистов, бухгалтеров, менеджеров и других специалистов целый день работают с сервером, на котором находится эта база, «мучая» его своими запросами. Сервер, как ему и положено, добросовестно трудится, пересылая нужную информацию пользователям. Теперь представьте, что к этим работникам присоединились еще пять, которые осваивают известную «рабочую» программу — игру Quake. В результате количество сетевых запросов настолько возрастает, что сеть не успевает их все вместе обслуживать. Это приводит к возникновению задержек. Вот здесь и встает вопрос о пропускной способности: 10, 100 Мбит/с или более.

Финансовые затраты. Безусловно, та сумма, которую вы в состоянии потратить на организацию сети, также влияет на выбор ее класса. Если ограничений в капиталовложениях нет, то следует серьезно подумать об использовании такого стандарта, как 1000Base, который обеспечивает максимальную на сегодняшний день производительность и отличную расширяемость, чего с лихвой хватит на 5–10 лет.

Рассмотрим реальные примеры сетей и выбор соответствующего класса для их построения (табл. 5.1–5.5).

Таблица 5.1. Пример выбора класса сети (обычная сеть)

Предназначение сети	Сетевые компоненты	Количество компонентов
Обычная сеть	Рабочая станция	2–4
	Принтер	1

Как видно из данных табл. 5.1, сеть совсем небольшая. Для нее рекомендуется использовать топологию «общая шина» и стандарт 10Base-2 или 10Base-T. При этом вы не только сэкономите деньги, но и обеспечите достаточно приемлемую

скорость передачи данных — 10 Мбит/с. Также можно задуматься об использовании одного из беспроводных стандартов, поскольку в случае малого количества рабочих станций достигается теоретический предел производительности.

Таблица 5.2. Пример выбора класса сети (офисная сеть)

Предназначение сети	Сетевые компоненты	Количество компонентов
Офисная сеть	Рабочая станция	8–11
	Принтер	4
	Сетевой принтер	1
	Сервер базы данных	1

В табл. 5.2 приведен пример офисной сети, характерной для большинства малых и средних частных предприятий, занимающихся неопределенного рода бизнесом: от продажи книг до реализации продуктов питания.

В этом случае рекомендуется использовать топологию «общая шина» или «звезда». Второй вариант предпочтительней, так как предполагает дальнейшее развитие сети и переход с технологии 10 Мбит/с на 100 Мбит/с. Однако если возможно скорое развитие предприятия и переезд на новое место, лучшим выбором будет использование технологии «общая шина» с применением комбинированных сетевых адаптеров. Объясняется это достаточно просто — зачем вкладывать деньги в организацию сети со скоростью 100 Мбит/с в старом здании, если можно это сделать в новом — элементарная экономия денежных средств.

Таблица 5.3. Пример выбора класса сети (домашняя сеть)

Предназначение сети	Сетевые компоненты	Количество компонентов
Домашняя сеть	Рабочая станция	12–20
	Принтер	7
	Файл-сервер	1
	Общий доступ в Интернет	1

Данные табл. 5.3 — яркий пример средней домашней сети, которая имеет все шансы на дальнейшее развитие. В этом случае можно использовать любую топологию, однако лучше предпочесть топологию «звезда». В случае если нужно организовать связь между отдельно стоящими зданиями, можно использовать беспроводное оборудование или проложить оптоволокно, поскольку оно более устойчиво к воздействию атмосферных явлений.

Таблица 5.4. Пример выбора класса сети (малая корпоративная сеть)

Предназначение сети	Сетевые компоненты	Количество компонентов
Корпоративная сеть	Рабочая станция	25–50
	Принтер	15
	Сетевой принтер	2
	Файл-сервер	2
	Сервер базы данных	1
	Почтовый сервер	1
	Шлюз в Интернет	1

В табл. 5.4 описан начинающий представитель корпоративной сети со всеми вытекающими особенностями. Данный тип характеризуется постоянным развитием, что предъявляет свои требования к классу.

В этом случае рекомендуется использовать топологию «звезда» в паре со стандартом 100Base-TX. Хороший запас как по скорости, так и по расширяемости сети обеспечивает ее спокойное существование на протяжении нескольких лет.

Таблица 5.5. Пример выбора класса сети (крупная корпоративная сеть)

Предназначение сети	Сетевые компоненты	Количество компонентов
Корпоративная сеть	Рабочая станция	50–150
	Принтер	40
	Сетевой принтер	5
	Файл-сервер	2
	Сервер базы данных	3
	Принт-сервер	1
	Почтовый сервер	1
	Шлюз в Интернет	1

К серьезным сетям — серьезные требования! Такой девиз должен быть у системных администраторов подобных сетей.

Большое количество компьютерной техники и серверов обязательно приведет к повышению сетевого трафика, и, как следствие, возрастут требования к пропускной способности сети. В этом случае в качестве неплохой стартовой площадки может послужить топология «звезда» со стандартом 100Base-TX, однако следует задуматься о скором переходе на 1000Base.

Если компания создается с нуля, необходимо также задуматься об использовании оптоволокна, особенно если между филиалами налажен именно такой вид связи.

5.2. Определение необходимого сетевого оборудования

От того, является ли будущая сеть одноранговой или сетью с выделенным сервером, напрямую зависит количество оборудования, которое необходимо для ее создания. В частности, это касается использования выделенных серверов.

Здесь приведен обобщенный список для обоих типов сети.

- **Сетевая плата.** Количество сетевых плат зависит от числа компьютеров, которые подключены к сети (учитывают и клиентские машины, и серверы). Если к сети подключены сетевые принтеры без сетевых плат, этот факт также следует учесть. Кроме того, в компьютер могут устанавливаться и дополнительные сетевые платы, в зависимости от того, какие функции он выполняет (например, является интернет-шлюзом).
- **Концентратор (точка доступа), коммутатор.** Количество концентраторов зависит от используемой топологии сети. В сетях с топологиями «общая шина» или «кольцо» концентратор может служить только связующим звеном подсетей. Если сеть состоит всего из одного сегмента, концентратор не нужен вообще. Если используют топологию «звезда», то все зависит от количества подключаемых сетевых устройств и количества портов на концентраторе. Что касается использования коммутатора, то в последнее время он полностью вытеснил концентраторы. Поскольку выполняет гораздо больше функций и делает это более качественно за те же деньги.
- **Маршрутизатор.** Как правило, в «средней» по размерам сети используют один или два маршрутизатора. Если сеть насчитывает всего несколько компьютеров, использование маршрутизатора не обязательно. Это же относится и к коммутатору.
- **Мост.** Наличие моста определяется наличием разнородных сегментов сети. Если таковых нет, использовать мост бессмысленно.
- **Модем.** Количество модемов может быть разное. В сети могут использоваться как локальные, так и выделенные модемы.

- **Сервер.** Количество серверов зависит от потребностей сети. Если используется сеть на основе выделенного сервера, должен присутствовать хотя бы один сервер, содержащий учетные записи пользователей. Кроме этого, отдельно могут использоваться и другие серверы, например баз данных и файловый.
- **Расходные материалы.** Количество расходных материалов зависит от числа компьютеров, топологии и класса сети. При использовании топологии «общая шина» для подключения одного компьютера требуются два коннектора, один Т-коннектор и соответствующее количество кабеля. При использовании топологии «звезда» потребуются лишь два коннектора (плюс два защитных колпачка) и количество кабеля, необходимое для соединения компьютера с концентратором или другим компьютером (в случае соединения только двух машин). Сюда же можете добавить короба, скобы, дюбеля и т. д.

Часть 2

Проводная сеть

Глава 6

Топология и стандарты проводной сети

- Топология «общая шина»
- Топология «звезда»
- Топология «кольцо»
- Комбинированные топологии
- Стандарты проводной сети Ethernet
- Преимущества и недостатки проводной сети

Перед началом создания проводной (кабельной) сети следует выяснить, как и где будут располагаться подключаемые компьютеры. Также нужно определить места для необходимого сетевого оборудования и то, как будут проходить связывающие кабели. Это и есть топология сети.

От выбора топологии зависит очень многое, в частности необходимое сетевое оборудование, а также будущая судьба сети, то есть перспектива ее расширения.

Каждая из существующих технологий имеет свои правила, устанавливающие тип кабеля, который будет соединять компьютеры, максимальную длину сегмента[1], способ прокладки кабеля и т. д.

Сегодня существуют три различные топологии проводной сети — «общая шина», «звезда» и «кольцо». Часто можно встретить компьютерные сети, объединяющие в себе свойства всех топологий.

6.1. Топология «общая шина»

Такая сеть представляет собой набор компьютеров, подключенных вдоль одного кабеля (рис. 6.1). Сеть в данном случае строится на основе коаксиального кабеля.

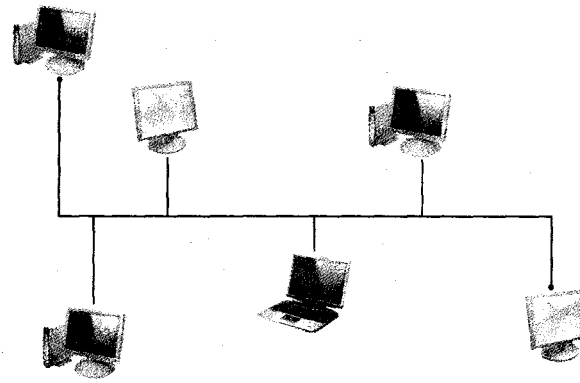


Рис. 6.1. Сеть, построенная по топологии «общая шина»

[1] Сегмент — максимальная длина кабеля между двумя соседними компьютерами или компьютером и сетевым устройством (концентратором, маршрутизатором, репитером и т. д.).

Данная топология была первой, которая активно использовалась и используется до сих пор. Для работы сети нужен всего один центральный кабель и отрезки, соединяющие с ним все компьютеры.

Особенность сети, построенной по топологии «общая шина», заключается в передаче сигнала сразу всем компьютерам. Чтобы определить, какой из них должен его принять, используется специальный MAC-адрес, который соответствует данному компьютеру, вернее, его сетевой карте. Адрес зашифровывается в каждый из сигналов, или пакетов, передаваемых по сети. Кроме того, информацию в каждый конкретный момент времени может передавать только одна машина. Это является слабым местом данной топологии, так как с возрастанием количества подключенных машин, которые хотят одновременно пересылать сообщения, скорость передачи заметно падает.

Что касается надежности сети, построенной по топологии «общая шина», то она работает, пока соблюдаются все правила ее построения и отсутствует разрыв кабеля. Как только появляется разрыв — вся сеть перестает работать, пока неисправность не устранят или пока на компьютер, предшествующий разрыву, не будет установлен терминатор. В этом случае удается спасти работоспособность хотя бы части сети.

Несмотря на недостатки, эта топология идеально подходит для создания сети из нескольких компьютеров, особенно если они находятся в одном помещении, а средств практически нет. С другой стороны, встретить сетевые карты или коннекторы для подобного рода сети становится все труднее, что в скором времени приведет к ее «уходу на пенсию».

6.2. Топология «звезда»

При этой топологии все компьютеры (каждый своим кабелем) подключаются к некоторому сетевому устройству, например концентратору. Подобное подключение напоминает звезду (рис. 6.2), этим и объясняется название. Подобная топология находит свое применение в сетях на основе витой пары.

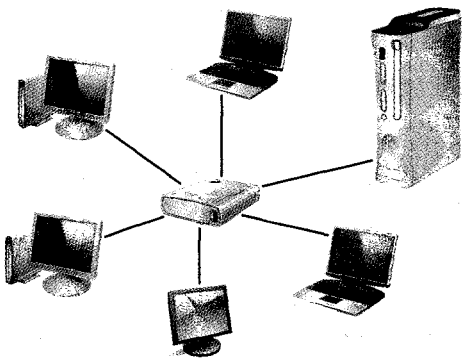


Рис. 6.2. Сеть, построенная по топологии «звезда»

Данный тип топологии — самый распространенный благодаря надежности и хорошей расширяемости сети.

Недостатком можно назвать только ее сравнительно высокую стоимость. Так, к каждому рабочему месту нужно подвести отдельный кабель. Кроме того, кабели подключают, например, к дорогостоящему многопортовому коммутатору.

С одной стороны, выход из строя коммутатора останавливает работу всей сети. С другой — поломка одного из компьютеров никак не влияет на работоспособность остальных участников сети.

Для расширения сети, построенной по топологии «звезда», достаточно подключить дополнительный концентратор, коммутатор или маршрутизатор (более дорогой вариант), обладающий необходимым количеством портов.

Сигнал, поступающий от передающего компьютера, идет на вход коммутатора, усиливается и передается сразу всем подключенным к нему машинам и остальным сетевым устройствам, поэтому не может потеряться по дороге.

6.3. Топология «кольцо»

Если кабель, к которому подключены компьютеры, замкнут, то такая топология называется «кольцо» (рис. 6.3).

При таком подключении каждый компьютер вынужден передавать возникший сигнал по кругу, предварительно его усиливая. Это выглядит следующим образом. Когда одной рабочей станции нужно передать данные для другой, она формирует специальный маркер, содержащий адрес передающего и принимающего компьютера, и непосредственно данные. После этого сформированный маркер передается в сеть. Попадая в кольцо, сигнал переходит от одного компьютера к другому, пока не найдет адресата. Если адрес в маркере совпадает с адресом компьютера, то получившая эти данные машина посылает уведомление о получении. Таким образом, каждый компьютер принимает полученный маркер, проверяет адрес, в случае несовпадения усиливает его и передает дальше по кольцу.

После того как данные достигают адресата, новый маркер поступает в кольцо и переходит к следующему компьютеру, которому нужно передать сообщение.

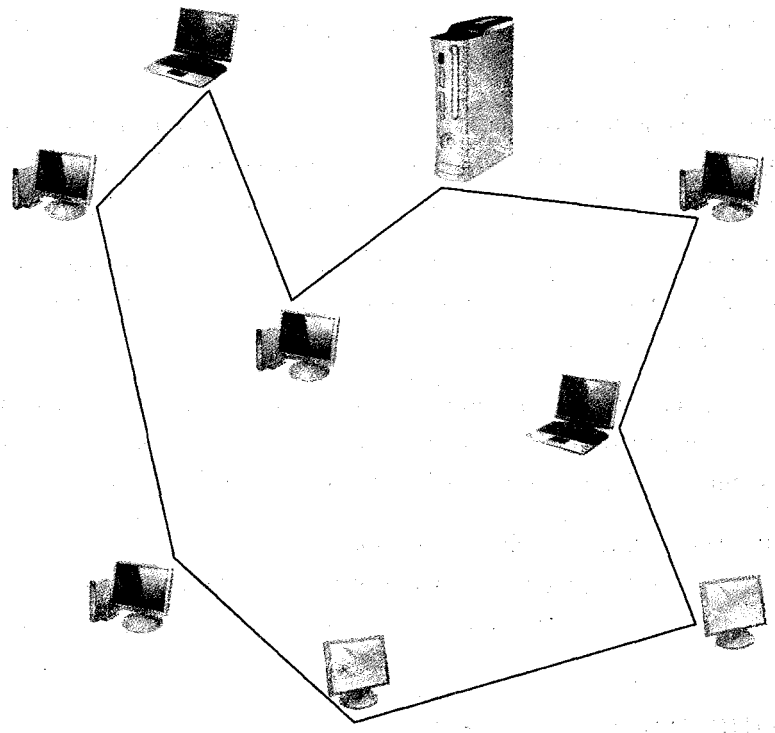


Рис. 6.3. Сеть, построенная по топологии «кольцо»

Данная топология встречается все реже, так как основной ее недостаток — ненадежность сети. Ведь стоит одному компьютеру выйти из строя, и сеть полностью перестает функционировать, поскольку появится разрыв.

6.4. Комбинированные топологии

Под комбинированной топологией подразумевается любой из вариантов, когда происходит пересечение (объединение) двух или более разных топологий.

Предположим, существуют две сети, построенные по разным топологиям и находящиеся в соседних зданиях или офисах. Когда необходимо соединить их в одну функциональную сеть, предстоит решить, следует ли приводить их к общему виду или оставить так, как есть. Чаще (особенно если хочется сэкономить средства) их просто соединяют, не изменяя топологии каждой. В этом случае получаются комбинированные топологии, например «звезда» и «общая шина» (рис. 6.4) или «звезда» и «кольцо».

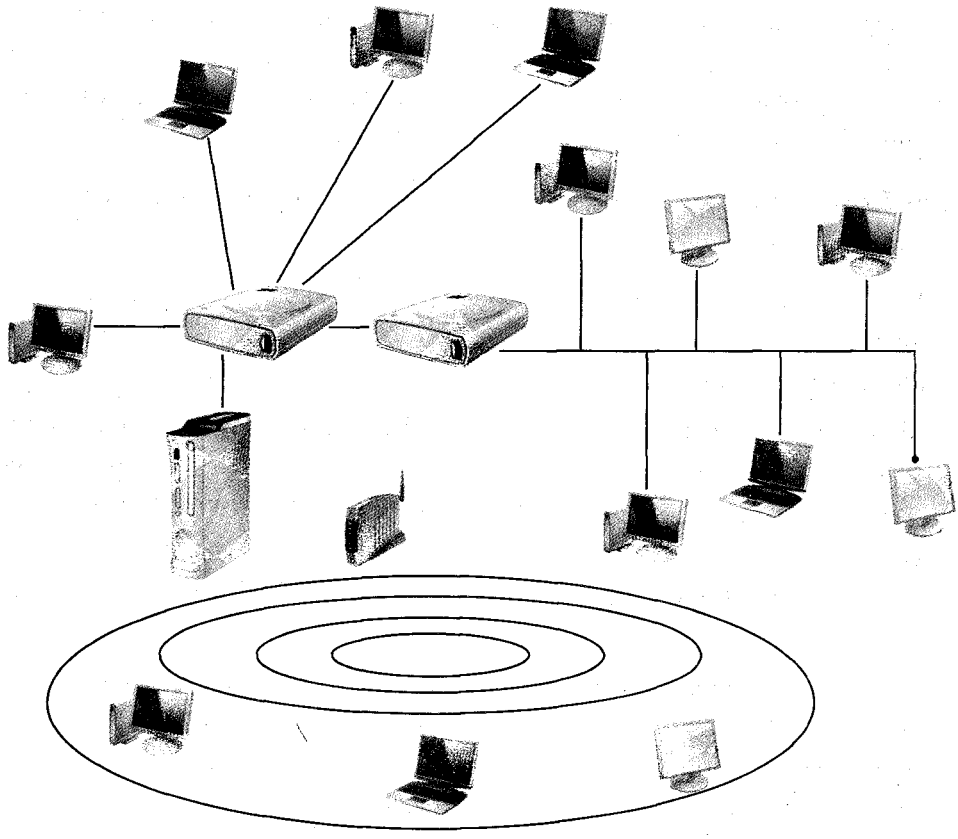


Рис. 6.4. Сеть, соединяющая в себе топологии «звезда» и «общая шина»

6.5. Стандарты проводной сети Ethernet

Одним из важнейших параметров сети, от которого непосредственно зависит ее производительность, является стандарт. За все время существования локальных сетей их накопилось достаточно много, поэтому вы сможете выбрать для себя подходящий.

Понятие стандарта

Что такое стандарт и зачем он нужен?

Представьте себе, из какого количества разнообразных компонентов состоит локальная сеть. Во-первых, компьютер и сетевая операционная система; во-вторых, сетевая карта; в-третьих, концентраторы, маршрутизаторы и т. п.;

в-четвертых, программное обеспечение, работающее с сетевой картой, и т. д. Требования ко всем этим компонентам разнообразны, кроме того, их выпускают разные производители, поэтому без согласованности трудно достичь приемлемого результата. Для этого и существует стандарт.

Разработкой стандартов занимаются крупные организации и комитеты, перечисленные ниже.

- Международная организация по стандартизации (International Organization for Standardization, IOS[1]) — учреждение, состоящее из ведущих организаций разных стран, которые занимаются разработками стандартов.
- Международный союз электросвязи (International Telecommunications Union, ITU) — постоянно действующая организация, выпустившая много разнообразных стандартов, в основном телекоммуникационных.
- Институт инженеров электротехники и радиоэлектроники (Institute of Electrical and Electronic Engineers, IEEE) — крупнейшая организация, которая занимается определением сетевых стандартов.
- Ассоциация производителей компьютеров и оргтехники (Computer and Business Equipment Manufacturers Association, CBEMA) — организация производителей аппаратного обеспечения США, которая занимается разработкой стандартов по обработке информации.
- Американский национальный институт стандартов (American National Standards Institute, ANSI) — организация, занимающаяся разработкой стандартов (начиная с сетевых и заканчивая стандартами языков программирования), в том числе и в составе ISO.

Ниже описаны некоторые сетевые стандарты, разработанные IEEE для проводных (кабельных) сетей.

Ethernet 10Base-2

Данная реализация сети относится к топологии «общая шина» и работает на скорости 10 Мбит/с. Для создания сети используется тонкий (0,25 см) коаксиальный кабель, поэтому часто можно услышать название «тонкая Ethernet» или «тонкий коаксиал».

---

[1] Часто используют другое название организации — International Standards Organization и, соответственно, название стандарта — ISO.

Сети, построенные в соответствии со стандартом Ethernet 10Base-2, характеризуются простотой и низкой стоимостью. Это позволяет использовать их в качестве стартовой площадки для домашней или офисной сети.

Коаксиальный кабель прокладывают по ходу расположения компьютеров. Чтобы заглушить конечный сигнал (избавиться от ухода его в никуда), применяют терминаторы, которые устанавливают на обоих концах центрального кабеля.

Для подключения кабеля к сетевой карте в него врезают Т-коннектор, который одним концом соединяется с BNC-коннектором на ее выходе, а два других служат для соединения центрального кабеля.

Максимальная длина одного сегмента кабеля не должна превышать 185 м[1]. Увеличить длину сегмента примерно до 925 м позволяют концентраторы (репитеры), усиливающие передаваемый сигнал. При этом существуют следующие ограничения:

- не более 5 сегментов;
- не более 4 репитеров между любыми двумя точками;
- не более 3 используемых сегментов.

Среди пользователей это правило получило название «5–4–3». Кроме того, нельзя забывать следующие ограничения:

- не более 30 сетевых подключений на сегменте без репитера;
- не менее 50 см между двумя сетевыми точками.

Также учтите, что чем больше будет подключено сетевых устройств, тем медленнее будет работать сеть.

В табл. 6.1 рассмотрены основные достоинства и недостатки Ethernet 10Base-2.

Таблица 6.1. Преимущества и недостатки Ethernet 10Base-2

Преимущества	Недостатки
Дешевая в построении сеть	Ограничения в длине сегмента, количестве компьютеров и активного оборудования

[1] На практике при использовании качественных сетевых карт длина сегмента может достигать 220–300 м.

Преимущества	Недостатки
Хорошо подходит для организации сети с небольшим количеством компьютеров	При образовании колец из кабеля возникают наводки и помехи сигнала
Легкая расширяемость сети	В случае повреждения центрального кабеля перестает функционировать вся сеть
	Снижение скорости передачи данных при большом количестве компьютеров
	Максимальная теоретическая скорость передачи составляет всего 10 Мбит/с

Ethernet 10Base-5

Данная реализация сети относится к топологии «общая шина» и работает на скорости 10 Мбит/с. Для создания сети используют толстый (0,5 см) коаксиальный кабель, поэтому этот стандарт иногда называют «толстый Ethernet» или «толстый коаксиал».

Как и в случае с Ethernet 10Base-2, данный стандарт является достаточно дешевой альтернативой хорошей сети. Его основные преимущества перед Ethernet 10Base-2 — увеличенная длина сегмента, большее количество рабочих станций, а также большая устойчивость к помехам. Общая протяженность сети может составлять 2,5 км при условии использования пяти репитеров.

Основные ограничения:

- не более 5 сегментов;
- не более 4 репитеров между любыми двумя точками;
- не более 3 используемых сегментов;
- не более 100 сетевых подключений на сегменте без репитера;
- не менее 2,5 м между двумя сетевыми точками.

Для того чтобы компьютер можно было подключить к сети, необходимо, кроме сетевой карты, иметь еще и специальное устройство, называемое трансивером. Его подключают непосредственно к сетевой карте, которая должна обладать разъемом AUI. При этом длина кабеля между ресивером и сетевой картой может достигать 50 м, что облегчает возможную перестановку компьютера в другое место.

В табл. 6.2 рассмотрены основные достоинства и недостатки Ethernet 10Base-5.

Таблица 6.2. Преимущества и недостатки Ethernet 10Base-5

Преимущества	Недостатки
Устойчивый к помехам сигнал	Дорогая в построении
Легкая расширяемость сети	В случае повреждения центрального кабеля перестает функционировать вся сеть
Большая длина сегмента	Снижение скорости передачи данных при большом количестве компьютеров
	Максимальная теоретическая скорость передачи составляет всего 10 Мбит/с
	Необходимо дополнительное устройство — трансивер

Ethernet 10Base-T

Ethernet 10Base-T относится к топологии «звезда» и работает на скорости 10 Мбит/с. Для создания сети используют неэкранированную телефонную витую пару.

Имея преимущество сети топологии «звезда», данный тип все же встречается редко из-за использования телефонного кабеля, чувствительного к наводкам.

Максимальная длина сегмента сети, которая построена на стандарте Ethernet 10Base-T, — 100 м (сказывается отсутствие экрана провода), хотя, как и в случае с Ethernet 10Base-2, существуют репитеры, удлиняющие сегменты.

В отличие от сетей стандарта Ethernet 10Base-2, сети Ethernet 10Base-T имеют меньшую устойчивость к помехам, зато они более гибкие и позволяют легче локализовать неисправность.

В табл. 6.3 приведены основные достоинства и недостатки Ethernet 10Base-T.

Таблица 6.3. Преимущества и недостатки Ethernet 10Base-T

Преимущества	Недостатки
Дешевая в построении сеть	Ограничения в длине сегмента
Хорошо подходит для организации сети из любого количества компьютеров	Выход из строя центрального концентратора приводит к сбою всей сети
Легкая расширяемость сети	
Достаточная защищенность	
Простая локализация неисправности	
В случае повреждения центрального кабеля выходит из строя только один сегмент сети	

Ethernet 10Base-F

Ethernet 10Base-F относится к топологии «звезда» и работает на скорости 10 Мбит/с. Для создания сети используют волоконно-оптический кабель, данные по которому передаются на частоте 500–800 МГц.

Поскольку для монтажа используют оптоволокно, такая сеть обладает максимальной защищенностью от электрических и электромагнитных наводок. Это гарантирует хороший сигнал на всей протяженности сегмента. Кроме того, длина сегмента в данном случае намного больше, чем у рассмотренных выше вариантов — до 2 км.

Сеть с применением этого стандарта достаточно часто используется для соединения между собой отдельно стоящих зданий.

В табл. 6.4 рассмотрены основные достоинства и недостатки Ethernet 10Base-F.

Таблица 6.4. Преимущества и недостатки Ethernet 10Base-F

Преимущества	Недостатки
Количество компьютеров не ограничено	Дорогая в построении сеть
Легкая расширяемость сети	
Максимальная защищенность	
Простая локализация неисправности	
В случае повреждения центрального кабеля выходит из строя только один сегмент сети	

Fast Ethernet 100Base-TX

Сеть стандарта Fast Ethernet 100Base-TX — «старший брат» сети, использующей стандарт Ethernet 10Base-T. Данный стандарт также подразумевает использование топологии «звезда».

Основное его отличие от своего «собрата» — скорость передачи данных. Здесь она составляет 100 Мбит/с, что в 10 раз больше, чем у стандарта Ethernet 10Base-T.

Аналогично Ethernet 10Base-T сеть стандарта Fast Ethernet 100Base-TX строится на основе кабеля «витая пара», однако с использованием отдельных пар проводов для передачи и приема данных. При этом применяют как неэкранированные, так и экранированные провода, на которые накладывается ограничение — они должны быть скручены по всей длине, кроме концов (1–1,5 см), к которым присоединяют коннекторы.

Как и в Ethernet 10Base-T, длина сегмента не должна превышать 100 м.

В табл. 6.5 представлены основные достоинства и недостатки Fast Ethernet 100Base-TX.

Таблица 6.5. Преимущества и недостатки Fast Ethernet 100Base-TX

Преимущества	Недостатки
Повышенная скорость передачи данных (100 Мбит/с)	Ограничения в длине сегмента (до 100 м)
Достаточно дешевая в построении сеть	Ограничения в количестве компьютеров (до 1024)
Хорошо подходит для организации сети из любого количества компьютеров	Выход из строя центрального концентратора приводит к выходу из строя всей сети
Легкая расширяемость сети	
Достаточная защищенность	
Легкая локализация неисправности	
В случае повреждения центрального кабеля выходит из строя только один сегмент сети	

Fast Ethernet 100Base-FX

Fast Ethernet 100Base-FX — еще один стандарт, позволяющий строить сети с использованием дорогого, но сверхзащищенного оптоволоконного материала, причем в данном случае используют два кабеля.

Основное преимущество оптоволоконных сетей — длина сегмента, которая в зависимости от режима передачи данных и оптоволоконного разъема составляет от 412 м (полудуплексный режим) до 2 км (дуплексный режим). Кроме увеличенной до 100 Мбит/с скорости передачи данных, все остальные характеристики остались без существенных изменений. Максимальное количество подключаемых рабочих станций — 1024.

Gigabit Ethernet

Существует несколько стандартов, которые входят в состав Gigabit Ethernet. В частности, стандарт 1000Base-T подразумевает использование кабеля, на основе витой пары 5-й категории. При этом используются все четыре пары проводников. Максимальная длина сегмента составляет 100 м.

Существуют также стандарты, например 1000Base-LX, которые в качестве кабельной системы используют оптоволокно. В этом случае максимальная длина

сегмента может составлять 5 км[1] для одномодового кабеля и 550 м для многомодового.

10 Gigabit Ethernet

На сегодняшний день стандарты 10 Gigabit Ethernet (10GBase-X, 10GBase-R и 10GBase-W) являются самыми перспективными и позволяют построить наиболее производительную сеть. Для этих целей используется оптоволоконный кабель. Максимальная длина сегмента может составлять 40 км. Чтобы достичь таких результатов, используется высокая частота передачи сигнала и длина волны лазера.

Token Ring

Token Ring относится к топологии «кольцо» и работает на максимальной скорости 16 Мбит/с. Его разработали специалисты компании IBM в 1970-х годах. Для создания сети используют экранированный или неэкранированный кабель на основе витой пары.

При работе сеть использует маркер — поток данных, управление которым осуществляет любой компьютер, передающий информацию. Если маркер «захвачен» каким-либо компьютером, то все остальные ждут, пока он освободится.

Таким образом, получив управление над маркером, компьютер передает часть данных (кадр) по кольцу, предварительно вставив в него адрес компьютера-получателя. Когда сообщение доходит до адресата, он принимает их, делает об этом пометку и пересылает далее по кольцу[2]. Приняв свои же данные, но уже с пометкой о приеме, компьютер-отправитель продолжает передачу или возвращает маркер в сеть для дальнейшего использования другой машиной.

В отличие от обычного «кольца», сеть Token Ring использует в своей работе концентратор. Это позволяет исключать варианты, когда из-за одного компьютера перестает работать вся сеть. В данном случае, обнаружив неисправный компьютер (неисправную сетевую карту), маркер просто проходит дальше,

---

[1] Общая длина сети может достигать 70 км, что зависит от используемого активного сетевого оборудования.

[2] Движение данных по кольцу происходит только в одном направлении.

чем обеспечивается большая отказоустойчивость системы. Однако остается главный недостаток — разрыв центрального кабеля приводит к выходу из строя всей сети.

Данный стандарт имеет довольно скромные показатели. Чтобы обеспечить работу сети на максимальной скорости, в зависимости от типа используемого кабеля длина сегмента не должна превышать 60–100 м. При длине сегмента 150–300 м достигается скорость не более 4 Мбит/с.

Как и в других стандартах, разрешается использование репитеров, что позволяет удлинить максимальный сегмент до 350–700 м.

Максимальное количество пользователей — 72 (в случае применения кабеля более высокой категории — до 260).

6.6. Преимущества и недостатки проводной сети

Рассмотрев достаточно много сетевых стандартов, которые находят свое применение в случае использования той или иной сетевой топологии, можно составить список основных преимуществ и недостатков проводной сети. Данная информация вам обязательно пригодится и позволит сравнить проводной и беспроводной варианты, что, в свою очередь, окончательно поможет вам определиться с выбором типа будущей сети.

Итак, начнем. Преимуществ у проводной сети достаточно много.

- Высокая производительность. Как вы уже знаете, существуют стандарты, которые позволяют передавать данные в сети со скоростью более 100 Мбит/с. Как показывает практика, этой скорости вполне хватает для комфортной работы достаточно большой сети с несколькими серверами. Кроме того, в любой момент можно перейти и на более быстрый стандарт, просто поменяв имеющееся оборудование на более скоростное.
- Практически неограниченная расширяемость сети. Запаса по количеству подключаемого оборудования хватает для сети любого объема.
- Возможность обслуживания сегментов сети с разными топологиями. Этот факт очень важен, поскольку позволяет соединить воедино сети с разными топологиями. Для этого вам всего-навсего потребуется иметь соответствующий мост или маршрутизатор. При этом можно организовывать виртуальные сети с четко ограниченными наборами прав доступа и т. п.

- Широкие возможности настройки сетевого окружения (DNS, DHCP, шлюзы, домены, рабочие группы и т. д.).
- Защищенность сети. Проводная сеть является достаточно защищенной средой, поскольку для того, чтобы к ней подключиться, злоумышленнику придется либо получить доступ к концентратору, либо каким-то образом произвести врезку в существующую сетевую магистраль или кабель.
- Несложная локализация неисправности (в случае использования топологии «звезда»).
- Возможность выбора среди стандартов сети оптимального показателя «качество/цена».
- Возможность высокоскоростного доступа в Интернет.

Из недостатков можно отметить следующие.

- При большом количестве компьютеров дорогая в создании. Особенно этот факт заметен, если приходится прокладывать сеть по всем правилам. В этом случае вам необходимо подключать новый компьютер, используя для этого достаточной длины кабель, который зачастую необходимо прокладывать в коробах с возможными переходами между этажами. В случае невозможности подключения к существующей системе приходится покупать дополнительное активное оборудование.
- Сложность добавления нового рабочего места в случае использования топологии «звезда».
- Необходимо знание основ прокладки кабеля и обжима коннекторов.
- Требуется четкая организация рабочих мест.
- Очень плохая мобильность сетевых устройств.
- В случае создания домашней сети требуется разрешение на проводку кабельной системы.

Глава 7

Сеть на основе коаксиального кабеля

- Правила прокладки кабеля
- Подготовка кабеля
- Монтаж разъемов BNC
- Установка Т-коннекторов и заглушек

Одними из первых были сети, построенные на основе коаксиального кабеля. Для их создания используется специальный кабель (тонкий или толстый), имеющий волновое сопротивление 50 Ом, диаметр которого влияет на основные технические характеристики сети.

При построении сети на основе коаксиального кабеля используют топологию «общая шина» — все компьютеры подключаются к общей магистрали с помощью Т-коннекторов.

Если проводить аналогию с сетью, в основе которой лежит витая пара, то Т-коннектор играет ту же роль, что и сетевая розетка. К ним присоединяют отрезки кабеля, соединяющие сетевые карты компьютеров с главным сетевым кабелем. Каждый такой кабель обжат с двух сторон специальным коннектором.

Сети на основе коаксиального кабеля с каждым годом встречаются все реже, ведь их пропускная способность составляет всего 10 Мбит/с (на практике этот показатель сильно зависит от количества подсоединенных компьютеров), а поднять производительность невозможно. Однако если вы хотите создать сеть, затратив минимум усилий и финансов, и не предъявляете высоких требований к ее производительности, то коаксиальный кабель подойдет как нельзя лучше. Кроме того, этот способ идеален, если нужно соединить всего несколько компьютеров в пределах одной-двух комнат.

ПРИМЕЧАНИЕ

Из видеоуроков «Урок 7.1. Обжим коаксиального кабеля» и «Урок 7.2. Подключение коаксиального кабеля к компьютеру», которые находятся на компакт-диске, прилагаемом к книге, вы узнаете, как происходит подготовка кабеля и обжим коннекторов, а также как подключить готовый кабель к компьютеру.

7.1. Правила прокладки кабеля

Вспомним об основных ограничениях сети, построенной с применением коаксиального кабеля (стандарт Ethernet 10Base-2):

- длина сегмента не должна превышать 185 м;
- не более 5 сегментов;
- не более 4 репитеров между любыми двумя точками;
- не более 3 используемых сегментов;

- не более 30 сетевых подключений на сегменте без репитера;
- не менее 50 см между двумя сетевыми точками.

Проектировать сеть нужно исходя из этих ограничений.

При прокладке кабеля, как и в любом другом деле, придерживайтесь определенных правил, что предотвратит сбои в работе вашей сети.

1. Обдуманно выбирайте место прокладки кабеля. Не забывайте, что главным элементом рассматриваемого типа сети является ее носитель — сам кабель. Если произойдет обрыв центрального кабеля, то вся сеть перестанет функционировать, поэтому он должен быть проложен в местах, гарантирующих максимальную защиту кабеля.
2. Не допускайте натяжения кабеля. Сеть не является цельной структурой, а представляет собой цепь соединенных сегментов, поэтому любое натяжение может негативно сказаться на одном из образованных контактов. Наиболее критичными участками являются места соединения кабеля с коннекторами.

ВНИМАНИЕ

Нарушение целостности контактов или обрыв кабеля приводит к нестабильной работе сети или ее полному выходу из строя.

3. Избегайте создания лишних петель кабеля, каждая из них не только уменьшает полезную длину сегмента, но и создает электромагнитные наводки, особенно если лишний кабель хаотично организован или сложен петлями.
4. Чтобы избавиться от нежелательной петли, обрежьте кабель и соедините его с помощью I-коннектора (барел-коннектора) или T-коннектора. Однако не следует слишком увлекаться таким методом — чем реже встречаются места соединения, тем меньше потеря сигнала на всем сегменте сети и надежнее ее работа.
5. Следите за изгибами кабеля. Если нужно придать изгиб, например, необходимо обогнуть стену и прибить кабель с помощью скобок к плинтусу, то старайтесь делать его не менее 50 мм[1]. Если не придерживаться этого правила, то в месте перегиба может лопнуть внешняя оболочка и повредиться мед-

[1] Минимальный изгиб равен 10 радиусам кабеля, то есть для кабеля радиусом 5 мм минимальный изгиб — 50 мм.

ная изоляция (экран). Это не приведет к сбою в работе сети сразу, однако со временем агрессивная внешняя среда сделает свое черное дело.

6. Старайтесь избегать прокладки возле проводов электропитания и электрощитов, ведь они являются мощнейшим источником электрических наводок, которые создают помехи для нормального прохождения сигнала по любому кабелю, в том числе и по коаксиальному. По этой причине если на пути следования встречается протяженный участок электролинии, то лучше обойти его, проложив кабель по специальным пластмассовым коробам, например по верху стены. Этим вы, конечно, увеличите общую протяженность кабельной магистрали, зато избавитесь от электрических наводок, которые постоянно создают проблемы.
7. Избегайте прокладки кабеля возле отопительных конструкций. Аналогично электропроводке, нагрев кабеля также вносит изменения в среду передачи данных. Изменение сопротивления центрального проводника коаксиального кабеля может привести к нестабильной работе сети. Поэтому старайтесь не прокладывать кабель вдоль батареи центрального (или другого) отопления. Для этого можете воспользоваться теми же коробами: даже если провести кабель возле батареи, но прикрыть его коробом, то он будет менее подвержен нагреву.
8. Используйте специальные пластиковые короба и трубы. Данное правило особенно актуально, если кабель нужно проложить под землей или на открытом воздухе.

   Как известно, в земле вещества разлагаются. Хотя скорость разложения кабеля небольшая, в определенных условиях (постоянная влажность земли, ее минеральный и химический состав и т. д.) она может увеличиться многократно.

   Аналогичным образом негативно влияет внешняя окружающая среда, когда кабель проводят на открытом воздухе. Постоянная смена погоды, дождь и солнце, налипание снега и мороз уменьшают срок службы кабеля и, как следствие, всей сети. Как уже было сказано выше, чтобы уменьшить влияние вредных факторов, используют специальные пластиковые короба или трубы.
9. Используйте обжимные коннекторы, что сделает сеть более устойчивой к обрывам, а значит, более долговечной.

Соблюдая эти простые правила, можно начинать проектирование сети и подготовку необходимых компонентов: отрезков кабеля, коннекторов для их обжима, Т-коннекторов для соединения частей кабеля и терминаторов, которые отражают сигнал.

7.2. Подготовка кабеля

Для прокладывания сети используют коаксиальный кабель с волновым сопротивлением 50 Ом. Внешне он неотличим от обычного телевизионного, но ни в коем случае не путайте их. Телевизионный кабель имеет волновое сопротивление 75 Ом, и при его использовании сеть функционировать не будет.

Как вы уже знаете, для прокладки сети с топологией «общая шина» применяют коаксиальный кабель двух видов: толстый (диаметром 2,5–4 мм) и тонкий (диаметром 4–6 мм). Однако самое большое отличие в использовании того или другого кабеля заключается в максимальной длине сегмента. При использовании толстого кабеля она может даже превышать допустимые 185 м[1], в то время как тонкий коаксиальный кабель этого преимущества не имеет.

Выбрав нужный тип кабеля, необходимо его подготовить. Предварительно попробуйте спроектировать будущую сеть на бумаге: нарисуйте план квартиры (офиса, дома), определите места, где будет прокладываться основной кабель, обозначьте расположение компьютеров и репитеров и т. д.

Создавая будущий эскиз сети, не забывайте о правилах прокладки кабеля (см. выше). Несоблюдение элементарных норм может привести к постоянным сбоям в работе. Поэтому обязательно еще раз сверьтесь с правилами и внесите нужные изменения в планировку сети.

Для прокладки кабеля могут использоваться специальные пластиковые короба, которые обеспечивают ему дополнительную защиту. Такой короб состоит из двух частей — основы и крышки. Основу короба крепят с помощью дюбелей и болтов в выбранном месте его прокладки, а крышка закрывает основу, когда кабель уже находится внутри.

Если использование коробов не входит в ваши планы, обязательно воспользуйтесь специальными скобами, с помощью которых кабель крепится к стене или плинтусу. При выборе скоб будьте внимательны, поскольку их неподходящий диаметр не только усложнит прокладку кабеля, но и не обеспечит нужной степени прижима его к поверхности.

---

[1] Иногда длина максимального сегмента составляет 300–400 м. Немаловажную роль в этом также играет класс сетевого адаптера — таких показателей достигают при использовании адаптеров известных производителей, например 3COM.

После этого можно приступать к работе.

Вспомним принцип построения сети на основе коаксиального кабеля.

- Центральная магистраль кабеля с обоих концов «глушится» специальными коннекторами — терминаторами, внутри которых установлен обычный резистор с сопротивлением 50 Ом. Делается это для блокирования дальнейшего распространения сигнала. Один из коннекторов обязательно должен заземляться, для чего используют специальную цепочку, закрепленную на нем.

ПРИМЕЧАНИЕ

Многие игнорируют вопрос заземления. Если вы не хотите периодически производить замену вышедших из строя сетевых адаптеров, не следует обходить эту проблему стороной. Кроме того, сеть постоянно будут терзать «разнообразные» сбои. В конце концов, все равно придется использовать заземление.

- Для подключения компьютера в центральную магистраль врезают Т-коннектор, имеющий отвод для подключения к сетевой карте компьютера. Т-коннектор — одноблочная структура, поэтому для его врезки в центральную магистраль концы кабеля должны быть снабжены коннекторами, которые устанавливаются с каждой стороны Т-коннектора.
- Если центральная магистраль была разрезана (перебита) случайно, то для восстановления сегмента можно использовать I-коннектор (барел-коннектор) или Т-коннектор.

Как видите, все очень просто. Осталось только осуществить задуманное. Главная задача заключается в подготовке отрезков кабеля нужной длины.

СОВЕТ

Готовя отрезки кабеля, увеличивайте их длину на 10–20 %. Как правило, лишние сантиметры уходят на более удобную прокладку и обжим коннекторов.

Отмерив отрезок кабеля нужной длины, отрежьте его. Для этого воспользуйтесь резцами инструмента для обжима коннекторов (см. рис. 4.23) или обычными ножницами.

Если для прокладывания кабеля вы используете пластиковые короба, нужно их подготовить. Выбрав место, где будет проходить кабель, закрепите основу короба. Далее аккуратно уложите в нее кабель и закройте крышкой. Как правило,

в коробе остается достаточно места для укладки и других кабелей, например телефонного.

На краях короба у вас должны остаться концы кабеля достаточной длины для создания петли нужного размера, которая должна свободно доставать выход на сетевой карте компьютера.

Далее обрежьте концы кабеля. Старайтесь делать разрез ровным — это избавит вас от повторного обрезания кабеля.

С помощью специального инструмента для снятия изоляции (рис. 7.1) снимите примерно 20 мм внешней оболочки (вместе с 20 мм снимается примерно 8–10 мм внутренней оболочки вместе с окружающим ее медный экраном).

Рис. 7.1. Снимаем изолирующую оболочку

Для этого откройте инструмент (нажав на среднюю часть, вы поднимете верхнюю, освобождая отверстие, в которое нужно вставить кабель) и вставьте в него конец кабеля. Делайте это с таким расчетом, чтобы с правой стороны инструмента торчал кусочек длиной 2–4 мм. После этого сделайте два-три поворота вокруг оси кабеля.

ПРИМЕЧАНИЕ

Количество оборотов подбирают экспериментальным путем с таким расчетом, чтобы при обрезе внешней оболочки не повреждался медный экран внутренней.

Затем, потянув нож вправо, снимите обрезанную часть внешней оболочки.

Обрезать оболочку можно и с помощью ножа, однако делайте это осторожно и старайтесь не повредить при этом жилы экрана.

Дальнейшая подготовка кабеля зависит от типа используемых для обжима коннекторов.

7.3. Монтаж разъемов BNC

После подготовки кабеля можно переходить к обжиму BNC-коннекторов.

Различают три вида BNC-коннекторов, каждый из которых имеет свои преимущества и недостатки.

- **Обжимные коннекторы** наиболее распространены среди создателей сетей. Основные их преимущества — обеспечение надежного контакта и легкость обжима. Недостаток — одноразовость: в случае обрыва провода требуется новый коннектор, поскольку использование старого невозможно в силу полученных при обжиме деформаций. Для обжима такого типа коннекторов используют специальный обжимной инструмент. При некоторой сноровке можно применять и обычные плоскогубцы.
- **Накручивающиеся коннекторы** обеспечивают простоту монтажа, для которого не нужны дополнительные инструменты. Однако они очень чувствительны к натяжению кабеля, из-за чего происходит нарушение контакта.
- **Коннекторы под пайку** — когда-то часто используемый тип коннекторов, сегодня встречается редко. Основная причина — сложность монтажа, требующего наличия паяльника и умения с ним работать. Нарушение контакта в случае плохой припайки проводников приводит к постоянным сбоям сети и к трудностям локализации места разрыва.

На подготовленный кабель наденьте металлическую трубочку (она в дальнейшем послужит для окончательного обжима корпуса коннектора). В накручивающемся коннекторе она является частью корпуса и содержит внутреннюю резьбу. Аналогичным образом наденьте трубочку на кабель с таким расчетом, чтобы в дальнейшем ее можно было накрутить на него в сторону коннектора.

На кончик внутреннего проводника наденьте латунный сердечник коннектора (рис. 7.2). Обязательно проследите, чтобы он покрывал весь оголенный проводник вплоть до пластикового диэлектрика. Если этого не сделать, то в процессе вставки в коннектор непокрытый сердечником участок проводника может согнуться или, еще хуже, сломаться. Если участок оголенного проводника слишком длинный, то отрежьте лишнее, воспользовавшись резцами инструмента или ножницами.

Теперь нужно обжать латунный сердечник (рис. 7.3). Для этого воспользуйтесь соответствующим углублением

Рис. 7.2. Надеваем на подготовленный кабель металлическую трубочку и латунный сердечник

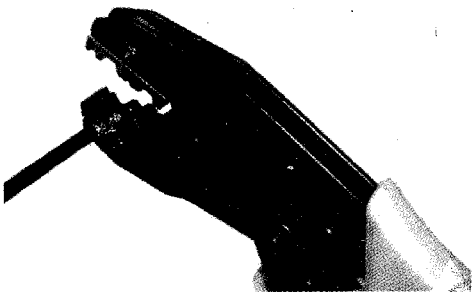


Рис. 7.3. Обжимаем латунный сердечник

в обжимном инструменте. Углубление такого размера всего одно, поэтому ошибиться сложно. Еще раз проверив, надет ли сердечник на проводник до конца, аккуратно установите его в найденное углубление и сильно сожмите ручки инструмента.

ПРИМЕЧАНИЕ

В коннекторе под пайку на данном этапе нужно припаять проводник к сердечнику. Для этого, после того как конец проводника покажется из сердечника, покройте его канифолью. Далее приложите жало паяльника к соединению и прогрейте его без припоя. В результате нагрева обе составляющие припаяются друг к другу минимумом припоя, который всегда находится на жале паяльника.

Аккуратно расплетите медный экран. Затем наденьте корпус коннектора до упора, стараясь при этом не нажимать очень сильно. Проследите, чтобы латунный сердечник, вставленный в корпус, торчал из него почти на всю длину, иначе он не сможет плотно войти в разъем на сетевой карте. После этого распределите равномерно медный экран по всей поверхности торца корпуса разъема. Затем аккуратно наденьте металлическую трубочку до упора на торец корпуса таким образом, чтобы она прикрыла медный экран (рис. 7.4).

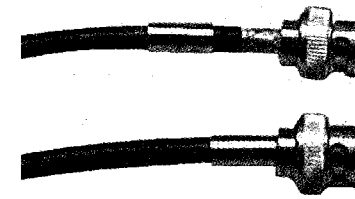


Рис. 7.4. Надеваем металлическую трубочку

ПРИМЕЧАНИЕ

При использовании накручивающегося коннектора осторожно накрутите металлическую трубку до упора в корпус.

Последний штрих — обжим металлической трубочки вокруг торца корпуса разъема. Для этого раскройте инструмент (рис. 7.5) и найдите вырез нужного размера на рабочей поверхности пресса. По длине он совпадает с длиной металлической трубочки или немного меньше ее. Установите в него металлическую трубочку так, чтобы поверхность пресса покрывала ее по всей длине. Сильно сожмите ручки инструмента. Многие инструменты снабжены своего рода фиксатором, который издает щелчок, когда обжим коннектора закончен. Если такого фиксатора в вашем инструменте нет, сами определите момент окончания обжи-

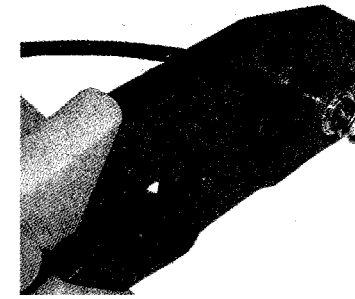


Рис. 7.5. Обжимаем коннектор с помощью обжимного инструмента

ма. В результате металлическая трубочка плотно сожмет торец корпуса разъема, приняв форму шестиугольника (по форме выреза на прессе инструмента).

7.4. Установка Т-коннекторов и заглушек

Установка Т-коннекторов и терминаторов является последним этапом в создании сети. Для нее не нужны вспомогательные инструменты.

Т-коннектор просто включают в разрыв кабельной системы. При этом два коннектора, находящиеся на концах кабеля, вставляют в Т-коннектор. На коннекторе есть два небольших выступа с противоположных сторон. Используя прорези на Т-коннекторе, зафиксируйте коннектор, вставив его до упора и немного провернув (рис. 7.6).

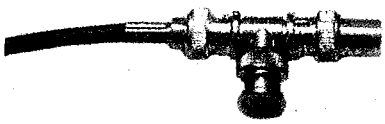


Рис. 7.6. Соединение Т-коннектора, BNC-коннектора и терминатора

Количество Т-коннекторов зависит от числа компьютеров, которые подсоединяются к сети.

Заглушек-терминаторов используют всего две. Каждую из них нужно надеть на конец кабельного сегмента. Как правило, делают это на последнем компьютере на одном из концов Т-коннектора, который надевают на разъем сетевой карты (рис. 7.7). Один из терминаторов необходимо обязательно заземлить. Для этого он снабжен цепочкой с контактом на конце, который можно прикрутить шурупом к любому заземленному предмету.

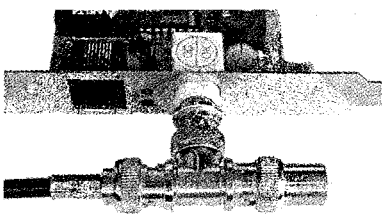


Рис. 7.7. Терминатор, установленный на Т-коннекторе сетевой карты

Проверить работоспособность сети можно будет после настройки операционной системы компьютера. А пока понаблюдайте: если на сетевой карте светится индикатор, значит, все нормально.

Глава 8

Сеть на основе витой пары

- Принципы прокладки проводки
- Подготовка кабеля
- Монтаж сетевых розеток
- Монтаж разъемов RJ-45

Сеть, построенная с применением кабеля на основе витой пары, — самый распространенный тип из-за ее легкой расширяемости и достаточного запаса производительности. Используя кабель пятой категории, можно добиться скорости передачи данных 100 Мбит/с, чего вполне хватает для выполнения большинства задач. Мало того, если придерживаться стандартов обжима кабеля, можно в дальнейшем использовать кабельную систему для модернизации сети до уровня Gigabit Ethernet.

Прежде чем приступить к действиям, нужно хорошо подготовиться — отсутствие теоретической базы может помешать вам в создании работоспособной сети.

Рассмотрим пример построения сети с использованием стандарта Fast Ethernet 100Base-TX.

ПРИМЕЧАНИЕ

Из видеоуроков «Урок 8.1. Обжим кабеля на основе витой пары» и «Урок 8.2. Подключение кабеля на основе витой пары к компьютеру», которые находятся на компакт-диске, прилагаемом к книге, вы узнаете, как правильно обжимать кабель на основе витой пары, а также как подключить готовый кабель к компьютеру.

8.1. Принципы прокладки проводки

Прежде всего вспомним об основных ограничениях сети, построенной с применением кабеля на основе витой пары:

- длина сегмента не должна превышать 100 м;
- количество компьютеров, которые подключены к сети, должно быть меньше 1024;
- количество повторителей в сети — не более 4;
- для соединения репитеров используется кабель длиной не более 5 м.

Планировать сеть нужно, исходя из этого. Однако прежде поговорим о кабеле, а точнее, о сигнале, который по нему передается.

Почему длина сегмента не должна превышать 100 м? Все очень просто. Возьмем для примера сеть, состоящую из двух компьютеров и одного репитера.

Предположим, что сформированный особым образом электрический сигнал должен пройти от одного компьютера к другому. Существует несколько факторов, влияющих на скорость доставки сигнала от отправителя к адресату.

- Сетевая карта отправителя. Формируется пакет данных, снабженный необходимой служебной информацией, после чего сигнал передается по кабелю, сопротивление которого идеально соотносится с сопротивлением выхода на сетевой карте. В обоих случаях оно составляет 50 Ом. Таким образом, первая задержка осуществляется сетевой картой и составляет 0,25 мкс — время, необходимое для формирования сигнала.
- Сигнал передается по кабелю, проходя расстояние от сетевой карты отправителя до первого репитера (концентратора). Учитывая то, что задержка, вызываемая сопротивлением кабеля, составляет 0,55 мкс[1], получаем вторую задержку.
- Сигнал проходит через репитер, одной из функций которого является обновление сигнала, то есть сигнал формируется заново. После этого он отправляется на все остальные порты репитера кроме того, с которого был получен. Таким образом, в зависимости от типа репитера[2] получаем третью задержку — от 0,35 до 0,7 мкс.

Данная последовательность описывает только половину пути, которую проходит сигнал от сетевой карты отправителя. Другая половина пути — доставка сигнала через остальную часть кабеля и сетевую карту получателя (адресата).

Согласно требованиям, предъявляемым к скорости передачи данных, общая задержка, например, для сети со скоростью 100 Мбит/с должна быть не более 5,12 мкс. Таким образом, получаем следующую формулу:

2 (первая задержка) + 2 (вторая задержка) + 2 – X (третья задержка) < 5,12.

Чтобы узнать, какое количество репитеров можно применять в сети, вводят неизвестное X. Если количество репитеров больше положенного, то сигнал будет недостаточно сильным, что приведет к появлению коллизий.

---

[1] Данный показатель определяет задержку в передаче сигнала на расстояние, равное 100 м.

[2] Различают репитеры двух классов. Репитеры второго класса формируют и передают сигнал примерно в 1,5–2 раза быстрее, чем аналогичные репитеры первого класса.

Топологические модели

При создании сети используется одна из двух топологических моделей.

Суть первой заключается в том, что при расчете задержек сигнала, которые возникают при его прохождении через сетевое оборудование, предполагается, что эти задержки являются максимально возможными.

При другой модели вычисляют реальную задержку. Это позволяет добиться максимальной длины сегмента. Подсчитать точно время задержек без специального оборудования достаточно сложно, поэтому вторую модель используют реже.

В случае использования первой модели допускается два варианта:

- применяют только один репитер (длина каждого сегмента не должна превышать 100 м) (рис. 8.1);

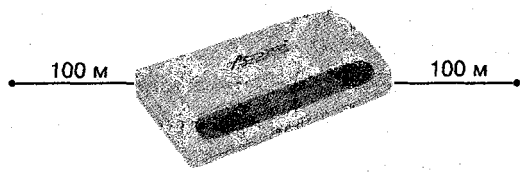


Рис. 8.1. Схема с одним репитером

- применяют два репитера (длина каждого сегмента не должна превышать 100 м; их соединяют отрезком кабеля длиной до 5 м) (рис. 8.2).

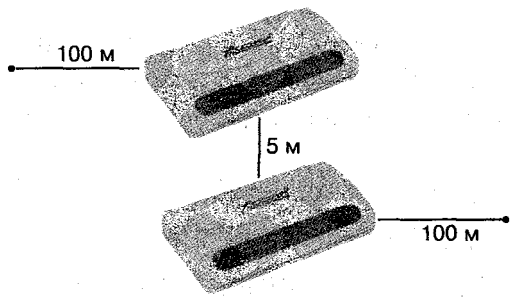


Рис. 8.2. Схема с двумя репитерами

Правила прокладки кабеля

Для бесперебойной работы сети при прокладке кабеля нужно придерживаться простых правил.

1. Правильно выбирайте место прокладки. Старайтесь исключать ситуации, когда на кабель можно будет случайно наступить, так как он может деформироваться или оборваться, что приведет к выходу из строя всей сети. На него также нельзя ставить тяжелые предметы.
2. Излишнее натяжение кабеля может привести к его обрыву возле коннектора, что также выведет из строя всю сеть. Кроме того, перепрыгивать через натянутый провод не понравится ни вам самим, ни уж точно вашему шефу. Это же правило относится и к случаю, когда нужно проложить кабель между двумя домами. Используйте для этого стальной трос (или прочный капроновый шнур), прикрепив к нему на одинаковом расстоянии хомуты, которыми будет удерживаться сам кабель.
3. Исключайте возможность скопления кабеля. Чрезмерное концентрация в одном месте, например сложенный кругами лишний отрезок, может вызвать электрические наводки, что непременно приведет к появлению коллизий.
4. Рано или поздно при прокладке кабеля наступает момент, когда нужно изогнуть кабель. В этом случае следует помнить, что радиус изгиба не должен быть меньше 4–5 см.
5. Избегайте прокладки кабеля вдоль электропроводки и возле электрощитов. Все это способствует возникновению электрических наводок в кабеле, что приводит к коллизиям.
6. Не прокладывайте кабель возле отопительных элементов. Батарея центрального отопления и другие теплогенерирующие приборы отрицательно влияют на него. Излишний нагрев может вызвать изменение в сопротивлении кабеля, из-за чего также возникают коллизии.

Усвоив эти простые правила, можно приступать к построению сети. Прежде всего подготовьте кабель, затем обожмите коннекторы. После этого можно подключать их к сетевым картам, подсоединяя кабель непосредственно к их разъемам или используя для этого специальные розетки.

8.2. Подготовка кабеля

Кабель на основе витой пары, как правило, продают в специальных бухтах. Кабель намотан на катушку и помещен в картонную коробку (рис. 8.3).

Прежде всего определите, сколько и какой длины нужны отрезки кабеля. Для этого необходимо примерно составить схему расположения компьютеров.

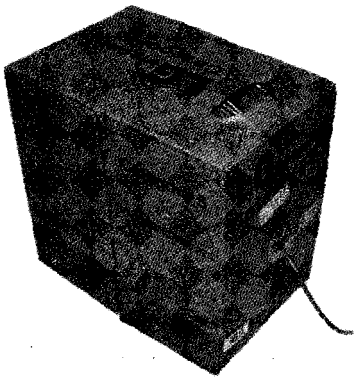


Рис. 8.3. Бухта с кабелем

Как показывает практика, сеть можно прокладывать правильно или необдуманно.

Правильный способ прокладки подразумевает использование специальных коробов, в которые прячут все кабели. Это делают не только с целью безопасности, но и чисто с эстетической точки зрения. Маршрут выбирают или стандартный[1], или не противоречащий правилам прокладки. Такой способ используют при создании сети в офисах или масштабных помещениях.

Второй способ подразумевает прокладку без строгой организации. Кабель можно вести в открытом виде, вдоль стен или просто перекидывать между компьютерами. Такой тип прокладки обычно используют в домашних условиях, когда не нужно соединять много компьютеров. Понятно, что предъявлять какие-либо требования к безопасности в этом случае бессмысленно.

Выбрав соответствующий способ прокладки кабеля, следует подумать, где будет находиться концентратор и (или) другое сетевое оборудование. Не забывайте, что применение кабеля на основе витой пары подразумевает использование топологии «звезда». Это означает, что все провода будут тянуться в одно фиксированное место — к вашему активному оборудованию. В связи с этим нужно заранее подготовить место, где оно будет располагаться. Если следовать правилам, то для сети, состоящей из 10–20 компьютеров, нужно организовывать отдельную коммуникационную комнату. Если выделить комнату невозможно, то попробуйте установить коммуникационный шкаф. Его размер подбирают согласно требованиям. Кроме того, можно выбрать шкаф, который крепится на стену, для него подойдет любой свободный угол или другое место в комнате.

Если будущая сеть не предполагает серьезных расширений, то для 5–10 компьютеров вполне можно использовать простенький концентратор.

---

[1] Как правило, кабель от компьютера прокладывают по стене и выводят в коридор, то есть основная линия идет вне помещения.

Создав предварительный рисунок сети на бумаге, можно приступать к подготовке отрезков кабеля нужной длины.

СОВЕТ

При подготовке отрезков кабеля увеличивайте их длину на 10–20 % для более удобной прокладки и обжима коннекторов или монтажа сетевых розеток.

Если следовать правилам, то с целью безопасности для подключения компьютеров к сетевому сегменту следует использовать специальные сетевые розетки.

ПРИМЕЧАНИЕ

Использовать сетевую розетку очень удобно, ведь при изменении места расположения компьютера не нужно удлинять весь кабельный сегмент. В этом случае просто создается новый шнур, соединяющий компьютер с розеткой.

Если вы хотите использовать такие розетки, то длину отрезков кабеля нужно считать до их места расположения.

От сетевой розетки к компьютеру будет идти другой кабель, называемый патч-кордом (см. главу 4). Длина патч-корда, как правило, составляет 2,5–3 м. Если расположение какого-либо компьютера относительно сетевой розетки не вписывается в данный размер, патч-корд придется сделать более длинным.

ВНИМАНИЕ

При подготовке патч-корда внимательно проводите необходимые измерения.

Подготовив отрезки нужной длины, можно приступать к работе по подготовке кабеля.

Если вы планируете прокладывать кабель в специальных коробах, прежде всего нужно закрепить основу на стене. Далее аккуратно поместите кабель в короб и закройте крышкой. На обеих сторонах короба должны остаться концы кабеля достаточной длины для удобного обжима или монтажа розеток.

Каждый конец кабеля аккуратно обрежьте, воспользовавшись резаком обжимного инструмента или обычными ножницами (рис. 8.4).

Снимите с кабеля внешнюю изоляцию длиной примерно 12–15 мм (рис. 8.5). Это можно сделать обжимным инструментом или ножом.

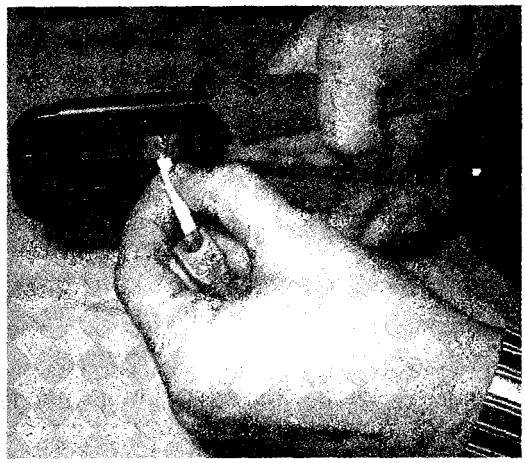


Рис. 8.4. Обрезаем конец кабеля

Рис. 8.5. Снимаем внешнюю оболочку кабеля

ВНИМАНИЕ

При снятии внешней оболочки не повредите изоляцию проводников.

Отделив пары проводников друг от друга, расплетите и выровняйте их.

Расположите проводники согласно одному из стандартов, к примеру EIA/TIA-568B (рис. 8.6).

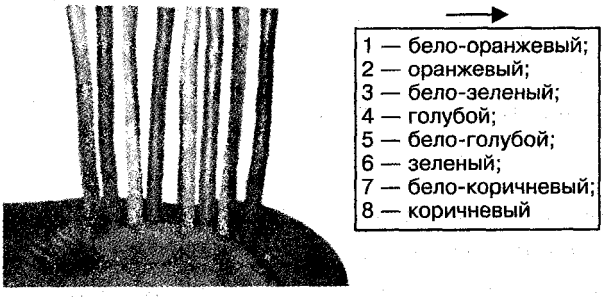


Рис. 8.6. Пример расположения проводников

ВНИМАНИЕ

Обязательно придерживайтесь единого стандарта при обжиме коннекторов и монтаже сетевых розеток.

Если проводники оказались слишком длинными, отрежьте излишек резцами обжимного инструмента или ножницами. Старайтесь оставлять длину проводников равной 12–15 мм[1].

Аналогичным образом поступите с патч-кордами.

После подготовки кабеля можно переходить к монтажу сетевых розеток.

8.3. Монтаж сетевых розеток

Как уже упоминалось выше, можно обойтись и без розеток. Однако если вы решили все делать по правилам, нужно их использовать.

Если снять с розетки верхнюю крышку (рис. 8.7), то будут видны две группы контактов. Для облегчения монтажа каждый из них пронумерован согласно нескольким самым популярным стандартам. Поэтому отсортировать нужным образом проводники кабеля не сложно.

После того как проводники расставлены согласно стандарту, который вы используете, их нужно зажать в соответствующие контакты. Для этого служит специальный инструмент — нож-вставка. Легкое нажатие ножом на проводник не только оголяет центральную жилу, но и надежно зажимает ее в контакте.

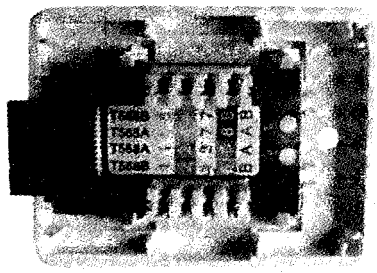


Рис. 8.7. Контактные группы

8.4. Монтаж разъемов RJ-45

После завершения подготовки кабелей и расстановки сетевых розеток (если они используются) можно приступать к обжиму коннекторов.

Как вы уже знаете, кабель, который соединяет сетевую карту компьютера с сетевой розеткой, называется патч-кордом. Если вы делали монтаж розеток, то у вас остались отрезки кабеля, которые и будут служить патч-кордами. Если использование сетевых розеток не предполагалось, патч-корды не нужны.

---

[1] Именно такая длина расплетенных проводников необходима для соблюдения стандарта 100Base-TX.

Как бы там ни было, перед вами стоит задача обжать концы кабеля коннекторами. Эту операцию нужно произвести как минимум дважды, а если используются сетевые розетки, то трижды (один из концов кабеля в этом случае уже зажат в контактных группах розеток).

Для обжима коннектора используют специальный обжимной инструмент (см. главу 4).

Чтобы правильно сделать обжим, придерживайтесь следующей схемы.

1. Возьмите подготовленный кабель.
2. Наденьте на кабель пластмассовый колпачок таким образом, чтобы его широкая часть была направлена в сторону кончиков проводников.
3. Проверьте правильность расположения проводников, руководствуясь изображением, показанным на рис. 8.6. На нем приведен пример расположения проводников согласно стандарту EIA/TIA-568B.

ВНИМАНИЕ

Не забывайте, что при создании сети, а именно при монтаже сетевых розеток и обжиме коннекторов, обязательно нужно использовать единый стандарт.

4. Проверьте, чтобы длина проводников не превышала 12,5–13 мм (примерно половина длины коннектора). Лишнюю часть удалите резцами обжимного инструмента или ножницами.
5. Расположите коннектор таким образом, чтобы окошко разъема находилось перед вами, а пластмассовая защелка — снизу коннектора.
6. Плотно сожмите проводники двумя пальцами. Затем медленным движением вставьте концы проводников в окошко разъема, чтобы они равномерно распределились по всей его ширине.
7. Проталкивая проводники вглубь коннектора, следите, чтобы они не поменяли свое расположение относительно друг друга.
8. Проталкивайте проводники до тех пор, пока они не упрутся в перегородку. Проследите, чтобы все проводники упирались в стенку. Если есть какое-либо отклонение, то вытяните их, выровняйте и повторите действия, описанные в пунктах 6–8.
9. После того как проводники плотно вставлены в коннектор, еще раз убедитесь в правильности их расположения согласно выбранному стандарту.

10. Если правильность расположения сохранилась, вставьте коннектор в соответствующее гнездо обжимного инструмента и сильно сожмите его (рис. 8.8).
11. Задвиньте на обжатый коннектор надетый ранее на провод пластмассовый колпачок (рис. 8.9).

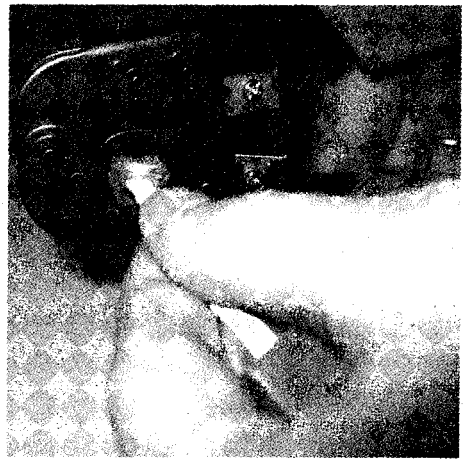


Рис. 8.8. Обжимаем коннектор с помощью специального инструмента

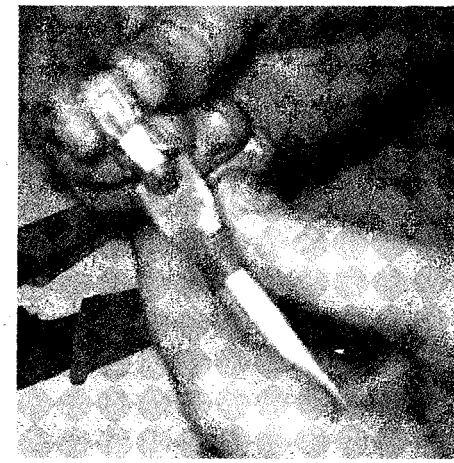


Рис. 8.9. Надеваем колпачок

Рис. 8.10. Обжатые коннекторы: правильно *(слева)*, неправильно *(справа)*

Если обжим коннектора выполнен качественно и по приведенной выше схеме, то у вас должен получиться коннектор примерно как на рис. 8.10 *слева*. Если вы игнорировали лишнюю длину проводников, то у вас получится так, как показано на рис. 8.10 *справа*. Вне зависимости от внешнего вида обжима коннектора его работоспособность сохраняется, однако надежность монтажа второго из них вызывает сомнение, легко представить, что с ним произойдет при натяжении кабеля.

Коннекторы можно обжать и без специального инструмента, пользуясь обычной отверткой, для этого они должны быть с контактными фиксаторами. Такой способ менее надежен.

ПРИМЕЧАНИЕ

В случае соединения нескольких компьютеров без применения коробов гораздо проще приобрести нужной длины отрезки кабеля с обжатыми коннекторами в компьютерном магазине или сервисе. В этом случае вам не понадобится обжимной инструмент. Кроме того, все отрезки кабеля можно снабдить клейкими лентами с указанием номера порта на концентраторе, что облегчит их идентификацию при подключении оборудования.

Часть 3

Беспроводная сеть

Глава 9

Спецификация и топология беспроводной сети

- Методы и технологии модуляции сигнала
- Топология беспроводной сети
- Стандарты беспроводной Ethernet
- Преимущества и недостатки беспроводной сети

Беспроводная сеть, как и проводная, требует изначального проектирования, то есть необходимо заранее, насколько это возможно, спланировать расположение клиентских компьютеров и их количество. Дело в том, что именно от этого зависит, какую из топологий сети необходимо будет использовать, что связано с особенностями распространения радиоволн.

Кроме того, действуют некоторые стандарты, которые описывают правила функционирования сети для обеспечения максимальной ее производительности.

Необходимо отметить, что существует несколько типов беспроводных сетей, которые характеризуются разными показателями производительности и условиями использования. Наибольшее распространение среди них получили Wi-Fi-сети, которые и будут рассмотрены в данной книге.

В этой главе я расскажу о топологиях беспроводной сети, сетевых стандартах, технологиях передачи данных и о многом другом.

9.1. Методы и технологии модуляции сигнала

Методы и технологии модуляции сигнала на физическом уровне меняются в зависимости от стандарта беспроводной сети. В этом нет ничего странного, поскольку каждая технология имеет свои ограничения и достичь каких-либо новых результатов с применением старых технологий удается крайне редко.

Как бы там ни было, на сегодняшний день существуют следующие спецификации и технологии физического уровня беспроводной сети.

- Спецификация для работы в инфракрасном диапазоне.
- Спецификация DSSS (Direct Sequence Spread Spectrum) — определяет работу устройств в диапазоне радиочастот по радиоканалам с широкополосной модуляцией с прямым расширением спектра методами прямой псевдослучайной последовательности.
- Спецификация FHSS (Frequency Hopping Spread Spectrum) — определяет работу устройств в диапазоне радиочастот по радиоканалам с широкополосной модуляцией со скачкообразной перестройкой частоты методами псевдослучайной перестройки частоты.
- Спецификация OFDM (Orthogonal Frequency Division Multiplexing) — определяет работу устройств в диапазоне радиочастот по радиоканалам с использованием подканалов с разными несущими частотами.

- Метод двоичного пакетного сверточного кодирования PBCC (Packet Binary Convolutional Coding).
- Технология кодирования Баркера — описывает способ кодирования данных с помощью последовательностей Баркера.
- Технология CCK (Complementary Code Keying) — описывает способ дополнительного кодирования битов передаваемой информации.
- Технология CCK-OFDM — описывает способ кодирования данных с помощью гибридного метода, что позволяет увеличить скорость передачи сигнала при невысокой избыточности данных.
- Технология QAM (Quadrature Amplitude Modulation, QAM) — описывает способ квадратурной амплитудной модуляции сигнала, который работает на скорости выше 48 Мбит/с.

Когда появились первые образцы оборудования, они работали в диапазоне частот 902–928 МГц. При этом достигалась скорость передачи данных 215–860 Кбит/с с использованием метода расширения спектра прямой последовательностью (DSSS). Указанный диапазон частот разбивался на каналы шириной около 5 МГц, что при скорости передачи данных 215 Кбит/с составляло 5 каналов. При максимальной скорости передачи данных спектр сигнала достигал 19 МГц, поэтому получался только один частотный канал шириной 26 МГц.

Когда это оборудование только появилось, то его скорости передачи данных было достаточно для многих задач при нескольких подключенных компьютерах. Однако чем больше присоединялось машин, тем ниже становилась скорость. Например, если к сети подключено 5 компьютеров, то реальная скорость передачи данных в 5 раз меньше теоретической. Вот и получается, что чем больше компьютеров в сети, тем меньше скорость, что при теоретической скорости передачи данных 860 Кбит/с чрезвычайно мало.

Конечно, скорость можно было бы со временем и увеличить, однако начали сказываться и другие факторы, самым главным из которых стало использование диапазона 900 МГц операторами мобильной связи. Именно этот факт и привел к тому, что первое оборудование не прижилось среди пользователей. После анализа сложившейся ситуации было принято решение использовать диапазон частот 2400–2483,5 МГц, а вскоре — 5150–5350 МГц и 5725–5875 МГц. Это позволило добиться не только большей пропускной способности, но и лучшей помехозащищенности. Кроме того, потенциал использования высоких частот намного больше.

Метод DSSS

Смысл расширения спектра методом прямой псевдослучайной последовательности (DSSS) заключается в приведении узкополосного спектра сигнала к его широкополосному представлению, что позволяет увеличить помехоустойчивость передаваемых данных.

При использовании метода широкополосной модуляции с прямым расширением спектра диапазон 2400–2483,5 МГц делится на 14 перекрывающихся каналов или три неперекрывающихся канала с промежутком в 25 МГц.

Для пересылки данных используется всего один канал. Чтобы повысить качество передачи и снизить потребление энергии[1] (за счет снижения мощности передаваемого сигнала), используется последовательность Баркера, которая характеризуется достаточно большой избыточностью, позволяющей избежать повторной передачи данных, даже если пакет частично поврежден.

Метод FHSS

При использовании метода широкополосной модуляции со скачкообразной перестройкой частоты диапазон 2400–2483,5 МГц делится на 79 каналов шириной 1 МГц. Данные передаются последовательно по разным каналам, создавая определенную схему переключения между ними. Всего существуют 22 такие схемы, причем схему переключения должен согласовать как отправитель данных, так и их получатель. Схемы переключения разработаны таким образом, что шанс использования одного канала разными отправителями минимален.

Переключение между каналами происходит очень часто, что обусловлено малой шириной канала (1 МГц). Поэтому метод FHSS в своей работе использует весь доступный диапазон частот, а соответственно и все каналы.

Метод OFDM

Метод ортогонального частотного мультиплексирования является одним из «продвинутых» и скоростных методов передачи данных. В отличие от методов DSSS и FHSS, он осуществляет параллельную передачу данных по нескольким частотам радиодиапазона. При этом данные еще и разбиваются на

[1] Большое потребление энергии является критичным для переносных компьютеров.

части, что позволяет не только увеличить скорость передачи, но и улучшает ее качество.

Данный метод модуляции сигнала может работать в двух диапазонах: 2,4 и 5 ГГц.

Метод PBCC

Метод двоичного пакетного сверточного кодирования (Packet Binary Convolutional Coding, PBCC) используется (опционально) при скорости передачи данных 5,5 и 11 Мбит/с. Этот же метод, только слегка модифицированный, используется и при скорости передачи данных 22 Мбит/с.

Принцип метода базируется на том, что каждому биту информации, который нужно передать, ставятся в соответствие два выходных бита (так называемый дибит), созданных в результате преобразований с помощью логической функции XOR и нескольких запоминающих ячеек[1]. Поэтому этот метод и носит название сверточного кодирования со скоростью 1/2, а сам механизм кодирования называется сверточным кодером.

ПРИМЕЧАНИЕ

При скорости входных битов N бит/с скорость выходной последовательности (после сверточного кодера) составляет 2N бит/с. Отсюда и понятие скорости — один к двум (1/2).

Использование сверточного кодера позволяет добиться избыточности кода, что, в свою очередь, повышает надежность приема данных.

Чтобы отправить готовый дибит, используют фазовую модуляцию сигнала. При этом, в зависимости от скорости передачи, используют один из методов модуляции: двоичная фазовая модуляция (BPSK, скорость передачи 5,5 Мбит/с) или квадратичная фазовая модуляция (QPSK, скорость передачи 11 Мбит/с). Смысл модуляции заключается в том, чтобы ужать выходной дибит до одного символа, не теряя при этом избыточности кода. В результате скорость поступления данных будет соответствовать скорости их передачи, но при этом уже иметь сформированную избыточность кода и более высокую помехозащищенность.

---

[1] В протоколах 802.11b и 802.11g используются сверточные кодеры, состоящие из шести запоминающих ячеек.

Метод PBCC позволяет работать со скоростью передачи данных 22 и 33 Мбит/с. При этом используется пунктурный кодер и другая фазовая модуляция.

Например, рассмотрим скорость передачи данных 22 Мбит/с, которая вдвое выше скорости 11 Мбит/с. В этом случае сверточный кодер согласно своему алгоритму работы из каждых двух входящих битов будет делать четыре исходящих. Это приводит к слишком большой избыточности кода, что не всегда подходит при тех или иных условиях помех. Поэтому, чтобы уменьшить лишнюю избыточность, используется пунктурный кодер, задача которого — удаление лишнего бита в группе из четырех битов, которые выходят из сверточного кодера.

Таким образом, каждым двум входящим битам в соответствие ставятся три бита, которые содержат достаточную избыточность. Далее они проходят через модернизированную фазовую модуляцию (8-позиционная фазовая модуляция, 8-PSK), которая упаковывает их в один символ, готовый к передаче.

Технология кодирования Баркера

Чтобы повысить помехоустойчивость передаваемого сигнала, то есть увеличить вероятность безошибочного его распознавания на приемной стороне в условиях шума, можно воспользоваться методом перехода к широкополосному сигналу, добавляя избыточность в исходный. Для этого в каждый передаваемый информационный бит «встраивают» определенный код, состоящий из последовательности так называемых чипов.

Чтобы особо не вникать в математические подробности, можно сказать лишь то, что, подобрав специальную комбинацию последовательности чипов и превратив исходящий сигнал практически в нераспознаваемый шум, в дальнейшем, при приеме, сигнал умножается на специальным образом вычисленную корреляционную функцию (код Баркера). В результате все шумы становятся в 11 раз слабее, при этом остается только полезная часть сигнала — непосредственно данные.

Казалось бы, что можно сделать с сигналом, который состоит из сплошного шума? На самом деле, применив код Баркера, можно достичь гарантированного качества доставки данных.

Технология CCK

Технологию кодирования с использованием комплементарных кодов (Complementary Code Keying, CCK) используют для кодирования битов данных с целью их сжатия, что позволяет достичь повышения скорости передачи.

Изначально эта технология начала использоваться в стандарте IEEE 802.11b, что позволило достичь скорости передачи данных 5,5 и 11 Мбит/с. При этом с ее помощью удается кодировать несколько битов в один символ. В частности, при скорости передачи данных 5,5 Мбит/с один символ равен 4 битам, а при скорости 11 Мбит/с — 8 битам данных.

Данный способ кодирования описывается достаточно сложными системами математических уравнений, в основе которых лежат комплементарные 8-разрядные комплексные последовательности.

Технология CCK-OFDM

Технологию гибридного кодирования CCK-OFDM используют при работе оборудования как с обязательными, так и с опциональными скоростями передачи данных.

Как уже упоминалось ранее, при передаче данных используют пакеты данных, имеющие специальную структуру. Как минимум эта структура содержит служебный заголовок. Так вот, при использовании гибридного кодирования CCK-OFDM служебный заголовок пакета строится с помощью CCK-кодирования, а сами данные — с помощью OFDM-кодирования.

Технология QAM

Технологию квадратурной амплитудной модуляции (Quadrature Amplitude Modulation, QAM) применяют в случаях высоких скоростей передачи данных (начиная с 24 Мбит/с). Суть ее в том, что повышение скорости передачи данных происходит за счет изменения фазы сигнала и его амплитуды. При этом используют модуляции 16-QAM и 64-QAM, которые позволяют кодировать четыре бита в одном символе при 16 разных состояниях сигнала в первом случае и шесть битов в одном символе при 64 разных состояниях сигнала во втором.

Обычно модуляцию 16-QAM используют при скоростях передачи данных 24 и 36 Мбит/с, а модуляции 64-QAM — при 48 и 54 Мбит/с.

9.2. Топология беспроводной сети

Специфика использования радиоэфира в качестве среды передачи данных накладывает свои ограничения на топологию сети. Если сравнивать ее с топологией проводной сети, то наиболее близкими вариантами оказываются топология «звезда» и комбинированная топология «кольцо» и «общая шина».

Следует упомянуть, что развитие беспроводных сетей, как и многое другое, проходит под неусыпным контролем соответствующих организаций. И самой главной среди них является Институт инженеров электротехники и электроники (Institute of Electrical and Electronic Engineers, IEEE). В частности, беспроводные стандарты, сетевое оборудование и все, что относится к беспроводным сетям, контролирует Рабочая группа по беспроводным локальным сетям (Working Group for Wireless Local Area Networks, WLAN), в состав которой входят более 100 представителей из разных университетов и фирм-разработчиков сетевого оборудования. Эта комиссия собирается несколько раз в год с целью совершенствования существующих стандартов и создания новых, базирующихся на последних исследованиях и компьютерных достижениях.

В России также организована ассоциация БЕспроводных СЕтей передачи ДАнных («БЕСЕДА»), которая занимается ведением единой политики в области беспроводных сетей передачи данных. Она же и контролирует развитие рынка беспроводных сетей, предоставляет различные услуги при подключении, создает и развивает новые центры беспроводного доступа и т. д.

Теперь что касается непосредственно топологии беспроводных сетей. На сегодняшний день используют два варианта беспроводной архитектуры или, проще говоря, варианта построения сети: *независимая конфигурация* (Ad-Hoc) и *инфраструктурная конфигурация*. Отличия между ними незначительные, однако они кардинально влияют на такие показатели, как количество подключаемых пользователей, радиус сети, помехоустойчивость и т. д.

Независимая конфигурация

Режим независимой конфигурации (рис. 9.1), часто еще называемый «точка-точка», или независимый базовый набор служб (Independent Basic Service Set, IBSS), — самый простой в применении. Соответственно такая беспроводная сеть является самой простой в построении и настройке.

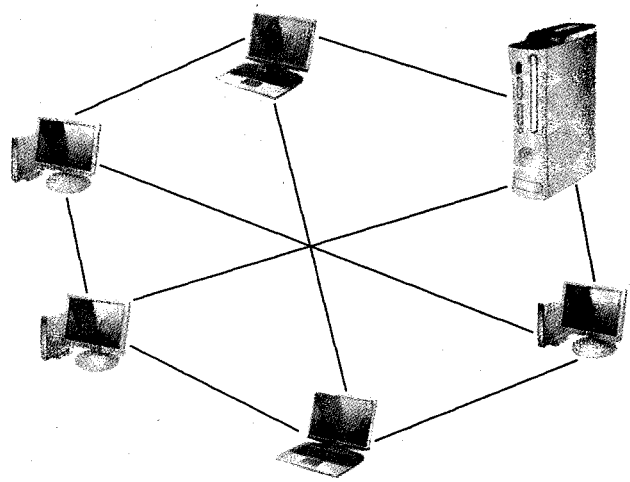


Рис. 9.1. Режим независимой конфигурации

Чтобы объединить компьютеры в беспроводную сеть, достаточно, чтобы каждый из них имел адаптер беспроводной связи. Как правило, такими адаптерами изначально оснащают переносные компьютеры, что вообще сводит построение сети только к настройке доступа к ней.

Обычно такой способ организации используют, если сеть строится хаотично или временно, а также если другой способ построения не подходит по каким-либо причинам.

Режим независимой конфигурации, хоть и прост в построении, имеет некоторые недостатки, главными из которых являются малый радиус действия сети и низкая помехоустойчивость, что накладывает ограничения на расположение компьютеров сети. Кроме того, если нужно подключиться к внешней сети или к Интернету, то сделать это будет непросто.

ПРИМЕЧАНИЕ

В случае соединения двух компьютеров при использовании узконаправленных антенн радиус действия сети увеличивается, а в отдельных случаях может достигать 30 и более километров.

Инфраструктурная конфигурация

Инфраструктурная конфигурация, или, как ее еще часто называют, режим «клиент/сервер», — более перспективный и быстроразвивающийся вариант беспроводной сети.

Она имеет много плюсов, главными из которых являются возможность подключения достаточно большого количества пользователей, более высокая помехоустойчивость, полный контроль подключений и многое другое. Кроме того, есть возможность использования комбинированной топологии и проводных сегментов сети.

Для организации беспроводной сети с использованием инфраструктурной конфигурации, кроме адаптеров беспроводной связи, установленных на компьютерах, также необходимо иметь как минимум одну точку доступа (Access Point) (см. рис. 4.13).

В этом случае конфигурация носит название базового набора служб (Basic Service Set, BSS). Точка доступа может работать как автономно, так и в составе проводной сети и служить мостом между проводным и беспроводным сегментами сети. При такой конфигурации компьютеры общаются только с точкой доступа, которая и руководит передачей данных между ними (рис. 9.2) (в проводной сети аналогом является концентратор).

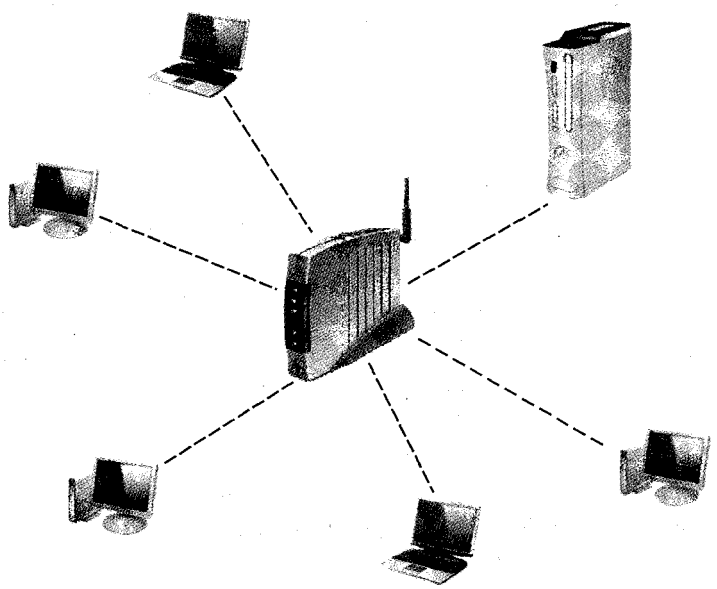


Рис. 9.2. Инфраструктурная конфигурация, базовый набор служб

Конечно, одной точкой доступа сеть может не ограничиваться, что и случается с ее ростом. В этом случае базовые наборы служб образуют единую сеть, конфигурация которой носит название расширенного набора служб (Extended

Service Set, ESS). В этом случае точки доступа обмениваются между собой информацией, передаваемой через проводное соединение (рис. 9.3) или через радиомосты, что позволяет эффективно организовывать трафик в сети между ее сегментами (фактически точками доступа).

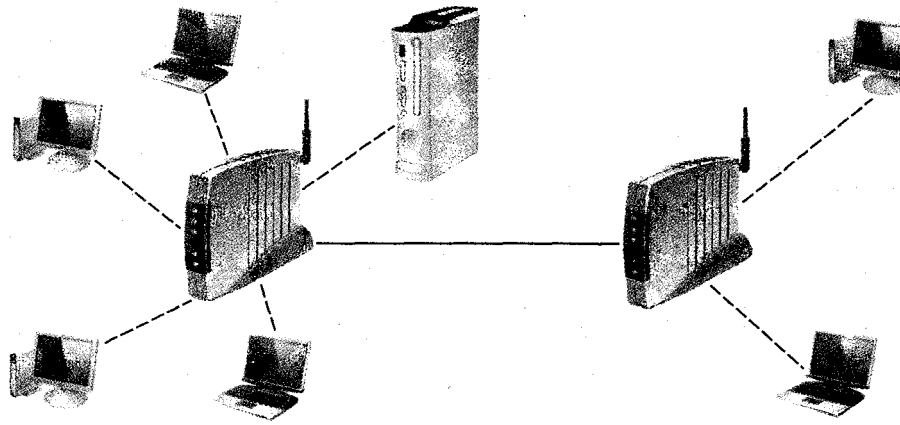


Рис. 9.3. Инфраструктурная конфигурация, расширенный набор служб

9.3. Стандарты беспроводной сети Ethernet

Развитие технологии Radio Ethernet началось с 1990 года. Первопроходцами стали специалисты Института инженеров электротехники и радиоэлектроники, которые были объединены в группу 802.11 Working Group. Разработка длилась более пяти лет и завершилась созданием спецификации IEEE 802.11 — группы стандартов для беспроводных локальных сетей.

Radio Ethernet представляет собой набор стандартов беспроводной передачи данных. Они получают все большее распространение среди пользователей Интернета благодаря некоторым преимуществам перед стандартами, использующими для передачи данных кабельную систему.

Ниже описаны все существующие стандарты IEEE 802.11, которые предписывают метод передачи данных, скорость передачи данных, метод модуляции, мощность передатчиков, полосы частот, на которых они работают, методы аутентификации, шифрования и многое другое.

С самого начала так сложилось, что часть стандартов работает на физическом уровне, часть — на уровне среды передачи данных, а остальные — на более вы-

соких уровнях модели взаимодействия открытых систем ISO/OSI. Существует следующее деление на группы:

- стандарты IEEE 802.11a, IEEE 802.11b и IEEE 802.11g — описывают работу сетевого оборудования (физический уровень);
- стандарты IEEE 802.11d, IEEE 802.11e, IEEE 802.11i, IEEE 802.11j, IEEE 802.11h и IEEE 802.11r — описывают параметры среды, частоты радиоканала, средства безопасности, способы передачи мультимедийных данных и т. д.;
- стандарты IEEE 802.11f и IEEE 802.11c — описывают принцип взаимодействия между собой точек доступа, работу радиомостов и т. п.

Стандарт IEEE 802.11

Стандарт IEEE 802.11 был первенцем в стандартах беспроводной сети. Работу над ним начали еще в 1990 году. Как и полагается, занималась этим рабочая группа из IEEE. Их целью была разработка единого стандарта для радиооборудования, которое работало на частоте 2,4 ГГц. При этом ставилась задача достичь скорости 1 и 2 Мбит/с при использовании методов DSSS и FHSS соответственно.

Работы над созданием стандарта закончились через 7 лет. Цель была достигнута, но скорость, которую он обеспечивал, оказалась слишком малой для современных потребностей. Поэтому рабочая группа из IEEE продолжила свою работу с целью создания новых, более скоростных стандартов.

При разработке стандарта 802.11 учитывались особенности сотовой архитектуры системы. Почему сотовой? Очень просто, достаточно вспомнить, что волны распространяются в разные стороны на определенный радиус. Вот и получается, что зона выглядит как сот. Каждый такой сот работает под управлением базовой станции, в качестве которой выступает точка доступа. Часто сот называют еще базовой зоной обслуживания.

Чтобы соты могли между собой общаться, используется специальная распределительная система (Distribution System, DS). Из недостатков распределительной системы стандарта 802.11 можно отметить отсутствие роуминга.

Также стандартом предусмотрена работа компьютеров без точки доступа в составе одного сота. В этом случае функции точки доступа выполняют сами рабочие станции.

Стандарт 802.11 разработан и ориентирован на оборудование, работающее в полосе частот 2400–2483,5 МГц. При этом радиус сота достигает 300 м, не ограничивая при этом топологию сети.

Стандарт IEEE 802.11a

IEEE 802.11a — перспективный стандарт беспроводной сети, который рассчитан на работу в двух радиодиапазонах: 2,4 и 5 ГГц. При этом используется метод OFDM, что позволяет достичь максимальной скорости передачи данных 54 Мбит/с. Кроме этой скорости, спецификациями предусмотрены и другие:

- обязательные — 6, 12 и 24 Мбит/с;
- необязательные — 9, 18, 36, 48 и 54 Мбит/с.

Как обычно, этот стандарт имеет свои преимущества и недостатки. Из преимуществ можно отметить следующие:

- использование параллельной передачи данных;
- высокая скорость передачи данных;
- возможность подключения большого количества компьютеров.

Недостатками являются:

- меньший радиус сети при использовании диапазона 5 ГГц (примерно 100 м);
- большая потребляемая мощность радиопередатчиков;
- более высокая стоимость оборудования по сравнению с оборудованием других стандартов;
- требуется наличие специального разрешения на использование диапазона 5 ГГц.

Чтобы иметь возможность достичь высоких скоростей передачи данных, стандарт IEEE 802.11a в своей работе использует технологию квадратурной амплитудной модуляции QAM.

Стандарт IEEE 802.11b

Работа над стандартом IEEE 802.11b (другое название — IEEE 802.11 High rate) была закончена в 1999 году, и именно с ним связано понятие Wi-Fi (Wireless Fidelity).

Его работа основана на методе прямого расширения спектра (DSSS) с использованием 8-разрядных последовательностей Уолша. При этом каждый бит данных кодируется с помощью последовательности дополнительных кодов (CCK). Это позволяет достичь скорости передачи данных 11 Мбит/с.

Как и базовый стандарт, стандарт IEEE 802.11b работает с частотой 2,4 ГГц, используя при этом не более трех неперекрывающихся каналов. Радиус действия сети при этом составляет около 300 м.

Отличительной особенностью этого стандарта является то, что в случае надобности (ухудшение качества сигнала, удаленность от точки доступа, помехи) скорость передачи данных может уменьшаться вплоть до 1 Мбит/с[1]. И наоборот, обнаружив, что качество сигнала улучшилось, сетевое оборудование автоматически повышает скорость передачи до максимального уровня. Этот механизм носит название динамического сдвига скорости.

ПРИМЕЧАНИЕ

Кроме оборудования стандарта IEEE 802.11b, часто можно встретить оборудование IEEE 802.11b+, отличие между которыми заключается лишь в скорости передачи данных. В последнем случае она составляет 22 Мбит/с благодаря использованию метода двоичного пакетного сверточного кодирования (PBCC).

Стандарт IEEE 802.11d

Стандарт IEEE 802.11d определяет параметры физических каналов и сетевого оборудования. Так, им описывается разрешенная мощность излучения передатчиков в допустимых законами диапазонах частот.

Этот стандарт очень важен, поскольку для работы сетевого оборудования используются радиоволны, которые, если не будут соответствовать указанным параметрам, могут помешать другим устройствам, работающим в этом или близко лежащем к нему диапазоне частот.

Стандарт IEEE 802.11e

Поскольку через сеть могут передаваться данные разных форматов и разной важности, то необходимо иметь механизм, который умел бы определять ее

[1] Предусмотрено поэтапное снижение скорости: 5,5, 2 и 1 Мбит/с.

и придавал их передаче необходимый приоритет. За это и призван отвечать стандарт IEEE 802.11e, который был специально разработан с целью передачи потокового видео или аудио с гарантированными качеством и доставкой.

Стандарт IEEE 802.11f

Стандарт IEEE 802.11f разработан с целью обеспечения аутентификации сетевого оборудования (рабочей станции), если компьютер пользователя перемещается от одной точки доступа к другой, то есть между сегментами сети. При этом вступает в действие протокол обмена служебной информацией (Inter-Access Point Protocol, IAPP), который необходим для передачи этой информации между точками доступа. При этом достигается эффективная организация работы распределенных беспроводных сетей.

Стандарт IEEE 802.11g

Наиболее продвинутым стандартом на сегодняшний день можно считать IEEE 802.11g, вобравший в себя все самое лучшее от IEEE 802.11b и IEEE 802.11b, а также содержащий много нового. Цель его создания — скорость передачи данных 54 Мбит/с.

Как и стандарт IEEE 802.11b, IEEE 802.11g создан для работы в условиях использования диапазона 2,4 ГГц. Стандарт предписывает обязательные и опциональные скорости передачи данных:

- обязательные — 1, 2, 5,5, 6, 11, 12 и 24 Мбит/с;
- опциональные — 33, 36, 48 и 54 Мбит/с.

Для достижения таких показателей используют кодирование с помощью последовательности дополнительных кодов (CCK), метод ортогонального частотного мультиплексирования (OFDM), метод гибридного кодирования (CCK-OFDM) и метод двоичного пакетного сверточного кодирования (PBCC). Следует отметить, что одна и та же скорость передачи может быть достигнута разными методами, но при этом обязательные скорости передачи данных достигаются только с помощью методов CCK и OFDM, а опциональные скорости — с помощью методов CCK-OFDM и PBCC.

Преимуществом оборудования стандарта IEEE 802.11g является его совместимость с оборудованием IEEE 802.11b, то есть вы сможете легко использовать

свой компьютер с сетевой картой стандарта IEEE 802.11 с точкой доступа стандарта IEEE 802.11g, и наоборот. Кроме того, потребляемая мощность оборудования этого стандарта намного ниже, чем аналогичное оборудование стандарта IEEE 802.11a.

Как и в случае со стандартом IEEE 802.11b+, существует аналогичный стандарт IEEE 802.11g+, который позволяет работать со скоростью 108 Мбит/с.

Стандарт IEEE 802.11h

Стандарт IEEE 802.11h разработан с целью эффективного управления мощностью излучения передатчика, выбора несущей частоты передачи и генерации нужных отчетов. Он вносит некоторые новые алгоритмы в MAC-уровень, а также физический уровень стандарта IEEE 802.11a. В первую очередь это связано с тем, что в некоторых странах диапазон 5 ГГц используют для трансляции спутникового телевидения, радарного слежения за объектами и т. п., что может вносить помехи в работу передатчиков беспроводной сети.

Смысл работы алгоритмов стандарта IEEE 802.11h заключается в том, что компьютеры беспроводной сети (или передатчики) при обнаружении отраженных сигналов (интерференции сигнала) могут динамически переходить на другой диапазон, понижать или повышать мощность передатчиков. Это позволяет эффективнее организовать работу уличных и офисных радиосетей.

Стандарт IEEE 802.11i

Стандарт IEEE 802.11i создан специально для повышения безопасности при работе беспроводной сети. С этой целью разработаны разные алгоритмы шифрования и аутентификации, функции защиты при обмене информацией, функции генерирования ключей и т. д., в частности:

- AES (Advanced Encryption Standard) — алгоритм шифрования, который позволяет работать с ключами шифрования длиной 128, 192 и 256 бит;
- RADIUS (Remote Access Dial-In User Service) — система аутентификации с возможностью генерирования ключей для каждой сессии и управления ими, включающая в себя алгоритмы проверки подлинности пакетов и т. д.;
- TKIP (Temporal Key Integrity Protocol) — алгоритм шифрования данных;

- WRAP (Wireless Robust Authenticated Protocol) — алгоритм шифрования данных;
- CCMP (Counter with Cipher Block Chaining Message Authentication Code Protocol) — алгоритм шифрования данных.

Стандарт IEEE 802.11j

Стандарт IEEE 802.11j разработан специально для условий использования беспроводных сетей в Японии, а именно для использования дополнительного диапазона радиочастот 4,9–5 ГГц[1]. Спецификация расширяет стандарт 802.11a добавочным каналом 4,9 ГГц.

ПРИМЕЧАНИЕ

На данный момент частота 4,9 ГГц рассматривается как дополнительный диапазон для использования в США. Из официальных источников известно, что этот диапазон готовится для применения органами общественной и национальной безопасности.

Данный стандарт расширяет диапазон работы устройств стандарта IEEE 802.11a.

Стандарт IEEE 802.11n

На сегодняшний день IEEE 802.11n — самый перспективный из всех стандартов, касающихся беспроводных сетей. К сожалению, он пока только разрабатывается, но перспективы, которые он предлагает, выглядят очень неплохо.

В перспективе стандарт должен обеспечить скорость передачи данных минимум в 100 Мбит/с, что фактически совпадает с наиболее распространенной скоростью в проводных сетях стандарта Ethernet 802.3.

Стандарт в своей работе будет использовать метод ортогонального частотного мультиплексирования (OFDM) и квадратурную амплитудную модуляцию (QAM), что, по идее, должно не только обеспечить высокую скорость передачи данных, но и полную совместимость со стандартами IEEE 802.11a, IEEE 802.11i IEEE 802.11g.

---

[1] Буква j в названии стандарта не означает, что он «японский». Она отображает алфавитную очередность стандартов.

Для увеличения скорости передачи данных планируется использовать несколько новых технологий, одной из которых является технология с множественным вводом/выводом (Multiple Input Multiple Output, MIMO). Смысл ее заключается в параллельной передаче данных по разным каналам с применением нескольких передающих антенн. Также подразумевается расширение канала до 40 МГц.

Стандарт IEEE 802.11r

Поскольку ни в каком из беспроводных стандартов толком не описаны правила роуминга, то есть перехода клиента от одной зоны к другой, то это призван сделать стандарт IEEE 802.11r.

9.4. Преимущества и недостатки беспроводной сети

В любом деле есть свои преимущества и недостатки, однозначно определяющие выбор той или иной технологии в конкретных условиях. Не обошла эта участь и беспроводные сети.

Основные преимущества беспроводной сети.

- Легкость создания и реструктуризации сети. Это один из основных плюсов беспроводной сети, поскольку позволяет приложить минимум усилий, а самое главное, минимум затрат для создания работоспособной и достаточно быстрой сети. Дело даже не в том, что проводную сеть иногда лень делать (бывает и такое), а в том, что, имея одну или более точку доступа, можно соединить в единую локальную сеть отдельно стоящие здания или находящиеся на большом расстоянии друг от друга компьютеры.

  Кроме того, беспроводную сеть можно создать тогда, когда делать проводную сеть накладно: для разных конференций, выставок, выездных семинаров и т. п. — быстро, красиво (без множества проводов) и эффективно. Не следует также забывать и о зданиях, прокладка кабельной системы в которых нарушает их историческую ценность.

  Что касается реструктуризации, то здесь дело обстоит совсем просто: добавляешь новый компьютер — и готово. Не возникает проблем ни при подключении типа Ad-Hoc, ни при создании точки доступа.

- Мобильность. Лучшие из технологий, которые есть в нашем мире, остаются таковыми только тогда, когда являются универсальными. На сегодняшний день основным показателем универсальности является мобильность, которая позволяет человеку заниматься своим делом, где бы он ни находился, в любых условиях. Мобильные телефоны, персональные ассистенты, коммуникаторы, переносные компьютеры — вот представители современных технологий.

  С появлением беспроводных сетей и соответствующих компьютерных технологий мобильность приобрела более широкое значение и позволяет соединить между собой любые способные на связь устройства, которыми так богата наша жизнь. Имея такое приспособление, вы можете спокойно передвигаться по своему городу и быть уверенным, что всегда останетесь на связи и сможете получить самую последнюю информацию.

- Подключение к другому типу сети. Беспроводную сеть всегда можно подключить к проводной. Делается это очень просто — используют совместимый порт[1] на точке доступа или радиомосте. При этом вы получаете доступ к ресурсам сети без всяких ограничений.

  Именно этот момент актуален, когда к общей сети нужно присоединить удаленные здания и точки, к которым проложить проводную сеть невозможно или слишком дорого.

- Высокая скорость доступа в Интернет. Немаловажным фактом является то, что, имея точку доступа с подключением к Интернету, вы сможете дать доступ к нему всем, кто находится в сети. При этом скорость будет намного выше той, которую могут предоставить обычные и даже xDSL-модемы.
  Это достаточно серьезная альтернатива такому дорогому решению, как оптоволоконный канал, прокладку которого не могут позволить себе даже многие крупные компании, чего не скажешь о приобретении точки доступа или радиокарты, которую может купить себе даже домашний пользователь. Дальше дело только за финансами, которые вы готовы выложить за предоставленный канал. Канал в 2–10 Мбит/с и более уже давно не считается большой роскошью в Европе, США или Канаде. Такое же настроение постепенно устанавливается и в странах СНГ.

---

[1] Как правило, на любой точке доступа имеется порт с разъемом RJ-45, что позволяет подключиться к сетям с таким распространенным стандартом, как 100Base-TX или 1000Base-TX.

К сожалению, беспроводная сеть обладает также и некоторыми недостатками.

- Низкая скорость передачи данных. Дело в том, что реальная скорость передачи данных заметно отличается от теоретической и зависит от количества преград на пути сигнала, числа подключенных к сети компьютеров, особенностей построения пакетов данных (большой объем служебных данных), удаленности машин и т. д.
  Например, рассмотрим стандарт IEEE 802.11g. В табл. 9.1 можно увидеть данные о радиусе сети при разных условиях использования.

Таблица 9.1. Радиус сети стандарта IEEE 802.11g при разных условиях использования

Условия использования	Радиус сети, м
Открытая местность, зона прямой видимости	до 300
Открытая местность с препятствиями	до 100
Большой офис	до 40
Жилой дом	до 20

В табл. 9.2 представлено соотношение скорости передачи данных и расстояния, на котором она действует.

Таблица 9.2. Соотношение скорости передачи данных и дальности действия для сети стандарта IEEE 802.11g

Скорость передачи данных, Мбит/с	Радиус сети, м
1	до 100
11	до 40
54	до 14

- Уязвимость сети. Безопасность сети — проводной или беспроводной — всегда ставилась превыше всего. Особенно важным вопросом это было для организаций, которые работают с деньгами или другими материальными ценностями. Что касается беспроводной сети, то она немного страдает от нормальных механизмов аутентификации и шифрования. Это доказал первый из протоколов шифрования — WEP, который кодировал данные с помощью ключа длиной 40 бит. Оказывается, чтобы вычислить этот самый ключ, достаточно в течение двух-трех часов анализировать перехваченные пакеты. Конечно, неопытному пользователю такое сделать сложно, но специалисту — очень даже под силу.
  Правда, не все так плохо, как кажется. Со временем появились другие алгоритмы шифрования, более умные и запутанные, использующие для кодирования

данных ключи длиной до 256 бит. Однако здесь возникает ситуация, когда необходимо выбирать между безопасностью и скоростью, поскольку увеличение длины ключа приводит к увеличению служебного заголовка, что заметно снижает скорость передачи данных.

- Высокий уровень расхода энергии. Это касается только пользователей переносных компьютеров и других мобильных устройств. Как известно, энергия их аккумуляторов небезгранична и любое дополнительно подключенное оборудование приводит к быстрому истощению. Конечно, существуют механизмы, позволяющие сводить потребление энергии к минимуму, но в любом случае аккумуляторы разряжаются достаточно быстро. Кроме того при этом уменьшается пропускная способность подключения к сети.
- Несовместимость оборудования. Вопросы совместимости устройств всегда интересовали пользователей.

  Обычно производители практикуют следующий подход: оборудование, разработанное раньше, способно работать с выпущенным позже. Это называется обратной совместимостью. С оборудованием для беспроводных сетей дела обстоят сложнее.

  На данный момент активно используют беспроводное оборудование стандартов IEEE 802.11a, IEEE 802.11b и IEEE 802.11g. Кроме того, в последнее время встречается оборудование с дополнительными стандартами типа IEEE 802.11b+ и IEEE 802.11g+, работающими в турборежимах и обеспечивающими удвоенную максимальную скорость передачи данных в сравнении с аналогичным оборудованием родных стандартов.

  Ситуация сложилась таким образом, что совместимости между устройствами практически не существует. Единственное, что облегчает жизнь, — это то что устройства стандарта IEEE 802.11g (и IEEE 802.11g+) имеют обратную совместимость с устройствами стандарта IEEE 802.11b (и IEEE 802.11b+) Найти же оборудование, поддерживающее все стандарты, практически нереально.

Глава 10

Вопросы безопасности сети

- Протокол безопасности WEP
- Протокол безопасности WPA
- Идентификатор точки доступа и MAC-фильтрация

Почему защищенность сети играет огромную роль? Ответ на этот вопрос прост: предприятие, на котором работает сеть, может в своей деятельности использовать и хранить секретные документы и данные. Кроме того, вряд ли кому-то понравится, если его личные документы сможет смотреть любой другой человек. Поэтому вполне логична необходимость средств безопасности, которые могут защитить данные в сети и саму сеть от вторжения извне.

Доступ к проводной сети можно получить, лишь имея физическое, то есть проводное, подключение к ней, а контролировать подключение достаточно просто.

Беспроводные сети в своей работе используют радиоволны, которые распространяются согласно определенным физическим законам и зависят от специфики передающих антенн в зоне радиуса сети. Контролировать использование радиоволны практически невозможно. Это означает, что любой, у кого есть компьютер или переносное устройство с радиоадаптером, может подключиться к сети, находясь в радиусе ее действия. Вычислить местоположение этого пользователя практически невозможно, поскольку он может быть как рядом, так и на значительном расстоянии и использовать антенну с усилителем.

Именно тот факт, что подключиться к беспроводной сети может любой, требует от ее организации серьезного уровня безопасности, который реализуется существующими стандартами.

Описанные ниже механизмы способны обеспечить некоторую безопасность в беспроводной сети.

- Механизм аутентификации рабочей станции, с помощью которого можно определить, кто подключается к беспроводной сети и имеет ли он право на это.
- Механизм защиты информации посредством ее шифрования с помощью специальных алгоритмов.

Если один из этих механизмов не используется, то можно сказать, что сеть является абсолютно незащищенной. Как минимум злоумышленник будет увеличивать трафик (Интернет, файловые ресурсы), как максимум — сможет навредить другой подключенной к вам сети.

На сегодняшний день стандартами предусмотрено несколько механизмов безопасности, позволяющих в той или иной мере защитить беспроводную

сеть. Обычно такой механизм содержит в себе как средства аутентификации, так и средства шифрования, хотя бывают и исключения.

Однако проблема защиты сети была и остается, поскольку, каким бы строгим ни был стандарт безопасности, это не означает, что все оборудование его поддерживает. Часто даже получается так, что, например, точка доступа поддерживает последние алгоритмы безопасности, а сетевая карта одного из компьютеров — нет. В результате сеть работает с тем стандартом, который поддерживают все ее компьютеры.

10.1. Протокол безопасности WEP

Протокол безопасности WEP (Wired Equivalent Privacy) — первый протокол безопасности, описанный стандартом IEEE 802.11. Для шифрования данных он использует ключ с разрядностью 40–104 бит. Кроме того, дополнительно применяется шифрование, основанное на алгоритме RC4, называемое алгоритмом обеспечения целостности данных.

Что касается обеспечения целостности данных, то его можно с натяжкой назвать шифрованием, поскольку для этого процесса используется статическая последовательность длиной 32 бита, присоединяющаяся к каждому пакету данных, увеличивая при этом служебную часть, которая и так слишком большая.

Необходимо отдельно упомянуть о процессе аутентификации, поскольку без него защиту передаваемой информации нельзя считать достаточной. Изначально стандартом IEEE 802.11 описаны два варианта аутентификации: для систем с открытым и с общим ключом.

Аутентификация с открытым ключом

Фактически этот метод аутентификации не предусматривает вообще никаких средств безопасности соединения и передачи данных. Выглядит это следующим образом. Когда двум компьютерам нужно установить связь, отправитель посылает получателю специально сформированный пакет данных, называемый кадром аутентификации. В свою очередь, получатель, приняв такой пакет, понимает, что требуется аутентификация с открытыми ключами, и отправляет аналогичный кадр аутентификации. На самом деле эти кадры,

естественно, отличаются друг от друга и, по сути, содержат только информацию об отправителе и получателе информации.

Аутентификация с общим ключом

Данный уровень аутентификации подразумевает использование общего ключа секретности, которым владеют только отправитель и получатель информации. В этом случае процесс выглядит следующим образом.

Чтобы начать передачу данных, отправителю необходимо договориться с получателем. Для этого он отсылает получателю кадр аутентификации, содержащий информацию об отправителе и тип ключа шифрования. Приняв его, получатель в ответ отсылает пробный текст, зашифрованный с помощью указанного типа ключа, в качестве которого используется 128-битный ключ алгоритма шифрования WEP. Получив пробный зашифрованный текст, отправитель пытается его расшифровать с помощью обговоренного ключа шифрования. Если результат расшифровки совпадает с текстом (используется контрольная сумма зашифрованного и расшифрованного сообщения), отправитель посылает получателю сообщение об успехе аутентификации. Только после этого передаются данные с использованием указанного ключа шифрования.

Вроде бы все выглядит достаточно просто и эффективно. На самом же деле практическое использование метода шифрования WEP показало, что алгоритм шифрования имеет явные прорехи безопасности, которые нельзя скрыть даже с помощью длинного ключа шифрования. Оказывается, опять же благодаря сторонним тестировщикам и хакерам, что, проанализировав достаточно большой объем трафика сети (3–7 млн пакетов), можно вычислить ключ шифрования. Не спасает даже 104-битный ключ. Благо компьютерные технологии и стандарты непрерывно развиваются и совершенствуются.

Конечно, это совсем не означает, что протокол безопасности WEP не годится совсем. Для небольших беспроводных сетей (несколько компьютеров) его защиты вполне достаточно, поскольку трафик такой сети сравнительно невелик и для его анализа и взлома ключа шифрования нужно потратить значительно больше времени.

Что же касается больших развернутых беспроводных сетей, то использование протокола WEP небезопасно и крайне не рекомендуется. Ко всему прочему, в Интернете можно найти множество специализированных утилит, которые

позволяют взломать защиту WEP-протокола и предоставить доступ к беспроводной сети. Именно поэтому для обеспечения нужного уровня безопасности лучше использовать более современные протоколы шифрования, в частности протокол безопасности WPA.

Конечно, можно использовать ключи шифрования максимальной длины, но не следует забывать о том, что это чревато уменьшением скорости передачи данных за счет увеличения избыточности передаваемой информации.

Другим выходом из описанной ситуации можно считать использование направленных антенн передачи сигнала. В некоторых условиях это хороший метод, но в домашних беспроводных сетях он неприменим практически.

10.2. Протокол безопасности WPA

Протокол безопасности WPA пришел на смену WEP в силу понятных причин, главной из которых является практическая незащищенность последнего. Именно эта незащищенность сдерживала развитие и распространение беспроводных сетей. Однако с появлением протокола WPA все стало на свои места.

WPA (Wi-Fi Protected Access) был стандартизирован в 2003 году и сразу оказался востребованным. Главным его отличием от протокола WEP можно считать наличие динамической генерации ключей шифрования, что позволило кодировать каждый отправляемый пакет собственным ключом. Кроме этого, каждое сетевое устройство в сети снабжается дополнительным ключом, который меняется через определенный промежуток времени.

Для аутентификации применяют протокол EAP (Extensible Authentication Protocol) через службу (сервер) дистанционной аутентификации RADIUS (Remote Authentication Dial-In User Service) или предварительно согласованный общий ключ. При этом аутентификация подразумевает вход пользователя с помощью логина и пароля, которые проверяются на сервере аутентификации RADIUS.

Для шифрования данных протокол использует модернизированный алгоритм шифрования RC4, основанный на протоколе краткосрочной целостности ключей TKIP (Temporal Key Integrity Protocol). Это позволяет не только повысить уровень защищенности данных, но и сохранить обратную совместимость с WEP.

Шифрование базируется на использовании случайного вектора инициализации IV (Initialization Vector) и WEP-ключа, которые складываются и в дальнейшем используются для шифрования пакетов. Результатом такого сложения может быть огромное количество разных ключей, что позволяет добиться практически стопроцентной защиты данных.

Также протокол безопасности WPA поддерживает усовершенствованный стандарт шифрования AES (Advanced Encryption Standard), который использует еще более защищенный алгоритм шифрования, намного эффективнее алгоритма RC4. Однако за это приходится платить повышенным трафиком сети и, соответственно, уменьшением ее пропускной способности.

На сегодняшний день активно используется версия протокола WPA2, которая предоставляет больше возможностей защиты среды.

ПРИМЕЧАНИЕ

Для использования протокола безопасности WPA необходимо, чтобы все устройства, подключенные к сети, имели его поддержку. В противном случае будет использован стандартный протокол безопасности WPE.

10.3. Идентификатор точки доступа и MAC-фильтрация

Каков бы ни был уровень безопасности, его будет всегда недостаточно. Однако это совсем не означает, что он должен быть настолько высок, насколько это возможно. Всегда должен быть достигнут компромисс, особенно если учесть тот факт, что каждый дополнительный алгоритм защиты съедает часть пропускной способности сети, что снижает скорость передачи данных.

Минимальным уровнем безопасности можно считать использование идентификатора точки доступа и MAC-фильтрации адресов устройств.

Идентификатор точки доступа

Любая точка доступа, которая участвует в работе беспроводной сети, имеет так называемый идентификатор точки доступа ESSID (Extended Service Set ID), который представляет собой 8-битный код. Если в сети несколько точек доступа, то в целях безопасности всем им присваивается одинаковый идентификатор.

Фактически ESSID — это название вашей беспроводной сети, которое вы можете менять на любое, применяя как буквы, так и числа. Поменять это название можно в любой момент, не забывая при этом сообщить ESSID каждой подключенной машине. Компьютер, который не будет знать ESSID, не сможет подключиться к вашей сети.

Чтобы еще больше усложнить задачу взломщикам, можно настроить точку доступа таким образом, чтобы она не транслировала ESSID в эфир.

MAC-ФИЛЬТРАЦИЯ

Фильтрацию по MAC-адресу можно считать природным способом защиты беспроводной сети. Дело в том, что MAC-адрес (Media Access Control) — идентификатор, который имеется у любого сетевого оборудования. Его применяют с момента появления первых сетевых устройств, и изменить его невозможно. Именно поэтому, используя фильтр по MAC-адресам в точке доступа, вы можете отсеивать непрошеных гостей, тем самым дополнительно защищая свою беспроводную сеть. Однако помните, существует программное обеспечение, которое позволяет подставлять чужой MAC-адрес и входить в сеть, используя чужие права.

Глава 11

Создание сети

- Правовые вопросы
- Условия использования режима Ad-Hoc
- Условия использования режима инфраструктуры

Беспроводная сеть — один из способов организации локальной сети, когда использование кабельной системы нежелательно или затруднено. Она наиболее удобна в создании. При организации сети не нужно рисковать, лазая по крышам, и делать отверстия в стенах, оконных рамах и т. п. Пользователи с радостью приветствуют такой подход, так как им не приходится загромождать свое рабочее пространство дополнительными проводами.

Именно поэтому создание беспроводной сети заключается не в ее монтаже, а в ее настройке на уровне драйверов и программных утилит. Более подробно о подключении устройств и настройке операционной системы читайте в пятой части книги. Тем не менее есть некоторые вопросы, которые нужно исследовать, прежде чем начать построение сети.

Первым делом необходимо точно представлять себе, что требуется для построения сети. Как известно, стандартами описаны только два варианта — инфраструктурный режим и режим Ad-Hoc («точка-точка»). Хотя они и похожи друг на друга, все-таки существуют определенные отличия, которые необходимо учитывать при планировании сети.

Кроме того, имейте в виду, что беспроводные сети являются контролируемым объектом со стороны государственных служб. А это означает, что необходимо знать правила ее использования и быть готовым к тому, что придется оформлять сеть по закону.

11.1. Правовые вопросы

Как уже упоминалось выше, государство контролирует использование радиоэфира. По-другому и быть не может, поскольку он применяется не только для связи локальных сетей, но и для передачи другой важной информации. В частности, эфир используется в военных целях, для средств общения с воздушным транспортом, для организации общения радиослужб и т. д. В связи с этим должны существовать правила, описывающие использование радиоэфира.

Таким образом, существует специальная государственная комиссия по радиочастотам (ГКРЧ), которая контролирует использование радиоэфира. Именно эта комиссия является автором некоторых положений и инструкций, которые должны соблюдаться организациями, использующими радиоэфир в своих целях.

Чтобы не углубляться в правовые дебри, можно сказать следующее. Если вы планируете использовать беспроводную сеть вне офиса, вам придется получить на это лицензию. На внутриофисные сети лицензия не требуется за исключением тех случаев, когда работа сети может мешать работе любой радиослужбы, находящейся в зоне действия вашей сети.

Если вы планируете организовать масштабную беспроводную сеть, обязательно проконсультируйтесь по этому вопросу в соответствующих органах.

11.2. Условия использования режима Ad-Hoc

Беспроводные сети Ad-Hoc самые простые по построению из двух существующих вариантов. Очень часто этот режим используют, когда необходимо быстро соединить небольшое количество (2–5) рядом расположенных компьютеров с намерением создать мобильную и быстро модернизируемую сеть. Кроме того, этот вариант незаменим, когда необходимо быстро и с минимальными усилиями передать данные между двумя компьютерами.

Главными недостатками такого варианта построения сети являются ее малый радиус действия и низкая помехозащищенность, что накладывает свои ограничения на расположение компьютеров.

Итак, какие условия при построении беспроводной сети в режиме Ad-Hoc должны выполняться и какие устройства и материалы нужны для ее построения?

Прямая видимость между подключаемыми компьютерами

При подключении в режиме Ad-Hoc очень важным фактором, влияющим на скорость работы беспроводной сети, является прямая видимость между подключаемыми компьютерами. Это связано с тем, что мощность передатчиков беспроводных адаптеров несколько ниже, чем, например, у точек доступа. Отсюда следует, что радиус действия сети сокращается примерно вдвое, по сравнению с радиусом сети, построенной с применением инфраструктурного режима, то есть при наличии точки (точек) доступа.

Для увеличения радиуса действия сети практически единственным выходом является применение более мощных антенн. Но для этого нужно, чтобы все адаптеры поддерживали сменные антенны.

В случаях, если между компьютерами существуют преграды, например стены офиса, радиус сети резко сокращается, а скорость может снижаться до минимума.

Стандарт беспроводных адаптеров

Как известно, от стандарта, в котором работают сетевые адаптеры, зависит скорость передачи данных в сети. Мало того, если на одном из компьютеров будет установлено устройство другого стандарта, который имеет более низкую скорость передачи данных, то и скорость работы сети в целом будет равняться скорости этого адаптера. Поэтому использование адаптеров единого стандарта является неплохой стратегией.

Если условия использования адаптеров с одинаковым беспроводным стандартом работы трудновыполнимы, тогда желательно не применять адаптеры со скоростью передачи данных менее 11 Мбит/с (стандарт IEEE 802.11b). Наиболее эффективным в этом случае будет использование адаптеров стандартов IEEE 802.11b+ и IEEE 802.11g, что позволит достичь теоретической скорости передачи данных 22 Мбит/с.

Беспроводные адаптеры

Для построения беспроводной сети в режиме Ad-Hoc можно использовать любые имеющиеся в продаже беспроводные адаптеры. Это могут быть USB-, PCI-, PC Card-адаптеры и др. Все зависит от того, какие компьютеры будут объединяться в сеть и какой из способов подключения беспроводного адаптера им более всего подходит или выгоден.

Однако если вы хотите, чтобы сеть работала максимально быстро и устойчиво, используйте адаптеры от одного производителя, например D-Link, 3COM и др. Кроме всего прочего, это позволит использовать некоторые фирменные возможности, которые зачастую имеются в адаптерах, например повышенную скорость передачи данных (108, 125 Мбит/с). Поэтому, прежде чем покупать оборудование, обязательно почитайте о нем отзывы и узнайте его технические характеристики, например, на веб-сайте производителя. Кроме того, очень полезно иногда бывает ознакомиться с отчетами о тестированиях выбранных вами устройств, которые часто проводят разного рода лаборатории.

Количество подключенных компьютеров

Количество подключенных к сети компьютеров всегда играло большую роль независимо от типа сети — проводная она или беспроводная. И связано это в первую очередь с особенностями обмена информацией между машинами. Особенно важным фактором это является для беспроводных сетей с использованием режима Ad-Hoc.

Когда один пользователь хочет передать другому файл, обмен данными с остальными компьютерами очень сильно тормозится, что приводит к задержкам. Теперь представьте себе, что несколько пользователей одновременно хотят обменяться файлами или скачать данные с одного компьютера. В этом случае пропускная способность сети падает практически до нуля.

Поэтому при планировании будущей сети имейте в виду, что для беспроблемной работы сети в режиме Ad-Hoc количество подключений не должно выходить за рамки 2–5 машин. Если количество подключаемых компьютеров превышает разумное число, более выгодным решением в этой ситуации будет использование точки доступа и режима инфраструктуры.

11.3. Условия использования режима инфраструктуры

Режим инфраструктуры подходит в тех случаях, когда к сети необходимо подключить достаточно большое количество пользователей. Кроме того, именно этот режим используется в случаях, когда требуется соединить две сети в одну или точка доступа подключается к маршрутизатору.

При использовании точки доступа количество подключенных компьютеров может доходить до 253. Конечно, совсем не обязательно доводить сеть до такого состояния, поскольку это приведет к полному ее упадку.

Итак, рассмотрим, что необходимо для создания сети в режиме инфраструктуры и какие условия должны при этом выполняться.

Условия использования и расположение точки доступа

Точка доступа — самое главное устройство в беспроводной сети, и от ее расположения зависит очень многое. Не следует забывать о том, что точка доступа

является связующим звеном между компьютерами, которые зачастую располагаются в самых невероятных местах.

Рассмотрим все по порядку.

Расположение точки доступа. Имея более мощный передатчик, нежели беспроводной адаптер, точка доступа позволяет осуществлять связь на более длинных дистанциях и с большей силой. Однако это совсем не означает, что ей по зубам любые препятствия в виде стен, потолков, деревьев, домов и т. д., любое из них создает помехи распространению радиоволн и снижает радиус действия сети в несколько раз.

При размещении точки доступа учитывайте все препятствия, которые могут стоять между точкой доступа и подключенными к ней компьютерами.

Если точка доступа используется внутри офиса или дома, постарайтесь поместить ее приблизительно посередине между компьютерами и с таким расчетом, чтобы достигалось по возможности максимальное количество компьютеров в прямой видимости. Это позволит им работать в сети с максимальной скоростью и минимальными помехами.

Если точка доступа используется вне помещения, то ее расположение должно обеспечивать прямую видимость с наиболее удаленными объектами сети.

Защита от погодных явлений. Погодные явления являются критичным фактором в тех случаях, когда антенна или сама точка доступа находятся на открытом воздухе, что делает ее особо уязвимой. В этом случае точка доступа обязательно должна быть оборудована механизмом защиты, спасающим ее «внутренности» от выхода из строя в момент грозы, когда в воздухе накапливается множество статической энергии, способной попасть через антенну внутрь устройства и повредить электронные схемы.

Именно поэтому в период планирования сети позаботьтесь о том, чтобы все наружные точки доступа или те из них, антенны которых находятся вне здания, обладали таким защитным механизмом.

Защита от статического электричества. Любое электронное устройство, питаемое от сети переменного напряжения, должно быть заземлено. Это правило достаточно серьезное, и оно должно выполняться любыми способами. Если же проигнорировать это требование, то устройство может повредиться или полностью выйти из строя.

Точка доступа

Точка доступа обязательна, если вы собираетесь использовать инфраструктурный режим сети. Поэтому отнеситесь внимательно к ее выбору.

Использовать точку доступа можно любую, благо их моделей существует достаточно много. Каждая из точек доступа способна организовать работу беспроводной сети. Однако не все способны делать это на высшем уровне.

Выбирая точку доступа, не скупитесь и приобретайте ту, которая имеет некоторые оригинальные функции или дополнительные возможности обеспечения безопасности. Советую отдать предпочтение тому устройству, у которого скорость передачи данных будет максимально возможной на текущее время. Не исключено, что вскоре появится новый стандарт, позволяющий передавать данный с намного большей скоростью, чем та, которой может обладать ваша «отсталая» точка доступа. Поэтому, выбирая устройство с максимальным быстродействием, вы будете идти в ногу со временем, обеспечивая при этом отличную пропускную способность вашей беспроводной сети.

При выборе точки доступа обязательно узнайте, какими дополнительными сетевыми функциями она обладает. Лучшим решением будет выбор устройства, которое может работать как маршрутизатор или мост. Рано или поздно это вам обязательно пригодится.

Кроме того, наличие нескольких Ethernet-портов у точки доступа обеспечит возможность подключения большего количества проводных пользователей к существующей беспроводной сети.

Мост

Мост — устройство, которое пригодится далеко не всем. Так, небольшой беспроводной сети, состоящей из десятка компьютеров, оно точно не нужно. Но для крупной сети, объединяющей различные топологии и технологии, мост — незаменимая вещь.

Главной задачей беспроводного моста является соединение сегментов проводной и беспроводной сетей в единую комбинированную сеть. Исходя из этого, при выборе модели моста ориентируйтесь на радиус его действия, поскольку расстояние между этими сегментами может быть достаточно большим. Обязательно проследите, чтобы мост максимально соответствовал возможным протоколам безопасности и шифрования данных.

Маршрутизатор

Маршрутизатор для небольшой беспроводной сети — достаточно бесполезное устройство, но для крупной офисной сети он крайне необходим.

Маршрутизатор, помимо маршрутизации пакетов между разными сегментами беспроводной сети, может использоваться для продления сети, предоставления общего доступа в Интернет и многого другого.

Поскольку на маршрутизатор ложится выполнение важной работы, то и возможностями он должен обладать неординарными, например, кроме последних версий протоколов безопасности, иметь встроенный Firewall, списки ограничений и выполнять другие полезные функции, которые могут пригодиться при работе с Интернетом.

Мощность передатчиков

Мощность передатчиков сетевых устройств играет большую роль и влияет на радиус действия сети. Однако существуют жесткие правила, регламентирующие эту самую мощность. Если использовать более мощные передатчики, это может вызвать сильные помехи у рядом находящихся радиоустройств, особенно тех, которые работают в том же диапазоне радиочастот, что и беспроводная сеть.

Если все-таки мощность передатчиков должна быть увеличена, об этом обязательно нужно известить органы контроля использования частот и оформить необходимые документы.

Беспроводные адаптеры

Беспроводные адаптеры, которые планируется использовать при подключении компьютеров, могут быть разных производителей и разных стандартов. Однако желательно все-таки применять оборудование одного стандарта и производителя, что позволит использовать всю функциональность и скорость сети по максимуму. Не забывайте, что при наличии хотя бы одного сетевого адаптера, например, стандарта IEEE 802.11b скорость сети ограничивается показателем 11 Мбит/с (или 22 Мбит/с), даже если сеть способна функционировать на скорости 108 или 125 Мбит/с.

Часть 4

Нестандартные сети

Глава 12

Сеть на основе телефонной проводки

Использование телефонной проводки в качестве физической среды для создания сетей практикуется уже достаточно давно, а если точнее, то примерно с середины 90-х годов. Подобный подход абсолютно оправдан: почему бы не использовать уже имеющуюся в здании телефонную проводку, если это возможно?

Инициатором такого способа передачи данных стала малоизвестная фирма Tut Systems, которая предложила способ передачи данных со скоростью 1 Мбит/с. На то время, конечно, существовали и более «продвинутые» варианты передачи данных, тем не менее этот понравился многим. Как результат, был сформирован альянс HomePNA (Home Phoneline Networking Alliance), который и взял в руки дальнейшую судьбу стандарта.

На сегодняшний день существуют два стандарта такой сети: HomePNA 1.0 и HomePNA 2.0. Главные отличия между ними — скорость и дальность передачи данных. Так, если стандарт HomePNA 1.0 подразумевает передачу данных на скорости до 1 Мбит/с на расстояние до 150 м, то HomePNA 2.0 достигает скорости 10 Мбит/с и действует на расстоянии 350 м. При этом может обслуживаться до 32 рабочих мест.

Также известно, что идет работа над стандартом HomePNA 3.0, который обеспечивает скорость передачи данных до 128 Мбит/с. Хотя он еще не принят, в продаже уже можно найти подобного рода устройства.

Чем же выгодна такая сеть? Вот только несколько причин, почему вы можете ее использовать:

- возможность применения телефонной проводки любой топологии;
- высокая степень защиты от шумов разной интенсивности;
- использование линий с разными характеристиками, которые могут динамически изменяться со временем или при определенных условиях;
- параллельная работа с установленными в линии устройствами, такими как модемы, факсы и т. д.;
- расширяемость сети;
- в качестве носителя можно использовать не только телефонный провод, но и любой другой, например коаксиал; мало того, можно использовать даже скрутки из неоднородных материалов, чем достигается повышение скорости сети до 15–20 Мбит/с.

Конечно, по многим причинам сеть стандарта HomePNA не может служить полноценной локальной сетью с многими рабочими местами. Дело в том, что теоретические показатели сети всегда гораздо выше реальных. Однако с помощью адаптеров HomePNA вы спокойно можете создать сеть из нескольких компьютеров в одной или двух комнатах. Кроме того, плюсом HomePNA является то, что она может легко входить в состав проводной или даже беспроводной сети или наоборот — служить удлиняющим мостом между существующими проводными или беспроводными сегментами сети.

Для создания сети вам потребуется лишь адаптер HomePNA (рис. 12.1) и кусок кабеля с обжатыми коннекторами RJ-11 (телефонный разъем).

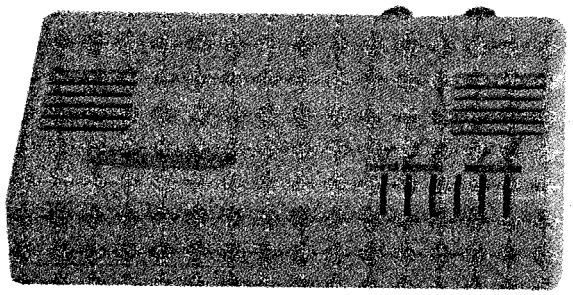


Рис. 12.1. Внешний вид HomePNA-адаптера

Настройка сети производится аналогично проводной сети, поскольку в сетях HomePNA используется тот же алгоритм передачи данных.

Глава 13

Сеть на основе электрической проводки

Вряд ли вы найдете здание, в котором бы не была проложена электропроводка. И уж тем более она проложена в доме, в котором живете вы. Как и в случае с сетями стандарта HomePNA, лет десять назад началась разработка стандартов, которые позволяют использовать в качестве физической среды передачи данных обычную электропроводку.

Подобное рвение оправданно, поскольку позволяет проложить сеть там, где невозможно использовать другие варианты. Примерами таких мест могут быть подвалы, бункеры и т. п. Кроме того, подобную сеть спокойно можно использовать и в офисе или дома, когда необходимо подключить небольшое количество компьютеров. Однако обо всем поподробнее.

Примерно в 2000 году был создан альянс HomePlug Powerline Alliance, в который вошли крупнейшие компании, связанные с сетями, такие как AMD, 3COM, Cisco Systems, Hewlett-Packard, Intel, Motorola и др. Целью альянса стала разработка стандарта с устойчивыми параметрами передачи данных с учетом всех особенностей электрической проводки.

Результатом работы альянса стало появление стандарта HomePlug 1.0, который позволяет достичь теоретической скорости передачи данных 10 Мбит/с на расстоянии до 300 м. Однако 300 м — это совсем не предел. Так, возможны несколько вариантов обмена информацией с использованием определенных сетевых адаптеров.

- **Низкоскоростной обмен.** В этом случае длина сети может исчисляться десятками километров, однако скорость очень низкая, может составлять десятки бит и использоваться для передачи служебных данных малого объема.
- **Среднескоростной обмен.** Этот вариант подразумевает длину сети в несколько километров со скоростью передачи данных до 50 Кбит/с. При этом используется полоса частот 50–533 Гц. Такой скорости уже вполне хватает, если необходимо производить удаленное управление устройствами.
- **Высокоскоростной обмен.** Наиболее приемлемый режим, используемый для организации офисных и домашних сетей. Длина сети может составлять 300 и более метров, при этом скорость передачи данных наиболее высокая. Для ее достижения используется диапазон частот 1,7–30 Мгц и метод мультиплексирования с ортогональным разделением частот OFDM, который также используется для работы и в беспроводных сетях.

Кстати, существует усовершенствованный стандарт с названием HomePlug Turbo. Главное его отличие от HomePlug 1.0 – скорость передачи данных, которая теоретически составляет 85 Мбит/с. Это означает, что вы можете подключить большее количество устройств и получить приемлемую скорость работы сети.

Из недостатков сети можно отметить сильную зависимость от шумов в проводке и ощутимое затухание сигнала при увеличении длины сети. Кроме того, крайне нежелательно подключать адаптеры к разного рода фильтрам и выпрямителям.

Для подключения компьютера к сети используется специальный Powerline-адаптер (различные его модификации). Наибольшее распространение получили PCI-устройства и Ethernet-конвертеры, которые подключаются к установленному в компьютере сетевому адаптеру с разъемом RJ-45 (рис. 13.1).

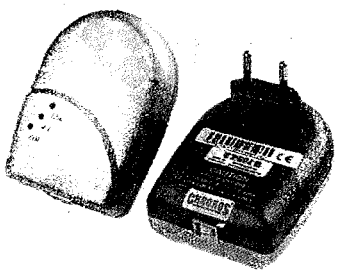


Рис. 13.1. Внешний вид Powerline-адаптера

Что касается безопасности сети, то для шифрования данных используется стандарт DES (Data Encryption Standard), который подразумевает применение 56-битного ключа шифрования. Как и в Ethernet-сетях стандартов IEEE 802.3 и IEEE 802.11, здесь используется MAC-адрес для идентификации устройства. Аналогично с беспроводными сетями имеется идентификатор сети Private Network Name.

Настройка параметров сети осуществляется стандартным способом и не вызывает Private Network Name. По умолчанию все подобного рода адаптеры имеют одинаковый идентификатор сети. Поэтому обязательно позаботьтесь о его смене, если не хотите увидеть в своей сети незваных гостей, которые территориально могут находиться в другом здании или даже в другом конце квартала.

Глава 14

Сеть из двух компьютеров

- Нуль-модемное соединение
- Соединение с помощью коаксиального кабеля
- Соединение с помощью кабеля на основе витой пары
- Соединение с помощью USB-кабеля
- Соединение через FireWire-порт
- Соединение через Bluetooth

Из одного компьютера сеть не организуешь. Чтобы создать сеть, нужны как минимум две машины. Такие мини-сети встречаются достаточно часто, особенно в домашних условиях.

В этой главе рассматриваются разные варианты соединения компьютеров. Каждый из них имеет свои недостатки и преимущества, поэтому вопрос определения оптимального по показателям цена/качество/скорость варианта ложится на самого пользователя исходя из конкретной ситуации.

Цель построения компьютерной сети одна — организовать обмен информацией. Сделать это можно разными способами, от чего во многом зависит функциональность сети.

14.1. Нуль-модемное соединение

Данное соединение подразумевает использование специального нуль-модемного кабеля, подключенного к коммуникационным портам (LPT или COM) на компьютерах, которые нужно соединить.

Скорость такого соединения нельзя назвать достаточной, поскольку она ограничена скоростью коммуникационного порта, которая, например, в случае использования COM-порта составляет всего 115 Кбит/с.

Чем привлекательно соединение компьютеров с помощью нуль-модемного кабеля? Для его осуществления не нужны сетевые карты. Однако это единственное преимущество.

Существенным недостатком является очень низкая скорость передачи данных, которая не позволяет обмениваться файлами больших размеров, например фильмами или музыкой. Теоретически это, конечно, можно сделать, но у кого хватит терпения ждать 5–10 часов, чтобы передать файл размером 600 Мбайт?[1]

Однако такой вариант соединения существует и используется. Поэтому следует рассмотреть его более подробно.

---

[1] При скорости передачи данных 115 Кбит/с (115 / 8 = 14,375 Кбайт/с) файл размером 600 Мбайт (600 × 1024 = 614 400 Кбайт) будет передаваться 11,87 × (614 400 Кбайт / / 14,375 Кбайт/с / 60 с / 60 мин).

В качестве приемника и передатчика информации используются коммуникационные порты, которые есть на любом компьютере, — LPT и COM. Коротко остановимся на их характеристиках.

Характеристики COM-порта

COM-порт (рис. 14.1) является последовательным портом, а это значит, что данные через него передаются только в одном направлении в каждый момент времени: последовательно и сериями — сначала в одну, потом в другую сторону.

Через последовательный порт подключают устройства, которые не требуют высокой скорости передачи данных, например модемы. Хотя в последнее время они практически не используются.

Максимальная скорость передачи данных через последовательный порт составляет 115 Кбит/с, чего вполне хватает для подключаемых к нему устройств.

Последовательные порты обозначаются индексами COM1, COM2 и т. д. Количество контактов в коннекторе (рис. 14.2) или разъеме порта составляет 9 или 25.

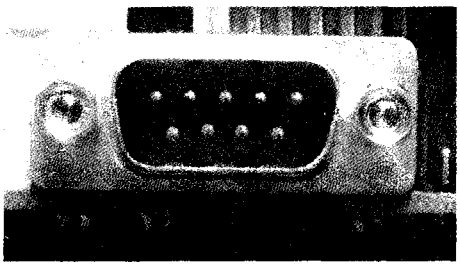


Рис. 14.1. Девятиконтактный COM-порт

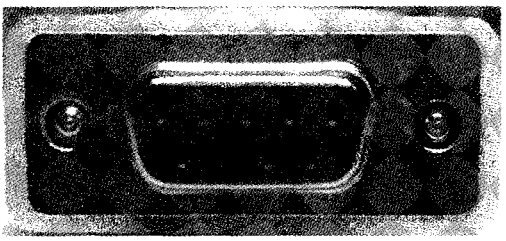


Рис. 14.2. Внешний вид COM-коннектора

Характеристики LPT-порта

LPT-порт (рис. 14.3) является параллельным портом. В отличие от COM-порта, данные через него могут передаваться параллельно и одновременно в двух направлениях, за счет чего достигается более высокая скорость передачи. Порт предназначен для подключения принтера, сканера, ZIP-привода и т. д.

Скорость передачи данных через параллельный порт составляет 800 Кбит/с и более, что зависит от режима работы. Параллельные порты обозначаются

индексами LPT1, LPT2 и т. д. BIOS компьютера поддерживает до трех параллельных портов. Контроллер одного порта встроен в главный набор микросхем (чипсет) на материнской плате, другие могут находиться на дополнительных платах расширения.

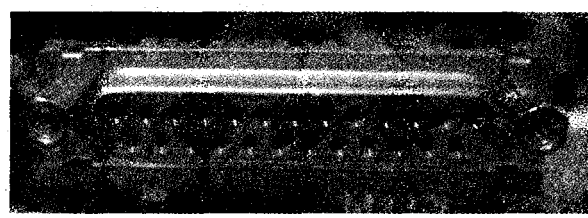


Рис. 14.3. Внешний вид LPT-порта

Параллельный порт обычно может работать в трех режимах.

- **SPP** (Standard Parallel Port) — осуществляет восьмиразрядный вывод данных с синхронизацией по опросу или по прерываниям. Максимальная скорость передачи данных — 800 Кбит/с. Может использоваться для ввода информации по линиям состояния, максимальная скорость приема данных — примерно вдвое меньше.
- **EPP** (Enhanced Parallel Port) — скоростной двунаправленный порт. Он обеспечивает передачу 8 бит данных в двух направлениях. EPP поддерживает режим, при котором порт за счет использования DMA может пересылать информацию из оперативной памяти на устройство и обратно, минуя процессор, что снижает нагрузку на последний. EPP принимает и передает данные в несколько раз быстрее, чем стандартный LPT. Этому также способствует буфер, сохраняющий данные до того, как их сможет принять устройство. Порт EPP полностью совместим со стандартным. Для использования его специфических функций нужно только, чтобы их поддерживала BIOS. Максимальная скорость передачи может достигать 2 Мбит/с.
- **ECP** (Enhanced Capability Port) — дальнейшее развитие параллельного порта. Одной из самых важных функций, реализованных в ECP, является сжатие данных. Это позволяет еще больше повысить реальную скорость передачи, которая в данном случае может достигать 16 Мбит/с. Сжатие возможно как программно (путем применения драйвера), так и аппаратно — самой схемой порта. Для сжатия используется метод RLE (Run Length Encoding), при котором последовательность из повторяющихся символов передается двумя байтами: первый определяет повторяющийся байт, а второй — количество повторений.

На рис. 14.4 показан LPT-коннектор.

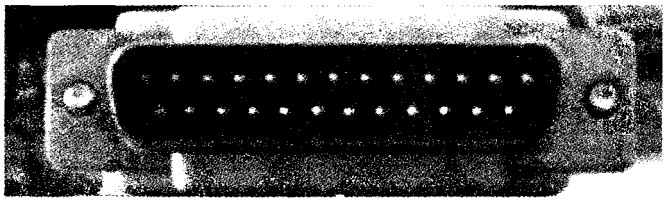


Рис. 14.4. Внешний вид LPT-коннектора

Режимы параллельного порта (SPP, EPP, ECP) можно задавать в BIOS Setup.

Подключение компьютеров

Для подключения двух компьютеров с использованием коммуникационного порта необходим нуль-модемный кабель.

На рис. 14.5 показан кабель для соединения COM-портов двух компьютеров. Он является универсальным, то есть позволяет подключаться как к 9-, так и 25-штырьковому коннектору.

Также можно использовать и кабель для подключения компьютеров через LPT-порт (рис. 14.6).

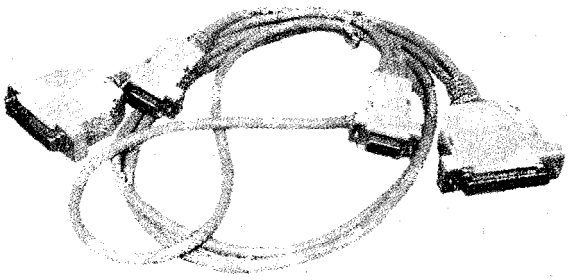


Рис. 14.5. Нуль-модемный кабель для соединения компьютеров через COM-порт

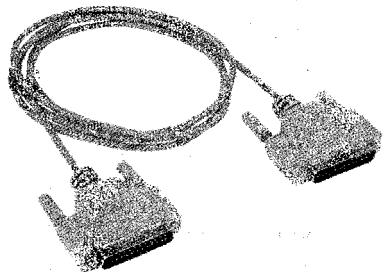


Рис. 14.6. Нуль-модемный кабель для соединения компьютеров через LPT-порт

Использование LPT-кабеля предпочтительнее, так как скорость передачи данных по нему выше, нежели через COM-порт.

Любой из нуль-модемных кабелей можно купить в специальных магазинах. Его также можно сделать и вручную, воспользовавшись паяльником. В последнем случае необходимо учитывать информацию, приведенную в табл. 14.1–14.3.

Таблица 14.1. Таблица вариантов соединения контактов для 25-контактных разъемов

25-контактный разъем	Соединение контактов							
1-й коннектор	1	2	3	4	5	6	7	20
2-й коннектор	1	3	2	5	4	20	7	6

Таблица 14.2. Таблица вариантов соединения контактов для 9-контактных разъемов

9-контактный разъем	Соединение контактов							
1-й коннектор	1	2	3	4	5	6	7	8
2-й коннектор	1	3	2	6	5	4	8	7

Таблица 14.3. Таблица вариантов соединения контактов для 9- и 25-контактных разъемов

Разъемы	Соединение контактов							
9-контактный коннектор	1	2	3	4	5	6	7	8
25-контактный коннектор	8	2	3	6	1	20	5	4

Как уже упоминалось, скорость передачи данных между портами по нуль-модемному кабелю небольшая, в частности для COM-порта она составляет максимум 115 Кбит/с. На практике эта скорость еще ниже, поскольку сильно зависит от длины кабеля, соединяющего порты. По этой причине не рекомендуется использовать кабели длиной более 2–3 м.

Подготовка операционной системы

Подключить нуль-модемный кабель к выбранным портам — только половина дела. Кроме того, нужно организовать программный обмен информацией.

Для примера рассмотрим настройки операционной системы Windows XP Professional. Поддержка подключения по нуль-модемному кабелю в ней уже встроена. Осталось только настроить это подключение в сетевом окружении.

Прежде всего загрузите окно сетевых подключений. Для этого выполните команду **Пуск ▸ Прог раммы ▸ Стандартные ▸ Связь ▸ Сетевые подключения**.

В окне **Сетевые подключения** отображаются все сетевые подключения, которые использует (или имеет) выбранный компьютер.

Для создания нового подключения в Windows XP предназначен мастер новых подключений, значок которого находится в нижней части окна **Сетевые подключения** (рис. 14.7).

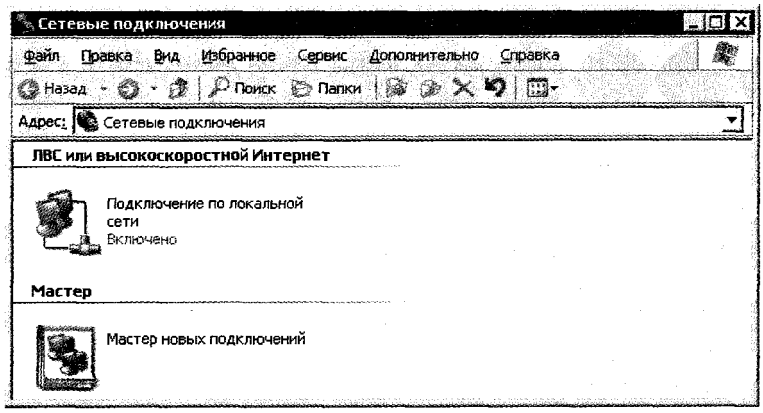


Рис. 14.7. Окно Сетевые подключения

Работа мастера новых подключений основывается на результатах ответов пользователя на вопросы. Таким образом он заблаговременно подготавливает нужные ресурсы. Нажимаем кнопку **Далее**.

В первом окне мастер спросит о том, какое из подключений необходимо создать. Под каждым из вариантов находится краткое описание, поэтому в них легко ориентироваться. В данном случае нужно выбрать **Установить прямое подключение к другому компьютеру** (рис. 14.8), после чего нажать кнопку **Далее**.

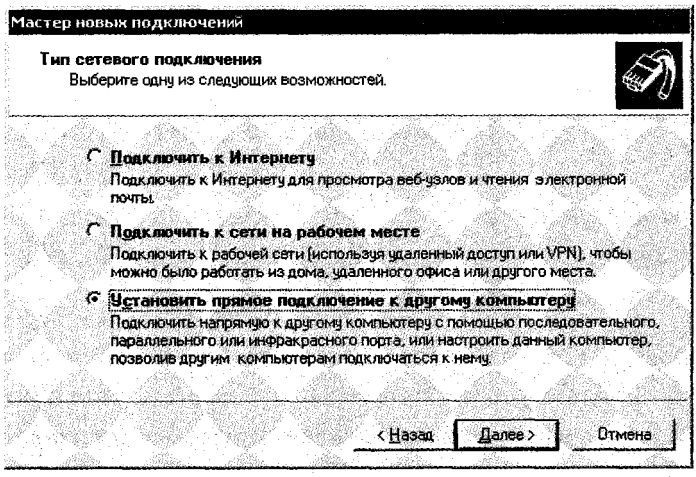


Рис. 14.8. Выбираем тип подключения

Следующее окно предложит вам выбрать из двух подключаемых компьютеров главный, то есть какой будет подключаться, а какой — ждать соединения.

Настройка этих подключений идентична, поэтому предположим, что нужно настроить второе, то есть **Принимать входящие подключения**. После установки переключателя в соответствующее положение нажмите кнопку **Далее**.

В следующем окне нужно выбрать порт, через который будет осуществляться соединение с другим компьютером. Для этого установите соответствующие флажки и нажмите кнопку **Далее** (рис. 14.9).

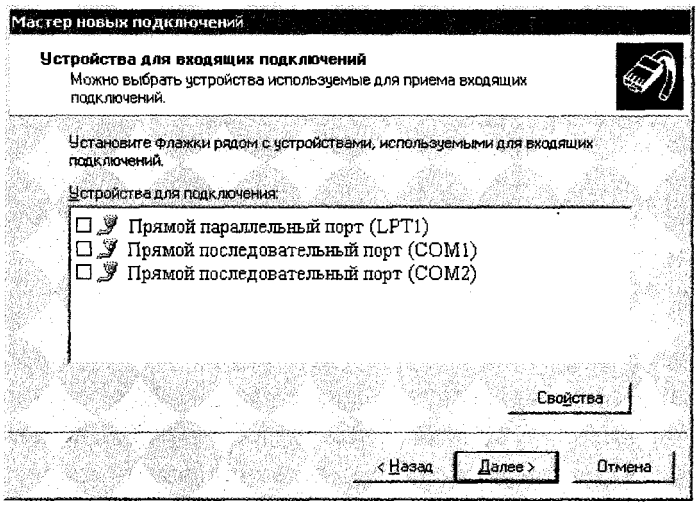


Рис. 14.9. Выбираем порт, используемый для соединения

Теперь система спросит вас, нужно ли разрешить использовать виртуальные частные подключения к Интернету. Фактически это является шлюзом в Интернет.

Этот вопрос вам предстоит решить самим. Однако если выхода в Интернет нет, использовать такой шлюз бессмысленно. Кроме того, подобного рода настройку лучше оставить администратору сети.

Установив нужный флажок, продолжите настройку. В следующем окне необходимо выбрать пользователей, которые будут иметь доступ к ресурсам компьютера. Для этого просто установите флажки напротив нужных позиций.

В следующем окне можно выбрать те службы и протоколы, которые смогут работать при прямом соединении с другим компьютером. Они не обязательно должны совпадать с уже используемыми службами и протоколами, действующими, например, в существующем локальном соединении.

Данный шаг является последним в настройке соединения через нуль-модемный кабель. Об этом вам сообщит окно, которое откроется после нажатия кнопки **Далее**.

После этого в окне **Сетевые подключения** появится новый значок с названием **Входящие подключения**, который отвечает за прямое соединение с другим компьютером (рис. 14.10).

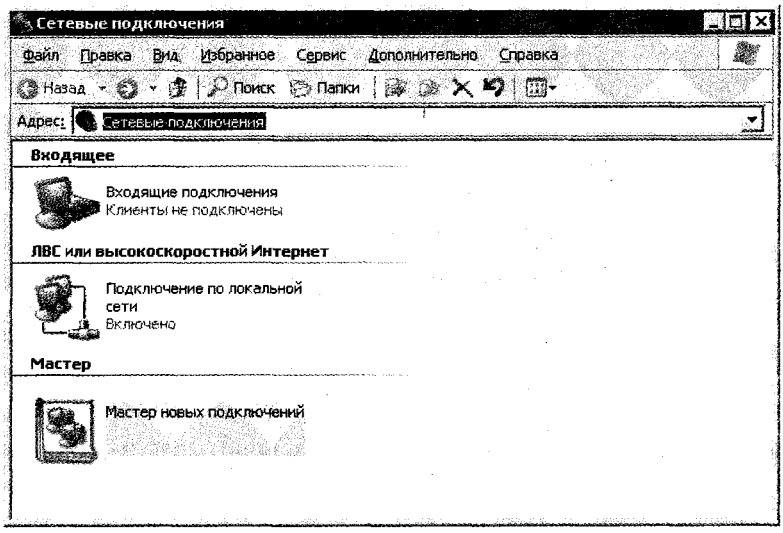


Рис. 14.10. Окно настроенных сетевых соединений

14.2. Соединение с помощью коаксиального кабеля

Для соединения двух компьютеров можно использовать те же средства, что и для соединения нескольких, например коаксиальный кабель.

В таком случае потребуются две сетевые карты, которые имеют разъем для подключения BNC-коннектора, два Т-коннектора, два терминатора, один из которых должен быть заземлен, и соответствующий инструмент (рис. 14.11).

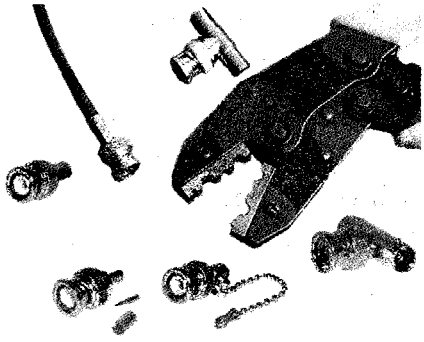


Рис. 14.11. Детали и инструмент, необходимые для соединения компьютеров с помощью коаксиального кабеля

При использовании коаксиального кабеля можно достичь скорости передачи данных 10 Мбит/с, причем при соединении только двух компьютеров практическая скорость (которая обычно меньше теоретической в 1,5–2 раза) вплотную приближается к теоретической. Конечно, ее показатель зависит от длины кабеля.

О том, как правильно обжать коннекторы, вы узнали из предыдущих разделов (см. главу 7).

Затем, предварительно надев на каждую сетевую карту по Т-коннектору, соедините один из концов Т-коннектора приготовленным кабелем. На второй конец каждого Т-коннектора наденьте по терминатору (рис. 14.12).

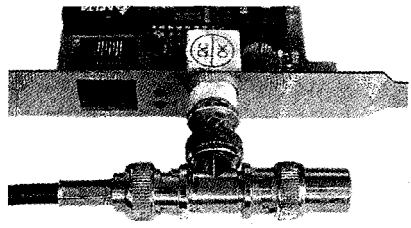


Рис. 14.12. Правильное соединение коннекторов и терминатора на разъеме сетевой карты

Один из терминаторов должен иметь цепочку, которую желательно соединить с заземлением. Если этого не сделать, то может выйти из строя одна из сетевых карт.

Как правило, на задней панели сетевой карты присутствуют минимум два индикатора, один из которых сигнализирует о наличии соединения, а второй — о его скорости.

ПРИМЕЧАНИЕ

На сетевых картах, поддерживающих работу в режимах 10 и 100 Мбит/с, присутствуют три индикатора. Первый показывает состояние соединения, второй — наличие подключения на скорости 10 Мбит/с, третий — на скорости 100 Мбит/с. Аналогичные индикаторы есть на сетевых картах, которые работают в режимах 100 и 1000 Мбит/с.

Если в процессе подключения не было допущено ошибок, то индикатор соединения должен гореть на обеих сетевых картах. Не гореть он может по следующим причинам:

- была допущена ошибка при обжиме коннекторов;
- сетевая карта плохо установлена в слот;
- неисправен слот, в который установлена сетевая карта;
- неисправна сетевая карта;
- поврежден кабель;
- неисправны сетевые адаптеры.

Если индикатор соединения горит на двух сетевых картах, значит, соединение установлено. Теперь, чтобы компьютеры могли обмениваться информацией, нужно установить драйверы, сетевые протоколы и настроить права доступа на ресурсы. О том, как это правильно сделать, читайте в пятой части книги, посвященной вопросам настройки программного обеспечения.

14.3. Соединение с помощью кабеля на основе витой пары

Этим способом можно соединить любое количество компьютеров. В случае соединения двух машин используют специальный кроссовер-кабель, распайка контактов которого отличается от стандартного патч-корда.

Как уже упоминалось, использование кабеля на основе витой пары позволяет добиться хороших показателей быстродействия сети. При использовании кабеля пятой категории теоретическая скорость передачи данных составляет 100 Мбит/с, а в случае соединения двух компьютеров она почти равна реальной.

Для соединения двух компьютеров с помощью кабеля на основе витой пары понадобятся два коннектора с двумя колпачками (можно и без них), отрезок кабеля нужной длины и соответствующий инструмент (рис. 14.13). Однако в этом случае при обжиме коннекторов нужно придерживаться немного других правил, нежели когда компьютеры соединяются посредством концентраторов или другого оборудования (см. главу 8).

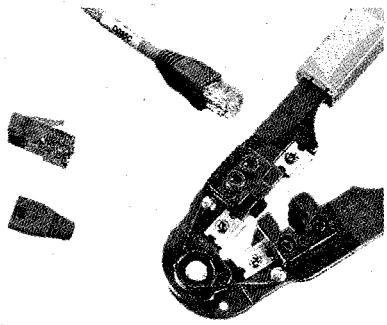
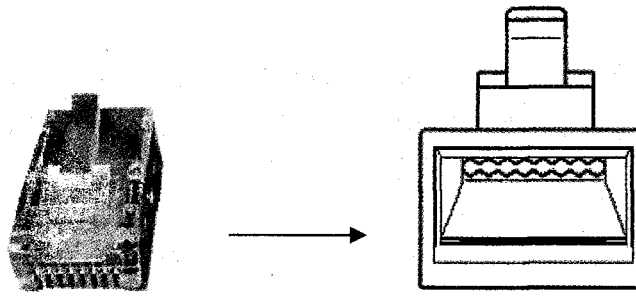


Рис. 14.13. Детали и инструмент, необходимые для соединения компьютеров с помощью кабеля на основе витой пары

Кабель, созданный по таким правилам, называется кроссовер-кабелем, или перевернутым кабелем. Однако перед тем, как рассказывать о принципе его создания, коротко рассмотрим структуру самого кабеля.

Возьмем для примера восьмижильный кабель. В кабеле пятой категории для передачи и приема данных соответственно используются по четыре проводника. Название витой пары он получил благодаря тому, что пары проводников скручены друг с другом. Кроме того, проводники все вместе также переплетены между собой.

Чтобы соединить два компьютера, не используя концентратор, нужно поменять местами некоторые пары проводников. На рис. 14.14 показано изначальное расположение проводников в коннекторе согласно стандарту EIA/TIA-568B.



1 — бело-оранжевый;
2 — оранжевый;
3 — бело-зеленый;
4 — голубой;
5 — бело-голубой;
6 — зеленый;
7 — бело-коричневый;
8 — коричневый

Рис. 14.14. Стандартное расположение проводников в разъеме

В табл. 14.4 показано, какие из проводников нужно поменять местами, чтобы получить кабель кроссовер.

Таблица 14.4. Распайка контактов кроссовер-кабеля

Первый RJ-45-разъем	Цвет провода	Второй RJ-45-разъем
1 контакт	Бело-оранжевый	3 контакт
2 контакт	Оранжевый	6 контакт
3 контакт	Бело-зеленый	1 контакт
4 контакт	Голубой	4 контакт
5 контакт	Бело-голубой	5 контакт
6 контакт	Зеленый	2 контакт
7 контакт	Бело-коричневый	8 контакт
8 контакт	Коричневый	7 контакт

После того как кабель собран, остается подключить его к сетевым картам. Если индикатор подключения на сетевой карте не горит, значит, была допущена ошибка при обжиме кабелей, конечно, если сама сетевая карта заведомо исправна.

После этого остается только настроить параметры сетевого окружения. О том, как это правильно сделать, читайте в пятой части книги.

14.4. Соединение с помощью USB-кабеля

Все современные персональные компьютеры имеют два, а некоторые даже четыре встроенных USB-порта. Поэтому в появлении средств соединения двух компьютеров через специальный USB-кабель нет ничего удивительного.

Скорость работы USB-порта, особенно стандарта 2.0, очень высокая, что позволяет организовать эффективное соединение двух компьютеров. При этом теоретически можно достичь скорости 480 Мбит/с.

USB-соединение, в силу использования кабеля, относится к нуль-модемным соединениям. Правда, данный тип не так распространен, как, например, соединение с помощью LPT-порта.

Главный недостаток USB-соединения — его относительно высокая стоимость. Многие пользователи предпочитают потратить те же деньги на покупку хороших сетевых карт и коаксиального шнура или кабеля на основе витой пары. Однако USB-соединение все же используют, и в некоторых случаях оправданно. Что, например, делать, если есть ноутбук без сетевой карты, а его нужно соединить с другим компьютером? Один из выходов — нуль-модемное соединение.

Для USB-соединения двух компьютеров используют специальный кабель (рис. 14.15), имеющий модуль, который отвечает за некоторые преобразования сигнала. Его длина составляет примерно 3–3,6 м, хотя может доходить и до 20 м. Однако помните: чем длиннее кабель, тем ниже скорость передачи данных.

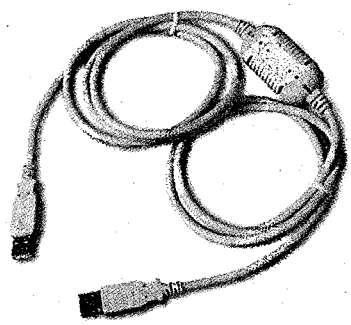


Рис. 14.15. USB-кабель, используемый для соединения двух компьютеров

Что касается доступа к общим ресурсам, то при таком типе подключения отображаются все папки каждого компьютера вне зависимости от прав доступа.

14.5. Соединение через FireWire-порт

Соединение через FireWire-порт — еще один вид соединения, обладающий высокой скоростью передачи данных, которая может достигать 400 Мбит/с.

FireWire — это последовательный порт, который поддерживает скорость передачи данных до 400 Мбит/с. Его изначальное предназначение — подключение к компьютеру видеоустройств, таких, например, как видеомагнитофон, а также другого оборудования, требующего быстрой передачи большого объема информации, в частности внешних жестких дисков.

Все современные модели материнских плат оснащают двумя и более FireWire-портами. Так почему не использовать их для организации быстрого соединения?

Для такого соединения вам нужно иметь следующее.

- FireWire-контроллер (рис. 14.16). В большинстве настольных компьютеров используются шестиконтактные порты, а в ноутбуках — четырехконтактные.
- FireWire-кабель. Тип кабеля зависит от типа FireWire-портов. Соответственно бывают кабели с четырех- и шестиконтактным разъемами.

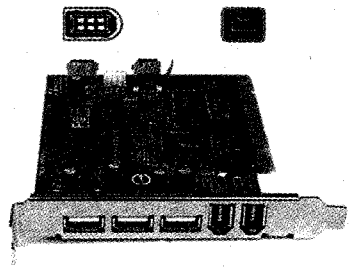


Рис. 14.16. FireWire-контроллер

Единственный неприятный момент такого соединения — слишком короткий кабель. Если пользоваться кабелем длиной до 4,5 м, то соединение будет работать на полную мощность — 400 Мбит/с. Увеличение его длины до 10–15 м приводит к резкому снижению скорости передачи до 50–80 Мбит/с, хотя и этого вполне хватает для любых работ.

Однако не расстраивайтесь. Если вам повезет и вы найдете FireWire-репитер (а такие встречаются в продаже), длина сегмента в этом случае может быть увеличена до 70–100 м.

14.6. Соединение через Bluetooth

Сегодня Bluetooth есть практически везде, начиная с бытовых приборов и заканчивая мобильными телефонами и компьютерами. Именно этот факт и является привлекательным и решающим, когда нужно быстро соединить два устройства.

Недостаток Bluetooth — низкая скорость и малый радиус действия, однако для быстрого перекидывания небольшого количества информации этот способ вполне подходит.

Технология Bluetooth — один из самых простых способов соединения двух компьютеров, все сводится к настройке программной части, поскольку Bluetooth-адаптеры у них стандартные. При этом Bluetooth позволяет достигать скорости 2–3 Мбит/с (последняя спецификация стандарта) при максимальном расстоянии 150 м.

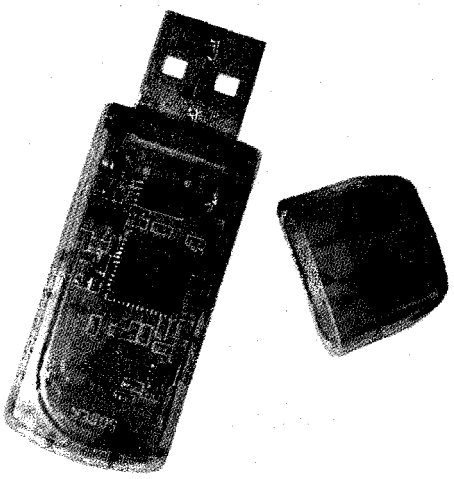


Рис. 14.17. Внешний вид Bluetooth-адаптера

Для соединения персональных компьютеров придется приобрести Bluetooth-адаптер (рис. 14.17) и подключить его к машине. Как правило, используются USB-адаптеры, подключаемые к USB-портам.

Чтобы заставить сеть работать, достаточно установить драйверы устройств, настроить рабочую группу и права доступа. О том, как это правильно сделать, читайте в пятой части книги, посвященной вопросам настройки программного обеспечения.

Глава 15

Домашняя сеть

- Проектирование сети
- Выбор топологий и стандарта
- Размещение оборудования
- Прокладка кабеля
- Использование беспроводного оборудования
- Необходимое сетевое оборудование

В последнее время начали активно распространяться сети, позволяющие связывать компьютеры, работающие в жилых домах. Понять причину этого очень просто: пользователи хотят прийти домой и получить практически тот же набор информационных услуг, к которым они привыкли на работе: в офисах и на предприятиях. А это — обмен файлами, общение в реальном времени, сетевые игры, электронная почта и, самое главное, Интернет.

Поскольку не существует и не может существовать никаких стандартов, которые бы описывали правила создания сети в подобных условиях, домашние сети создаются хаотично, основываясь на всех существующих стандартах, которые можно использовать в конкретном случае. Однако это совсем не означает, что это правильно. Как раз наоборот, если бездумно спроектировать сеть, вы рано или поздно столкнетесь с тем, что она не поддается расширению и поднять ее производительность невозможно. Кроме того, большую роль играет то, как вы проложите кабель или организуете радиоэфир, какое будете использовать оборудование и т. д. Обо всем этом читайте далее.

15.1. Проектирование сети

Проектирование и еще раз проектирование! Семь раз отмерь, один раз отрежь! Примерно такого типа девизы должны быть у вас, когда вы решаетесь организовать пусть даже небольшую, но сеть.

Почему проектирование настолько важно? Дело в том, что от проекта зависит выбор наилучшего варианта топологии, что, в свою очередь, определяет быстродействие сети или, по крайней мере, одного из ее сегментов.

Итак, приступим. Для начала соберите некоторую информацию о будущем наполнении сети, а именно:

- о количестве подключаемых компьютеров;
- о примерном расстоянии от компьютера до входа в помещение с учетом удобной прокладки кабеля;
- о наличии в комнате окна и примерном расстоянии от него до компьютера с учетом прокладки кабеля по близлежащей стене;
- о дополнительных вариантах размещения компьютера с целью уменьшения расстояния до окна и до входа в помещение;

- о наличии электрических и телефонных розеток возле компьютера;
- о наличии сетевого адаптера и его типе;
- об установленной операционной системе;
- об уровне подготовки пользователя для работы в сетевом окружении;
- о возможностях прокладки кабеля вне помещения (в коридоре);
- о возможностях прокладки кабеля;
- о пожеланиях пользователя.

Как видите, требуется достаточно много информации. Однако она, несомненно, поможет подобрать оптимальный (дешевый/производительный) способ проведения сети.

Теперь, чтобы представить себе визуальную картину из собранной информации, переведите ее на бумагу в виде плана расположения всех объектов.

Таким образом, вы получаете полуфабрикат проекта (или нескольких проектов) будущей сети. Следующий шаг — выбор топологии сети для связи между собой всех точек в проекте.

15.2. Выбор топологий и стандарта

Коротко напомню: топология — способ организации сети, который позволит добиться от нее максимальной производительности при минимальном вложении средств, но с учетом будущего роста сети.

От топологии и стандарта сети напрямую зависит ее быстродействие. На практике всегда приходится жертвовать соблюдением топологии с целью уменьшения затрат на создание сети. И в этом нет ничего странного. Такой подход оправдывает себя в том случае, если сеть создается временно или без учета ее расширения. Если же планируется создание сети, которая будет приносить деньги, то выбирать топологию следует очень продуманно, в противном случае при серьезном расширении вам придется делать незапланированное добавление нового или замену слабого активного оборудования, которое стоит больших денег.

Как показала практика, наиболее часто встречающийся вариант топологии — это «звезда». Намного реже встречается топология «общая шина». Бывают случаи, когда они пересекаются.

Рассмотрим выбор топологии на примерах.

Пример 1. Предположим, нам необходимо создать домашнюю сеть, которая объединяет компьютеры двух рядом расположенных многоэтажных домов. При этом количество подключаемых машин сравнительно небольшое — около двух десятков компьютеров на разных этажах. Планируется использование общего Интернета с подключением через ADSL-модем.

Более подробная информация:

- дома расположены напротив друг друга на расстоянии примерно 80 м;
- в доме А пользователи располагаются согласно табл. 15.1;
- в доме В пользователи располагаются согласно табл. 15.2.

Таблица 15.1. Данные по дому А

Этаж	Подключаемые квартиры и их расположение	Подключаемые компьютеры		Расстояние от компьютера до входной двери, м	Расстояние от компьютера до окна, м
1	1	2		18, 36	3, 6
3	3 смежные	1 кв.	2	10, 25	4, 3
		2 кв.	1	18	4
		3 кв.	1	30	7
4	2 напротив	1 кв.	1	16	3
		2 кв.	1	15	4
8	2 смежные	1 кв.	1	28	5
		2 кв.	1	19	10
10	4 смежные, по 2 с каждой стороны клетки	1 кв.	1	23	10
		2 кв.	2	12, 40	4, 5
		3 кв.	1	24	6
		4 кв.	1	33	7

Таблица 15.2. Данные по дому В

Этаж	Подключаемые квартиры и их расположение	Подключаемые компьютеры		Расстояние от компьютера до входной двери, м	Расстояние от компьютера до окна, м
2	1	1		26	4
4	2 смежные	1 кв.	1	17	3
		2 кв.	1	22	2
5	1	1		16	3
7	1	2		24, 36	5, 6

Внимательно изучив собранную информацию, можно предложить следующие варианты построения сети (рис. 15.1 и 15.2):

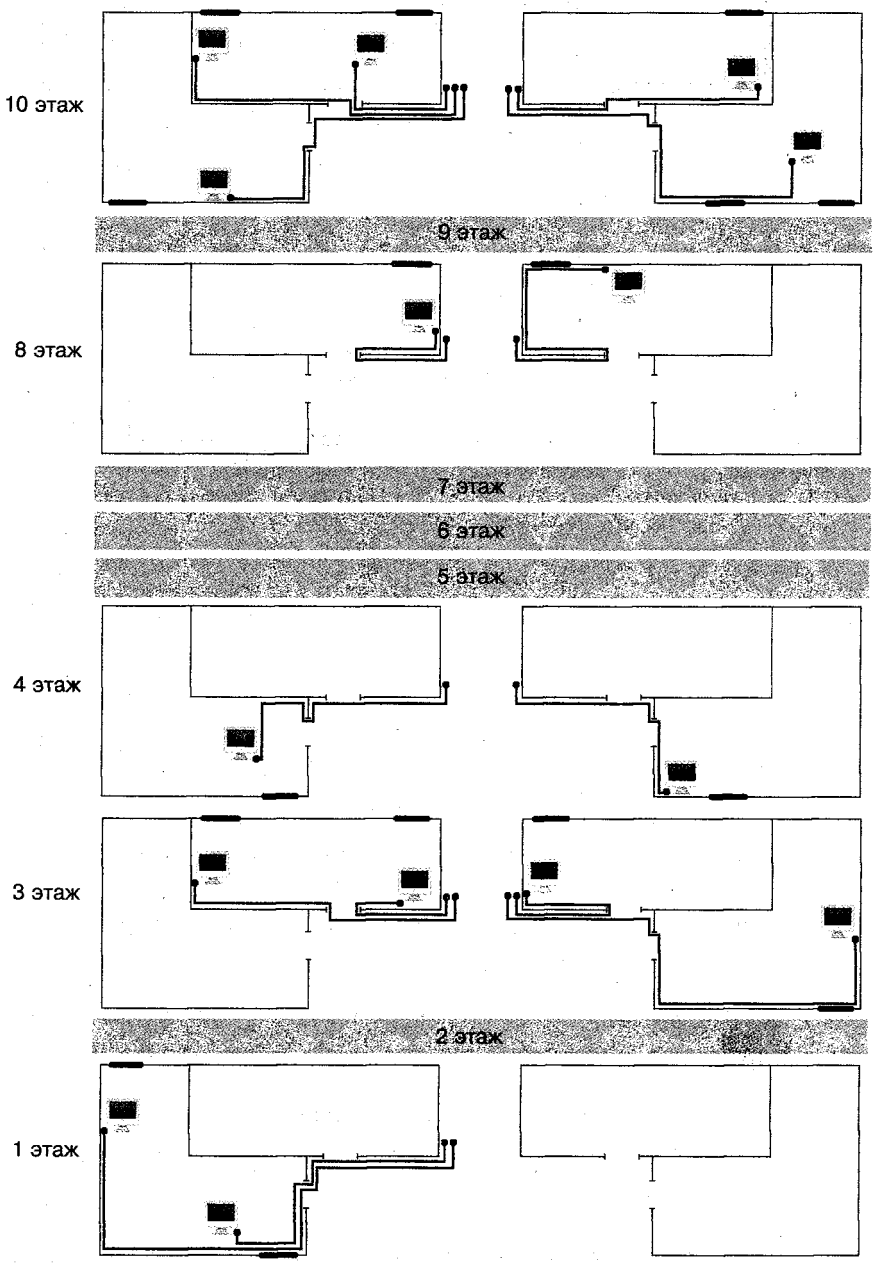


Рис. 15.1. Вариант теоретически «идеального» проекта сети дома А

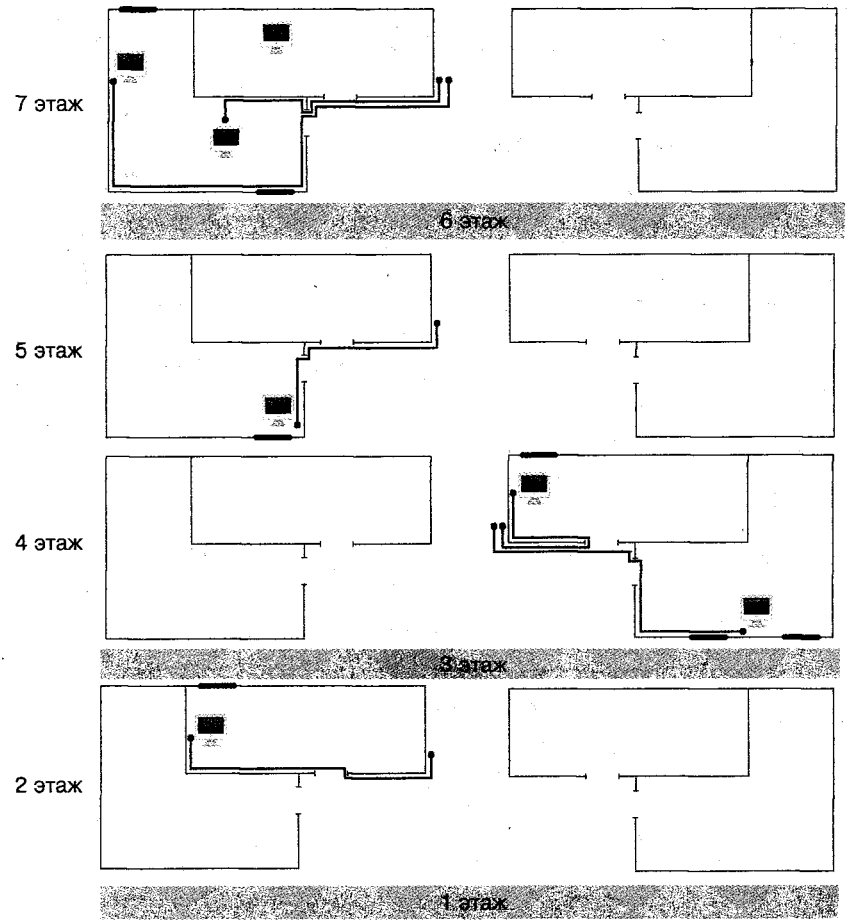


Рис. 15.2. Вариант теоретически «идеального» проекта сети дома В

- использование топологии «звезда» для подключения компьютеров и для соединения активного оборудования;
- использование топологии «звезда» для подключения компьютеров и топологии «общая шина» для соединения активного оборудования.

Другие варианты здесь неприменимы или не имеют смысла, поскольку усложняется прокладка кабельной системы или стоимость такой сети не вписывается в предполагаемый бюджет.

Пример 2. Предположим, вы являетесь владельцем небольшой фирмы, торгующей косметикой. Магазин фирмы по счастливому стечению обстоятельств

расположен в том же доме, где вы проживаете, только офис территориально находится в пристройке к первому этажу, а ваша квартира — на четвертом. В магазине работают 5 менеджеров, для учета продаж используется пакет «1С: Предприятие». Чтобы контролировать наличие продукции в магазине, находясь при этом в своей квартире, вы решаете создать сеть.

Обладая достаточным набором знаний и навыками, вы решаете не привлекать к созданию сети сторонних специалистов и все сделать своими руками с минимальными затратами.

Как и полагается, вы создаете варианты проектов будущей сети, с учетом того, что в ней будут работать в общей сложности 4 компьютера (3 — в офисе (рис. 15.3) и 1 — дома).

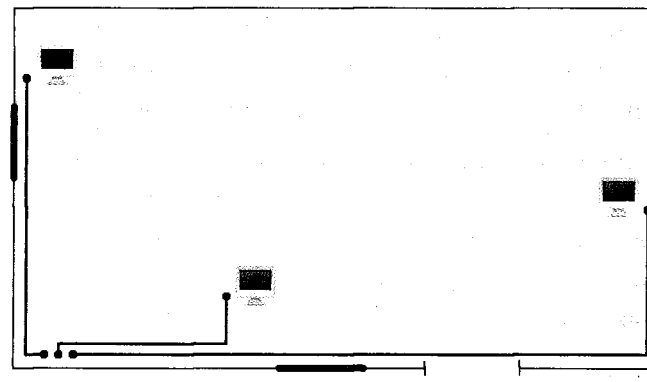


Рис. 15.3. Вариант проекта сети в магазине

Изучив информацию, можно предложить следующие варианты построения сети:

- использование топологии «звезда» для подключения всех компьютеров;
- использование топологии «общая шина» для подключения компьютеров в магазине и топологии «звезда» для подключения компьютера (компьютеров) в квартире.

Относительно выбора стандарта как в первом, так и во втором примере ориентируйтесь на наиболее быстрый и доступный. Например, если дело касается сети на основе витой пары, можно остановиться на стандарте IEEE 802.3 100Base-TX. Что касается разветвлений сети, которые могут в любой миг возникнуть, то здесь выбирать не приходится: для коаксиальных сегментов ориентируйтесь на тонкую Ethernet, для беспроводных — на IEEE 802.11g или IEEE 802.11g+.

15.3. Размещение оборудования

Никакая более или менее серьезная сеть не может обойтись без активного оборудования. Как минимум для малой сети это концентратор или точка доступа, для большой — концентраторы, коммутаторы, маршрутизаторы и т. д.

При размещении активного оборудования в случае домашней сети используются такие же подходы, как и при построении офисной сети, когда требуется выполнение определенных правил. Однако при этом используются выработанные практикой навыки и знания. А практика показала следующее.

- Такое дорогостоящее оборудование, как маршрутизаторы или коммутаторы, нужно устанавливать в тех местах, где сходятся не менее трех больших сегментов сети. При этом для размещения оборудования отводится отдельное помещение на техническом этаже или чердаке, которое снабжается металлической или бронированной дверью и сигнализацией, ведь стоимость оборудования может доходить до нескольких тысяч долларов.
- Если, например, в подъезде дома к сети хотят подключиться всего несколько человек, не имеет смысла устанавливать концентратор с большим количеством портов: в любой момент его можно заменить более мощным, а этот использовать в другом месте. В таком случае концентратор располагается на техническом этаже или чердаке и крепится на одной из стен.
- В случае если вам нужно подключить компьютеры в подъездах 1, 3, 4 и 5, концентраторы (или коммутаторы) лучше установить в подъездах 1, 3 и 5. Хотя этим вы и увеличиваете длину кабельного сегмента, зато не окажетесь в ситуации, когда близко расположенное активное оборудование мешает друг другу и приводит к замедлению действия сети.

И еще одно важное замечание: никогда не размещайте оборудование у пользователей сетей (за исключением себя лично). Этим вы поставите под угрозу функционирование сети, поскольку в нужный момент не сможете получить к нему доступ.

15.4. Прокладка кабеля

Прокладка кабеля осуществляется в зависимости от конкретных условий. Необходимо отметить, что желательно предварительно договориться с жильцами

дома и уведомить представителей жилищно-управленческих организаций о проведении работ. Благодаря этому вы не только сможете спокойно действовать, но и получите ценную информацию о том, где и как проложены электропроводка, телефонный кабель и другие коммуникации и как лучше будет протянуть ваш кабель.

Как показала практика, оптимальный способ прокладки кабеля — внешний, то есть вне дома. Многих может удивить такой подход, но объясняется он очень просто:

- проводка кабеля не требует особых усилий;
- прокладка кабеля вне дома никому не мешает;
- достигается наименьшая длина сегмента кабеля;
- мало кто позволит или захочет провести 20–30 м кабеля по стенам квартиры с евроремонтом, дорогими обоями, плиткой и т. д.;
- легкая и быстрая замена поврежденного сегмента;
- удобный подвод кабеля к центру управления на техническом этаже или чердаке.

Это далеко не полный список преимуществ такого способа прокладки кабеля.

Самый главный аргумент использования внешней прокладки — это легкость замены поврежденного сегмента кабеля. Опять же, как показала практика, повреждение кабеля происходит в основном умышленно (конкурирующая сеть, злобные соседи и т. д.). Именно поэтому гораздо выгоднее поменять свободно расположенный кабель, нежели менять его в распределительных щитах по всему подъезду. Кроме того, провести десяток кабелей по уже занятым коммуникационным каналам в распределительных щитах крайне сложно.

При прокладке кабеля вне помещения, то есть на открытом воздухе, нужно придерживаться следующих правил.

- Желательно использовать специальную гофрированную трубку. После помещения кабеля в трубку, где это только получится, прикрепите ее к стене любым способом. Концы трубки обязательно изолируйте, используя для этого строительную пену или силикон. Такая защита позволит, насколько это возможно, исключить контакт кабеля с внешней средой.

ПРИМЕЧАНИЕ

Если принято решение использовать гофрированную трубку, не приобретайте самый дешевый ее вариант. Как показывает практика, дешевая гофра часто не выдерживает даже одного сезона: за одно жаркое лето трубка теряет свои свойства, трескается и рассыпается на части.

- При протягивании кабеля между домами обязательно используйте связующий трос. Если этого не сделать, в скором времени кабель нужно будет менять: ветер, птицы, обледенение и *т. д.* сделают свое черное дело. Прежде всего установите трос, натянув его достаточно сильно. Для крепления на нем гофрированной трубки с кабелем (или несколькими кабелями) внутри используйте скобы, устанавливая их через каждые метр-полтора. Также можно использовать любой другой протянутый между домами кабель достаточной толщины, например телефонную магистраль.
- Закрепляйте кабель везде, где это возможно. Не допускайте провисания, даже если кабель висит вертикально: под воздействием собственного веса он может утратить некоторые технические характеристики, что будет приводить к коллизиям в сети.
- Обязательно изолируйте кабель. Используйте для этого любые доступные средства, но лучше те из них, которые нечувствительны к внешним воздействиям.
- Не забывайте, что длина сегмента кабеля ограниченна. Не следует оставлять большие петли, если этого не требует ситуация. Чем короче кабель, тем быстрее сеть и меньше коллизий.

Что касается прокладки кабеля внутри помещения (квартиры), можно использовать любой доступный способ. Главное, чтобы путь не был излишне длинным и в достаточной мере отвечал пожеланиям конечного пользователя. Если требуется, используйте специальный пластиковый короб, в который прячется сетевой кабель.

Чтобы провести кабель через окно, придется сделать отверстие в раме. После пропускания кабеля через него щели можно закрыть силиконом с внешней стороны рамы.

Если планируете подключать большое количество рабочих мест, используйте кабель «витая пара» пятой категории. Это позволит в случае надобности подключать к одному кабелю два компьютера либо при неисправности использовать другие пары проводников. При этом обязательно придерживайтесь

единого стандарта в обжиме коннекторов, иначе столкнетесь с проблемой несовместимости оборудования. В случае применения коаксиальных сегментов используйте тонкий кабель, поскольку он более гибкий и не требует дополнительного оборудования.

Также не забывайте о радиусе изгиба кабеля. В местах сильных перегибов оболочка кабеля трансформируется и лопается.

Если между домами достаточно большое расстояние, следует задуматься об использовании оптоволоконного кабеля. По цене он практически не отличается от кабеля на основе витой пары. Стоимость обжима двух оптоволоконных разъемов колеблется от $50 до 150, что зависит от наглости исполнителя. Зато плюсами такого сегмента являются его долговечность (кабель практически не боится температурных колебаний и влажности) и отсутствие затухания сигнала и помех.

15.5. Использование беспроводного оборудования

Когда приходит момент соединения двух удаленных домов, встает вопрос о возможных способах осуществления проекта. Выбор небольшой — оптоволоконный кабель или беспроводное оборудование.

Достоинства оптоволоконного кабеля нам известны, и его спокойно можно использовать для этого благородного дела.

А вот рассматривая вариант использования беспроводного оборудования, нужно учитывать следующие моменты.

- «Дальнобойность» беспроводного оборудования при использовании стандартных средств достаточно сомнительна. Достичь приемлемых результатов можно только с использованием внешней антенны.
- При применении внешних антенн могут появиться проблемы с легализацией использования радиоэфира, то есть придется оформлять сеть по всем правилам, за что нужно платить.
- Скорость передачи данных беспроводным оборудованием зависит от расстояния между объектами. А это означает, что при больших расстояниях, даже используя внешнюю антенну, вы, сами того не подозревая, создадите «узкое место», что значительно понизит реальную скорость передачи между сегментами сети.

- Стоимость двух хороших точек доступа и двух внешних антенн гораздо выше стоимости оптоволоконного кабеля с уже обжатыми коннекторами.
- Стоимость замены беспроводного оборудования в случае его выхода из строя гораздо выше стоимости нового оптоволоконного кабеля.
- При использовании беспроводного оборудования вам придется приобретать средства грозозащиты. Что, как показывает практика, практически никакой пользы не приносит, особенно если оборудование используется на окраине города.

Как видите, при использовании беспроводного оборудования в домашней сети гораздо больше недостатков, нежели преимуществ. Поэтому, прежде чем решиться на такой шаг, обязательно убедитесь в том, что обойтись без беспроводного оборудования никак нельзя.

Если решено все-таки применять беспроводное оборудование, используйте устройства наиболее быстродействующего стандарта. На сегодняшний день это IEEE 802.11g, с помощью которого можно достичь теоретической (!) скорости 122 Мбит/с.

15.6. Необходимое сетевое оборудование

Итак, вы спроектировали сеть и определились с ее топологией, способом прокладки кабеля или установкой беспроводного оборудования. Теперь необходимо решить, какое сетевое оборудование вам необходимо и в каких количествах.

В принципе, подход к покупке оборудования достаточно прост. На рынке представлено просто огромное количество производителей, поэтому выбрать одного из них не составляет никакой сложности. Из наиболее зарекомендовавших себя можно отметить производителей 3COM или Cisco, правда и цены на их оборудование выше: за качество нужно платить.

Выбор сетевых адаптеров

Что касается сетевых адаптеров, они могут быть от разных производителей. Кроме того, 70–80% всех компьютеров сети будут оборудованы встроенными устройствами с разъемом RJ-45. Для коаксиальных сегментов придется искать сетевые карты с BNC-разъемом (желательно, чтобы также был и разъем RJ-45).

Поэтому речь в основном идет о выборе активного сетевого оборудования, такого как концентраторы, коммутаторы и маршрутизаторы. Сюда же можно включить и беспроводное оборудование.

Выбор маршрутизатора

Начнем с самого главного — маршрутизатора. Он однозначно должен быть качественным, неплохо, если устройство будет предполагать возможность дальнейшего расширения сети. В связи с этим лучше приобретать модель от зарекомендовавшего себя производителя, например D-Link, Cisco или ZyXEL. Что касается количества портов на маршрутизаторе, оно должно быть достаточным для того, чтобы подключить все имеющиеся концентраторы и коммутаторы. Конечно, стоимость маршрутизатора зависит от количества портов, зато вы сможете эффективно разделять сегменты сети, обеспечивая тем самым наибольшую производительность. Также не забывайте, что в маршрутизаторе необходимо выделить один порт для подключения ADSL-модема или выделенной линии (например, оптоволокна). Если планируется использовать беспроводной Интернет, можно сразу подобрать маршрутизатор с беспроводным ADSL-модемом, тем самым сводя количество используемых устройств к минимуму.

Выбор концентраторов и коммутаторов

Лучше приобретать концентраторы одного производителя, причем с возможностью удаленного управления портами, что позволит вам отключать неиспользуемые порты или порты пользователей, которые просрочили платеж или просто создают проблемы для работы сети.

Следует хорошо подумать о количестве портов концентратора. Так, например, для подключения двух лестничных клеток достаточно одного 8-портового концентратора. Можно даже подсоединить еще один этаж, если использовать коаксиальный сегмент, который потом подключается к имеющемуся на концентраторе порту (обязательно приобретайте концентратор с таким портом!).

Однако большое количество концентраторов, кроме создаваемого лишнего шума в сети[1], еще и отберет у маршрутизатора лишние порты, которых, как показала практика, всегда не хватает. Поэтому, если количество подключаемых компью-

[1] Ведь концентратор рассылает входящие сообщения на все имеющиеся порты.

теров достаточно велико, следует рассмотреть вопрос приобретения не 8-, а 16- или 32-портовых концентраторов.

Хочу заметить, сегодня стоимость коммутаторов значительно снизилась, что приводит к постепенному вытеснению ими концентраторов. Эффект от использования коммутаторов вместо концентраторов очень положительный, поскольку первые — более интеллектуальные устройства по сравнению со вторыми. В отличие от концентратора, который передает сигнал на все порты, тем самым создавая лишний трафик, коммутатор распределяет данные в исключительно заданном направлении (отсюда и объяснение других названий коммутатора — свитч, переключение или перенаправление портов).

Второй несомненный плюс коммутатора — возможность удаленного управления, что позволяет администратору сети отключать «зарвавшихся» пользователей.

СОВЕТ

Если есть возможность, вместо концентраторов приобретайте коммутаторы. Преимущества их использования вы заметите практически сразу.

Выбор беспроводного оборудования

Если ситуация вынуждает использовать беспроводную связь, обязательно приобретайте оборудование одного производителя и одного стандарта. Производитель D-Link зарекомендовал себя с наилучшей стороны, да и продукция его составляет примерно 70 % рынка сетевого оборудования.

Как уже было упомянуто ранее, обязательно соблюдайте стандарт оборудования. На сегодняшний день наиболее скоростным и помехозащищенным является стандарт IEEE 802.11g. Как было упомянуто ранее, скоростные показатели некоторых моделей (модели g+) составляют 108, а иногда и 122 Мбит/с. Обязательно обратите внимание на это оборудование и, если это возможно, приобретайте именно его!

Эти рекомендации относятся к любому типу оборудования, будь то беспроводной адаптер или точка доступа.

Что касается использования внешней антенны, то здесь нужно исходить из существующих условий. Если наблюдается устойчивая связь с достаточно высокой скоростью, то с использованием антенны можно повременить.

Управление ресурсами сети

Когда дело касается домашних сетей, такое понятие, как управляющий компьютер, не рассматривается, ведь сервер стоит больших денег, а с расширением сети его мощности все равно не хватит. В то же время наличие в сети файловых серверов обязательно, поскольку их отсутствие отберет у пользователей один из главных козырей — бесплатный обмен мультимедийными файлами.

Файловый сервер не обязательно должен быть очень мощным. Им может быть рабочий компьютер любого пользователя, который решил поделиться со всеми своими файловыми ресурсами.

Что касается управления сетью, вам останется только раздавать новым пользователям статические IP-адреса, маску подсети и названия рабочих групп. В противном случае пользователи просто не смогут войти в сеть или будут информированы о том, что IP-адрес уже используется другой рабочей станцией.

Совсем другое дело, когда локальная сеть будет подключена к Интернету. В этом случае вам придется иметь компьютер, на котором будет установлена биллинговая система, ведущая учет используемого пользователями трафика с целью вычисления затрат. Опять же, как показала практика, подобный компьютер лучше всего арендовать или установить у провайдера Интернета и управлять им с помощью удаленного доступа.

Часть 5

Установка оборудования и настройка программной части

Глава 16

Настройка сети в Windows 2003 Server

- Выбор управляющего компьютера
- Создание домена
- Использование DNS-сервера
- Использование DHCP-сервера
- Использование механизма Active Directory
- Настройка общего доступа

16.1. Выбор управляющего компьютера

Функционирование локальной сети зависит не только от ее правильного проектирования и создания, но и от управляющего компьютера, который ее обслуживает. Именно поэтому выбор такого компьютера — следующий этап в настройке только что созданной сети.

Если дело касается домашней или офисной сети из нескольких компьютеров, установка отдельного сервера особого смысла не имеет, поскольку его роль может выполнить любая из подключенных машин.

Как бы там ни было, если планируется выделить компьютер под сервер, очень хорошо, если его конфигурация будет достаточно продуманной. Ниже, в табл. 16.1–16.5, дано описание нескольких конфигураций серверов разного назначения.

Таблица 16.1. Пример конфигурации принт-сервера

Комплектующие	Конфигурация
Процессор	Intel Celeron, 2,8 ГГц
Оперативная память	512 Мбайт
Видеокарта	32 Мбайт
Жесткий диск	60–80 Гбайт
Привод DVD-ROM	LITE ON, 16x/48x
Сетевая карта	3COM, 10/100 Мбит
Монитор	Samsung, 15 дюймов
Корпус	Midi Tower, 350 Вт
UPS	SMART APC, 450 Вт

Таблица 16.2. Пример конфигурации сервера базы данных

Комплектующие	Конфигурация
Процессор	Dual Pentium XEON
Оперативная память	4096 Мбайт
Видеокарта	32 Мбайт
Жесткие диски	SCSI Raid, 320 Гбайт; IDE, 400 Гбайт
Привод DVD-RW	LITE ON
Сетевая карта	3COM, 100 Мбит
Корпус	Server, 2x400 Вт
UPS	SMART APC, 1000 Вт

Таблица 16.3. Пример конфигурации сервера приложений

Комплектующие	Конфигурация
Процессор	Pentium IV, 3,2 ГГц
Оперативная память	2048 Мбайт
Видеокарта	32 Мбайт
Жесткий диск	SCSI Raid, 120 Гбайт
Привод DVD-ROM	LITE ON, 16x/48x
Сетевая карта	3COM, 100 Мбит
Монитор	Samsung, 17 дюймов
Корпус	Big Tower, 400 Вт
UPS	SMART APC, 600–1000 Вт

Таблица 16.4. Пример конфигурации файл-сервера

Комплектующие	Конфигурация
Процессор	Pentium IV, 2,6 ГГц
Оперативная память	2048 Мбайт
Видеокарта	32 Мбайт
Жесткие диски	SCSI Raid, 320 Гбайт; IDE, 200 Гбайт
Привод DVD-RW	LITE ON
Сетевая карта	3COM, 100 Мбит
Корпус	Full Tower, 2x400 Вт
UPS	SMART APC, 1000 Вт

Таблица 16.5. Пример конфигурации почтового сервера, интернет-шлюза

Комплектующие	Конфигурация
Процессор	Pentium IV, 2,4 ГГц
Оперативная память	1024–2048 Мбайт
Видеокарта	64–128 Мбайт
Жесткий диск	IDE, 80–300 Гбайт
Привод DVD-RW	LITE ON
Сетевая карта	3COM, 100 Мбит
Монитор	Samsung, 17 дюймов
Корпус	Midi Tower, 400 Вт
UPS	APC, 450–600 Вт

16.2. Создание домена

В качестве операционной системы, устанавливаемой на управляющий компьютер, будем использовать Microsoft Windows 2003 Server. Это одна из последних серверных операционных систем семейства Windows, которая зарекомендовала себя как устойчивая платформа, обеспечивающая корректную работу всех системных служб, необходимых для функционирования локальной сети любой сложности. Windows 2003 Server имеет набор мощных компонентов, каждый из которых отвечает за свой участок администрирования сети, что позволяет эффективно организовывать все нужные правила и настройки.

Если планируется объединять в сеть более 20 компьютеров, выбор операционной системы Microsoft Windows 2003 Server полностью оправдан. По этой причине остановимся более подробно на некоторых административных утилитах, которые вам, безусловно, придется использовать для настройки учетных записей пользователей и их прав.

Создание домена — важный шаг при настройке сети. Если коротко, то домен — управляющий компьютер, позволяющий использовать всю мощь администрирования доступа пользователя к ресурсам сети. Наиболее важными компонентами такого управления являются механизмы Active Directory, DNS- и DHCP-сервер. Для создания домена вам понадобится компакт-диск с дистрибутивом операционной системы.

Создать домен просто. Для этого достаточно воспользоваться мастером управления сервером, который появляется каждый раз при загрузке операционной системы (рис. 16.1).

Поскольку изначально операционная система не настроена на какое-то конкретное использование, чтобы научить ее быть доменом, необходимо добавить новую роль. Для этого нажмите кнопку **Добавить или удалить роль**.

Прежде чем продолжить работу, мастер настройки сервера предложит вам проверить готовность к этому вашего компьютера. Внимательно прочтите и рассмотрите каждый пункт. Для продолжения нажмите кнопку **Далее**.

Далее мастер произведет проверку существующих подключений, чтобы составить себе картину последующих действий. Это не займет много времени, поэтому дождитесь окончания процесса.

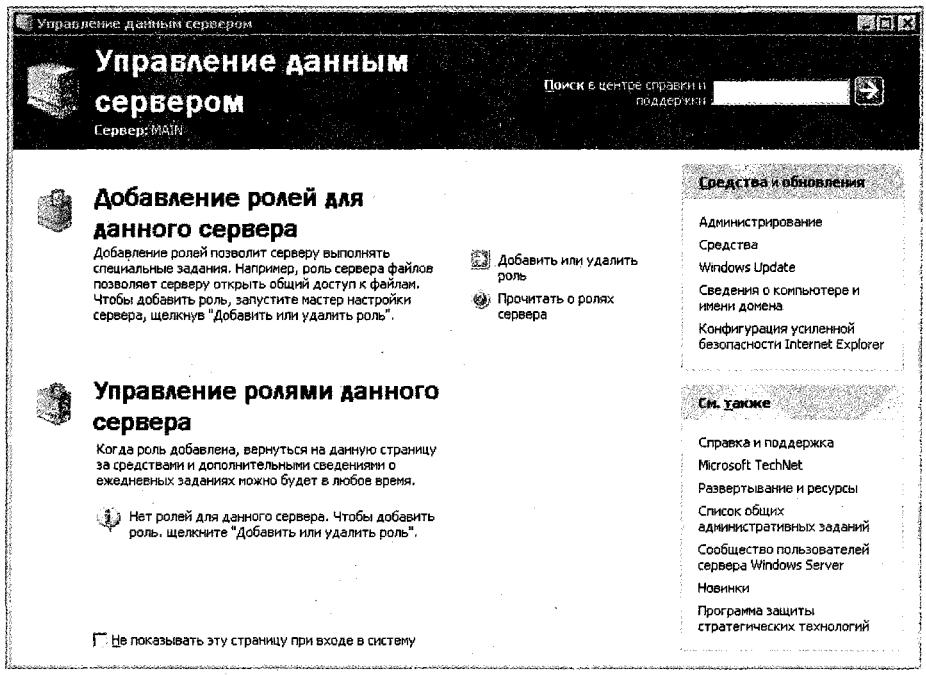


Рис. 16.1. Окно Управление сервером

Следующий шаг — выбор варианта настройки сервера. Поскольку мы хотим сделать компьютер доменом и он пока что один в сети, рекомендуется выбирать вариант **Типовая настройка для первого сервера**. Сюда входят все нужные нам механизмы и службы. Отметив первую позицию, нажимаем кнопку **Далее**.

Далее вам предложат ввести имя домена, оно будет отображаться в сети. Следуйте рекомендациям и обязательно оставьте слово `local` в названии домена.

ВНИМАНИЕ

Имя домена должно отличаться от имени данного компьютера. В противном случае мастер обнаружит конфликт и предложит альтернативное имя.

Для продолжения нажмите кнопку **Далее**.

В следующем окне (рис. 16.2) вам предложат указать имя домена, которое будет отображаться для рабочих компьютеров, на которых установлена операционная систем Windows ниже версии 2000 (например, Windows 98). Обычно имя не меняют, поэтому просто нажмите кнопку **Далее** для продолжения работы мастера.

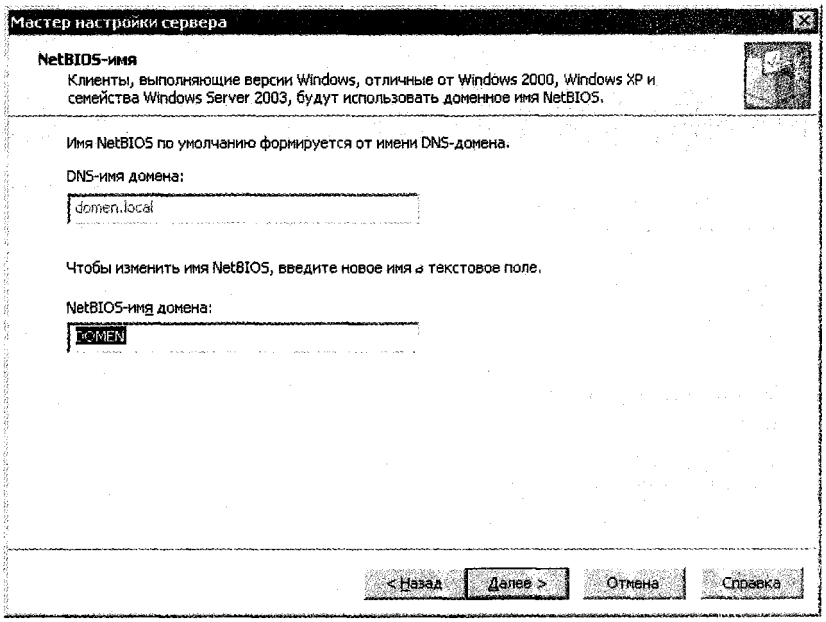


Рис. 16.2. Подтверждаем доменное имя

После этого мастер выдаст окно с итоговой информацией о компонентах, которые будут установлены. Для продолжения нажмите кнопку **Далее**.

Далее мастер предупредит вас, что в процессе установки может потребоваться перезагрузка компьютера, и попросит компакт-диск с дистрибутивом операционной системы. Установите диск в привод и нажмите кнопку **ОК** для продолжения. В случае если диска нет, можно указать любое другое место, где лежит дистрибутив. Для этого также нажмите кнопку **ОК** и укажите расположение нужной папки.

Процесс установки занимает некоторое время. При этом вы можете наблюдать текущий этап выполнения установки, запуск процессов копирования файлов и т. д. Вам остается только дождаться окончания процесса установки.

После автоматической перезагрузки компьютера и запуска операционной системы появится окно с информацией обо всех процессах, которые выполнил мастер настройки сервера. Для продолжения нажмите кнопку **Далее** и в следующем окне — кнопку **Готово**.

После этого загрузится уже знакомое окно настройки сервера, но теперь оно содержит ссылки на настройку установленных компонентов (рис. 16.3).

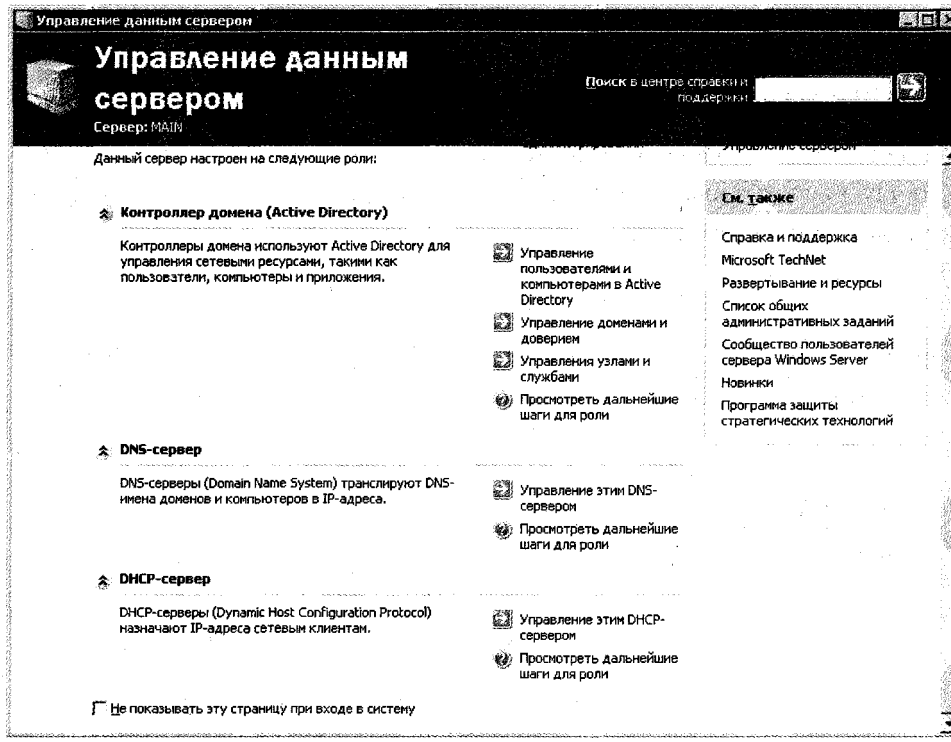


Рис. 16.3. Измененное окно настройки сервера

16.3. Использование DNS-сервера

DNS-сервер (Domain Name System, доменная система имен) используется для взаимодействия с установленными протоколами передачи данных, а именно: он позволяет осуществлять привязку имени компьютера к его IP-адресу. Связано это с тем, что, например, протоколу TCP-IP для обнаружения компьютера в сети, будь то локальная сеть или Интернет, требуется именно IP-адрес машины, а не его логическое имя.

Когда-то, в древние времена, функции DNS-сервера, если так можно выразиться, выполнял протокол NetBIOS, то есть с его помощью можно было искать компьютер, ориентируясь на его логическое имя. По понятным причинам эта технология давно устарела, поскольку имела больше недостатков, нежели преимуществ. Тем не менее еще до сих пор встречается связка TCP/IP и NetBIOS. Однако даже сам автор NetBIOS, коим является компания Microsoft, отказался от его использования и внедрил технологию DNS. Кроме того, DNS позво-

ляет организовать эффективную работу системных служб Интернета, что гарантирует доступ к веб-ресурсам, даже если адрес страницы меняется (требуется всего несколько часов, чтобы новый адрес заработал).

Если коротко, то DNS-сервер представляет собой древообразную структуру, состоящую из нескольких веток, основными из которых являются **Зона прямого просмотра** и **Зона обратного просмотра**. Обе содержат списки соответствий имени компьютера и его адреса (рис. 16.4).

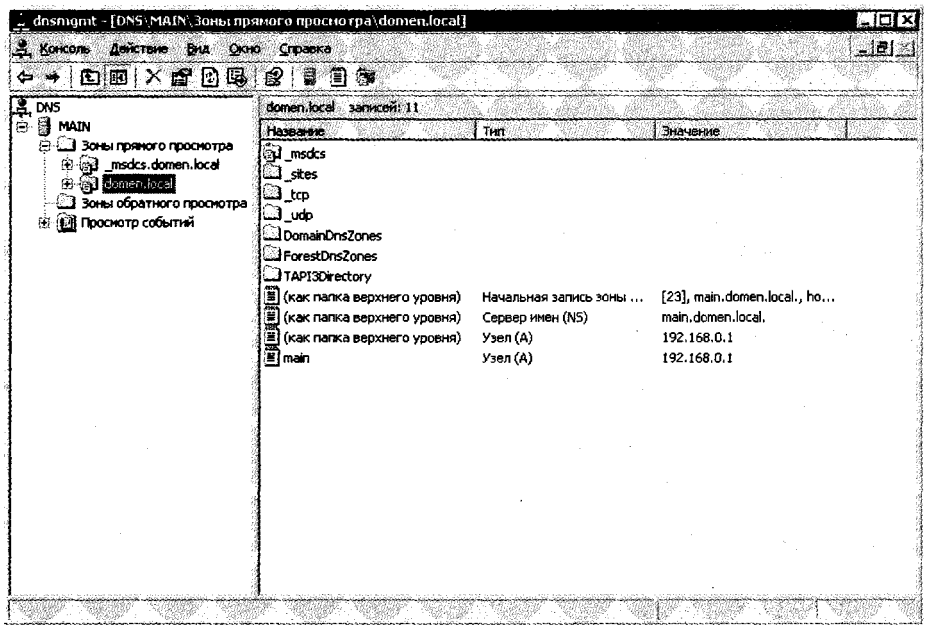


Рис. 16.4. Структура DNS-сервера

Списки соответствий создаются автоматически, обновляя данные, когда компьютер входит в сеть. При этом DNS взаимодействует с DHCP-сервером, что позволяет всегда содержать и обновлять актуальные данные. Поэтому вашего участия в настройке DNS-сервера не требуется.

16.4. Использование DHCP-сервера

DHCP-сервер (Dynamic Host Configuration Protocol, протокол динамического конфигурирования IP-адреса компьютера) — механизм, контролирующий регистрацию компьютера в сети с последующей выдачей ему IP-адреса.

Выдача IP-адресов происходит по определенным правилам. Так, изначально существуют области адресов (набор), которые могут быть задействованы для нужд локальной сети. Их количество зависит от наличия различных сегментов сети.

Область адресов распределяется между следующими группами.

- **Пул адресов.** Их составляют адреса, которые получаются путем вычитания из общей области адресов, которые входят в области исключений.
- **Арендованные адреса.** В данную группу попадают адреса, которые в данный момент арендованы подключенными к сети компьютерами или компьютерами, недавно подключавшимися к сети.
- **Резервирование.** В эту группу входят адреса, которые выделяются в постоянное пользование конкретным компьютерам сети. При этом конкретный адрес выделяется конкретному компьютеру, что жестко прописывается при настройке DHCP-сервера.

ПРИМЕЧАНИЕ

Из видеоурока «Урок 16.1. Настройка DHCP-сервера», который находится на компакт-диске, прилагаемом к книге, вы узнаете, как произвести настройку DHCP-сервера.

Теперь давайте рассмотрим, каким образом настраиваются группы адресов.

Область адресов

При инсталляции домена DHCP-сервер устанавливается автоматически. При этом создается одна область адресов в диапазоне 192.168.0.0–192.168.0.254. Это позволяет подключить к сети 254 компьютера, в том числе и управляющие серверы. Что касается DNS-сервера, то он автоматически привязывается к IP-адресу домена сети, на котором установлен DNS-сервер, то есть 192.168.0.1. Из соображения, что в сети могут существовать и другие служебные серверы, область адресов, доступная для свободного использования, уменьшается на 10 единиц. Поэтому реально область адресов состоит из адресов диапазона 192.168.0.10–192.168.0.254.

В этом очень легко убедиться, если вызвать свойства области. Для этого щелкните правой кнопкой мыши на позиции **Область** и выберите в появившемся меню пункт **Свойства**. В результате появится окно, показанное на рис. 16.5. Обратите внимание на поле **Начальный IP-адрес:**, адрес действительно начинается с числа 10.

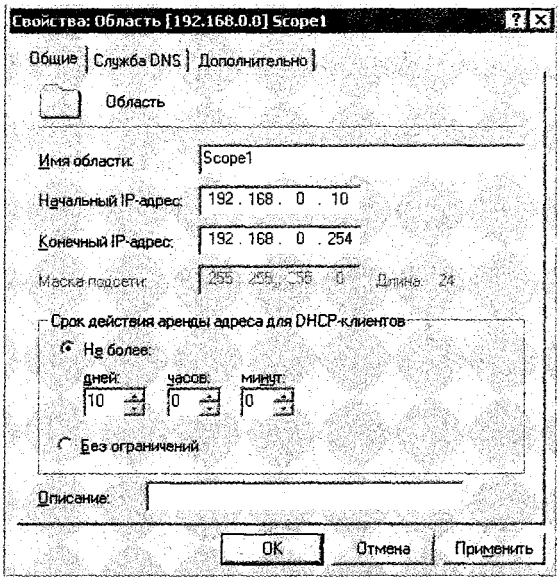


Рис. 16.5. Окно свойств области

Как бы там ни было, в данном окне вы можете вносить свои изменения. Так, если вам не нравится выделенный диапазон адресов области, можете его изменить на более узкий. Здесь же вы можете указать срок резервирования адреса. По умолчанию — 10 дней 3 часа. Если того требует ситуация, измените его на свое усмотрение или вообще отключите ограничения, установив переключатель **Без ограничений**. Обычно параметры по умолчанию позволяют функционировать сети в нормальном режиме и их можно не трогать.

Если вы перейдете на вкладку **Служба DNS**, у вас появится возможность настроить режим обновления списка соответствий имен и адресов DNS (рис. 16.6). По умолчанию установлено обновление только по запросу DHCP-клиента, что позволяет сократить трафик сети между сервером и рабочими станциями и разгрузить управляющий компьютер.

На вкладке **Дополнительно** (рис. 16.7) вы можете указать, как назначать динамические адреса разным клиентам. Под клиентом здесь понимается компьютер, использующий протокол DHCP или BOOTP для регистрации в сети. Ранее мы не рассматривали BOOTP-протокол, поскольку он является лишь прародителем DHCP-протокола и имеет более ограниченные возможности загрузки. В частности, BOOTP-протокол используется для подключения и регистрации в сети бездисковых компьютеров.

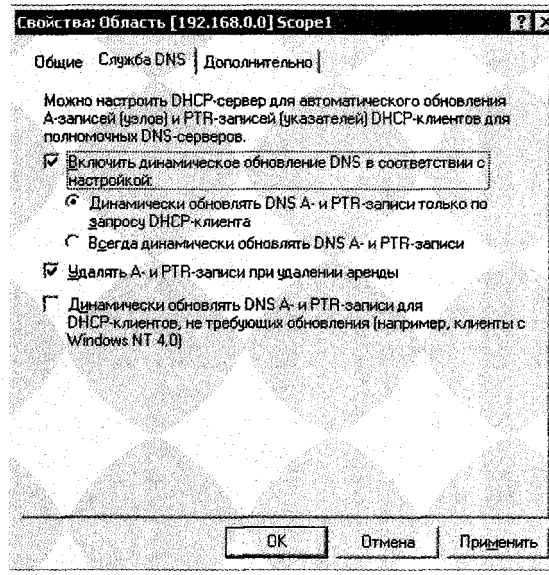


Рис. 16.6. Настраиваем обновление списка соответствий

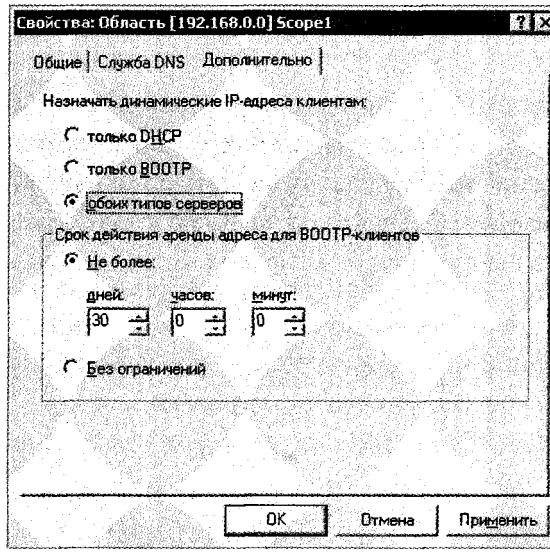


Рис. 16.7. Настраиваем способ выделения динамических адресов

Таким образом, если у вас в сети имеются подобного рода компьютеры, а BOOTP-сервер в сети отсутствует, его роль с легкостью может выполнять имеющийся DHCP-сервер. В таком случае на этой вкладке вы можете указать время аренды адреса или выбрать режим без ограничения времени аренды.

По умолчанию динамические адреса раздаются всем клиентам. Если в сети чужих клиентов нет, лучше установить переключатель **Назначать динамические IP-адреса клиентам** в положение **только DHCP**.

На этом настройка области адресов завершена.

Пул адресов

Пул адресов содержит в себе диапазоны адресов, которые нельзя использовать по разным причинам: эти адреса отводятся для серверов, сетевых принтеров, маршрутизаторов и коммутаторов, точек доступа и т. д.

Визуально это список адресов с указанными диапазонами. При этом в верхней части окна показывается весь диапазон адресов, а затем каждая новая запись отображает адрес или диапазон, который исключается из общедоступного списка.

Чтобы добавить нужный адрес или диапазон адресов в список исключений, достаточно щелкнуть правой кнопкой мыши в правой части окна и в появившемся меню выбрать пункт **Диапазон исключения**.

После этого появляется окно, в котором нужно указать начальный и конечный адреса диапазона, которые будут исключены из области аренды, и затем нажать кнопку **Добавить**.

Арендованные адреса

В группе **Арендованные адреса** (рис. 16.8) отображаются все адреса, которые на текущий момент выданы в аренду клиентам.

Количество этих адресов зависит от числа компьютеров в сети. В списке отображается арендованный IP-адрес, логическое имя машины, дата окончания срока аренды, тип протокола, уникальный идентификатор и комментарий.

Данный список наполняется автоматически при получении компьютером IP-адреса. Единственное, что вы можете делать с этим списком, — удалять записи. Для этого просто щелкните на нужной строке правой кнопкой мыши и выберите пункт **Удалить**.

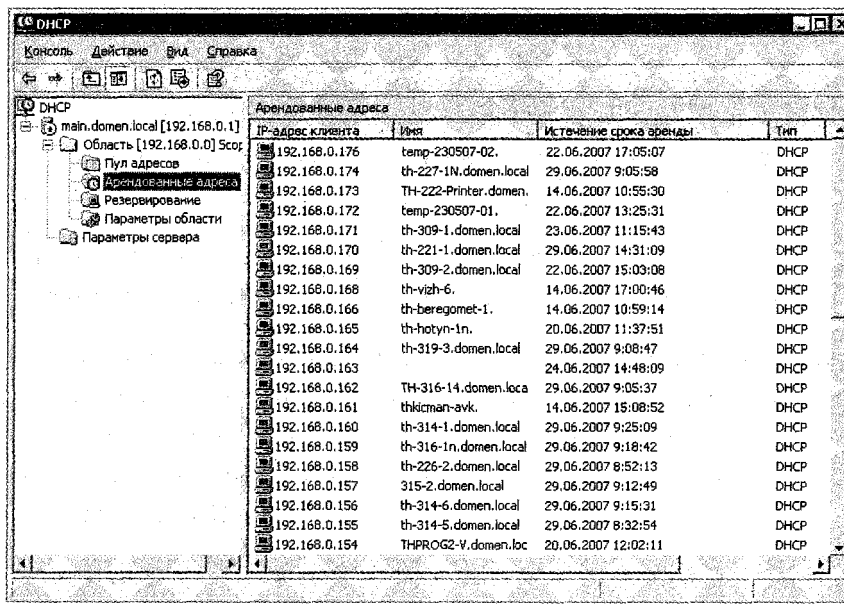


Рис. 16.8. Список арендованных адресов

Резервирование

В список **Резервирование** добавляются адреса из пула адресов, которые необходимо раз и навсегда закрепить за каким-либо устройством. Например, подобным образом можно поступить с серверами или другим важным оборудованием.

Резервирование гарантирует выдачу указанного IP-адреса устройству, у которого логическое имя и MAC-адрес совпадают с указанными при вводе данными.

Чтобы зарезервировать адрес, выберите в верхнем меню **Действие ▸ Добавить резервирование**. Далее в появившемся окне (рис. 16.9) введите имя компьютера, требуемый IP-адрес, MAC-адрес сетевого адаптера, описание и тип используемого для идентификации протокола. После нажатия кнопки **Добавить** система произведет анализ введенного MAC-адреса и, если он указан неверно, выдаст предупреждение.

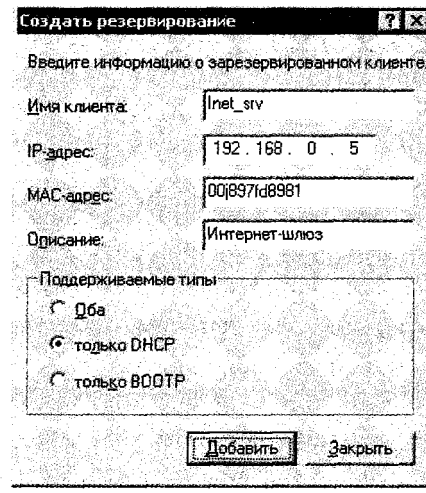


Рис. 16.9. Вводим данные для резервирования адреса

Параметры области

Под параметрами области следует понимать данные, сведения о которых отсылает DHCP-сервер по требованию DHCP-клиента, который в этой области находится. По умолчанию установлен лишь параметр, позволяющий узнавать адрес DNS-сервера. Кроме того, можно настроить более 60 дополнительных параметров.

Чтобы добавить параметр, щелкните правой кнопкой мыши на позиции **Параметры области** и в появившемся меню выберите пункт **Настроить параметры**.

В результате появится окно, содержащее список параметров области. Чтобы добавить новый параметр, просто установите нужный флажок. Каждый из параметров, в свою очередь, может иметь один или несколько настраиваемых параметров. Например, если вы установите флажок **DNS-имя домена**, вам необходимо будет в области **Строковое значение** указать полное DNS-имя сервера.

На вкладке **Дополнительно** можно настроить некоторые из уже установленных параметров области.

Параметры сервера

Параметры сервера идентичны параметрам области с той лишь разницей, что, добавив новый параметр сервера, вы тем самым автоматически добавляете аналогичный во все имеющиеся области.

16.5. Использование механизма Active Directory

Чтобы добавлять и настраивать подразделения, группы, компьютеры пользователей и многие другие административные объекты, в Microsoft Windows 2003 Server существует мощный механизм — Active Directory.

В дальнейшем, если вы возьмете на себя обязанности сетевого администратора, вам придется достаточно часто пользоваться им, поэтому рассмотрим более подробно такие операции, как создание подразделений, групп, пользователей и настройка их прав.

ПРИМЕЧАНИЕ

Видеоурок «Урок 16.2. Настройка Active Directory», который находится на компакт-диске, прилагаемом к книге, демонстрирует практический пример использования системной компоненты Active Directory.

Прежде всего запустите Active Directory. Для этого нажмите кнопку **Управление пользователями и компьютерами в Active Directory** (см. рис. 16.3) или выберите **Пуск ▸ Программы ▸ Администрирование ▸ Active Directory — пользователи и компьютеры**.

В результате откроется окно **Active Directory Users and Computers** (рис. 16.10).

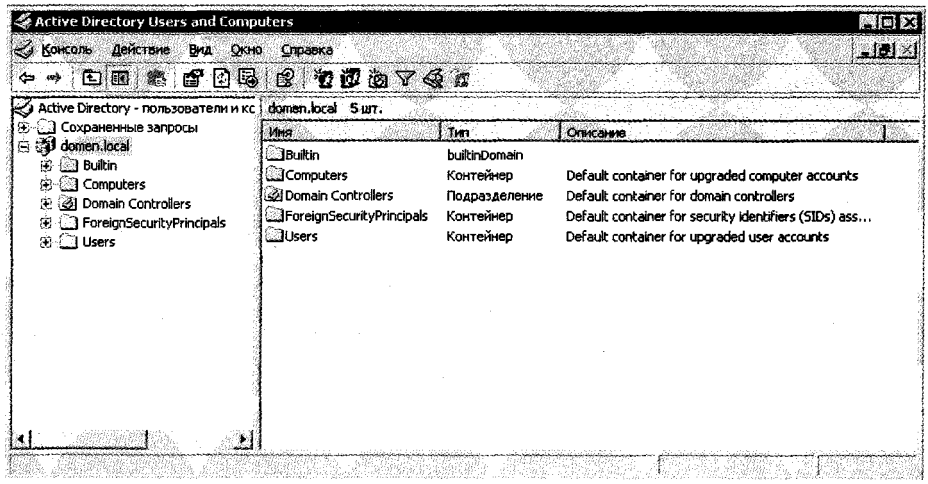


Рис. 16.10. Приложение Active Directory — пользователи и компьютеры

В нем отображается не только домен, объекты которого редактируются, но и группы и подразделения, содержащие некоторые стандартные административные объекты, такие как встроенные учетные записи и пользователи. Отображение выполнено в виде удобной древовидной структуры.

Ниже описан пример создания пользователя с добавлением его в группу и подразделение.

Создание подразделений

Подразделение внешне выглядит как папка, чем, собственно, и является. Основное его предназначение — разбиение всех создаваемых объектов на категории с целью их структуризации.

С применением подразделений весь объект выглядит как дерево, каждая ветка которого имеет собственную структуру.

Чтобы создать новое подразделение, нужно выбрать объект, к которому оно будет принадлежать.

ВНИМАНИЕ

При создании нового объекта не забывайте, что вы работаете с деревом. Поэтому сначала нужно указывать объект, к которому будет добавляться новая запись, а затем уже выбирать нужное действие.

Таким образом, выделив название домена, щелкните правой кнопкой мыши и в появившемся меню выполните команду **Создать ▸ Подразделение**.

При этом появится окно, в котором нужно ввести название подразделения, не забывайте, что оно должно обобщать все объекты, которые в нем будут находиться.

После нажатия кнопки **OK** будет создано подразделение с выбранным названием (в данном примере — `Бухгалтерия`), которое впоследствии можно увидеть в левой части окна **Active Directory Users and Computers**.

Подразделений может быть сколько угодно, но лучше этим не увлекаться, в противном случае вы просто не сможете найти нужного пользователя в изобилии созданных подразделений. Придерживайтесь правила: строго, функционально, удобно!

Создание группы

Использование группы выгодно в том случае, когда требуется настроить одинаковые права для нескольких пользователей. Например, определенные пользователи должны запускать программу «1С:Предприятие». Вместо того чтобы искать и подключать каждого из пользователей с последующей расстановкой прав доступа, необходимо просто заранее добавить их в одну группу, которую затем следует подставить в нужное место, и установить ее права.

Таким образом, приступим к созданию группы с размещением ее в созданном ранее подразделении **Бухгалтерия**.

Как и в предыдущем случае, сначала следует выделить нужный объект — подразделение **Бухгалтерия**.

Затем щелкните правой кнопкой мыши и выполните в контекстном меню команду **Создать ▸ Группа**.

В результате откроется окно, в котором вводится имя создаваемой группы (рис. 16.11).

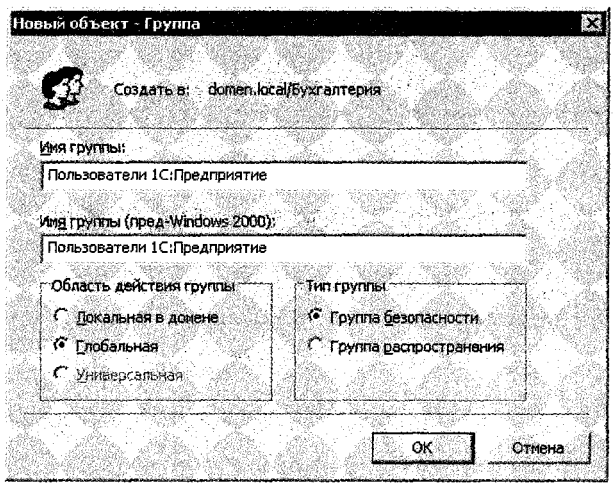


Рис. 16.11. Вводим имя группы

После нажатия кнопки **OK** группа будет добавлена в указанное подразделение.

Как и подразделений, групп может быть любое количество.

Создание учетной записи пользователя

Следующий шаг — добавление пользователей.

Воспользуемся данными из предыдущего примера. Чтобы создать учетную запись пользователя, поместить его в подразделение **Бухгалтерия**, выполните следующие действия.

Выделите объект `Бухгалтерия` и нажмите правую кнопку мыши. Затем в появившемся контекстном меню выполните команду **Создать ▸ Пользователь**.

После этого в появившемся окне введите информацию о пользователе: имя, фамилию, отчество, логин входа в домен (рис. 16.12).

ПРИМЕЧАНИЕ

Полное имя формируется автоматически после ввода имени и фамилии пользователя, однако оно начинается с имени (в данном примере — Александр Семенович Петров).

Согласно американским стандартам, полное имя начинается с имени пользователя и заканчивается фамилией. Согласно славянским — на первом месте стоит фамилия, а в конце — отчество. Поэтому, если вы хотите видеть привыч-

ное написание, вам придется вручную изменить расположение его составляющих в поле **Полное имя**. Мало того, именно так и следует сделать, поскольку в дальнейшем вы в любое время сможете отсортировать пользователей с целью поиска конкретного из них по фамилии.

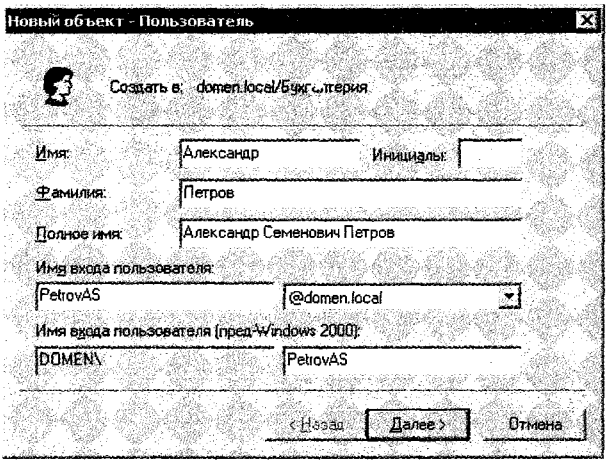


Рис. 16.12. Вводим регистрационные данные пользователя

После нажатия кнопки **Далее** появится новое окно, в котором нужно указать пароль, повторив его дважды. Также можно задействовать следующие параметры.

- **Требовать смену пароля при следующем входе в систему.** Обычно смена пароля пользователя запрашивается автоматически по истечении выбранного периода, например календарного месяца. Система сообщает пользователю, что срок действия пароля закончен и требуется ввести новый. Чтобы заставить пользователя сменить пароль преждевременно, установите данный флажок.
- **Запретить смену пароля пользователем.** Пользователь может сам менять пароль как планово, так и преждевременно. Чтобы запретить ему это делать, установите здесь флажок.
- **Срок действия пароля не ограничен.** Использование данного параметра подразумевает, что пароль пользователя не меняется в течение всего времени существования его учетной записи в Active Directory или до тех пор, пока этот параметр не будет отменен.
- **Отключить учетную запись.** Установленный флажок позволяет временно отключить учетную запись пользователя, не удаляя ее из Active Directory. В любой момент статус учетной записи может быть восстановлен.

После нажатия кнопки **OK** создается учетная запись пользователя, которая прописывается в выбранное подразделение, в чем можно убедиться, просмотрев его содержимое (в нашем случае это подразделение **Бухгалтерия** (рис. 16.13)).

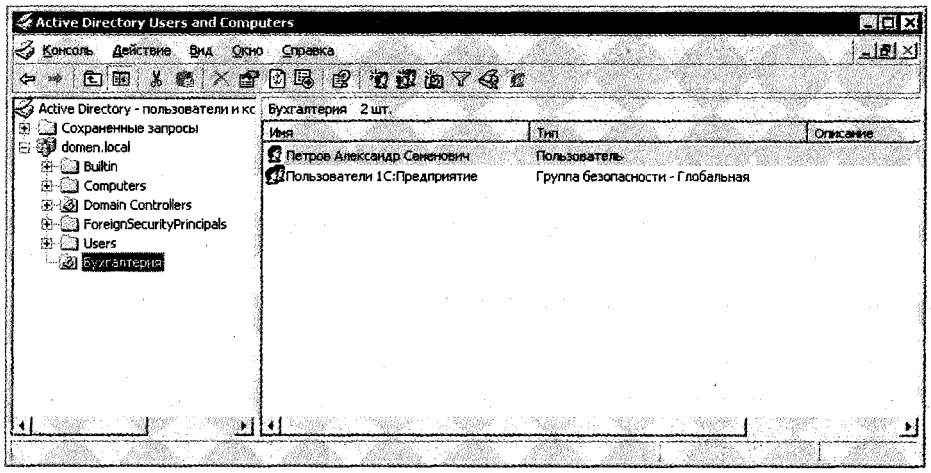


Рис. 16.13. Создание учетной записи пользователя завершено

ПРИМЕЧАНИЕ

По умолчанию при вводе пароля доступа действуют определенные правила. Так, пароль обязательно должен содержать цифру, букву и неалфавитный символ. При этом все вводится в латинской раскладке клавиатуры и длина пароля должна быть не менее 7 знаков, например, 38ik$sb. Также в пароле не должна участвовать даже малая часть логина. В дальнейшем, если это правило вас утомляет, ограничение можно убрать с помощью настройки механизма Политика безопасности домена.

Теперь, чтобы указать принадлежность пользователя к группе **Пользователи 1С:Предприятие**, сделайте следующее: щелкните правой кнопкой мыши на группе **Пользователи 1С:Предприятие** и в появившемся меню выберите пункт **Свойства**.

В результате появится окно свойств группы, содержащее несколько вкладок. Чтобы добавить в группу пользователя, перейдите на вкладку **Члены группы** и нажмите кнопку **Добавить**.

В появившемся окне (рис. 16.14) необходимо указать пользователей, которых нужно добавить в группу. По умолчанию система ориентирована на то, что вы помните логины пользователей и сможете набрать их прямо в этом окне. Конечно, если пользователей немного, такой подход вполне оправдан. Когда же пользователей много, запомнить их логины трудно и требуется механизм для облегчения их поиска и ввода в необходимое поле окна. Воспользуемся этим механизмом.

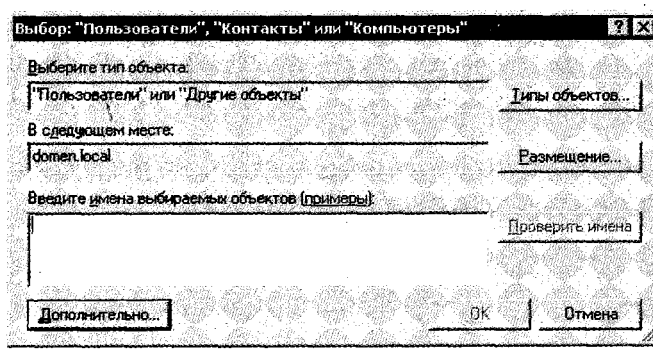


Рис. 16.14. Окно выбора пользователя

Для начала нажимаем кнопку **Дополнительно**.

Это приведет к расширению открытого ранее окна (рис. 16.15). В нашем случае появилась полезная кнопка **Поиск**, нажав ее, получаем список всех объектов в указанном домене. Теперь остается только выбрать нужных пользователей и нажать кнопку **ОК** или дважды щелкнуть кнопкой мыши.

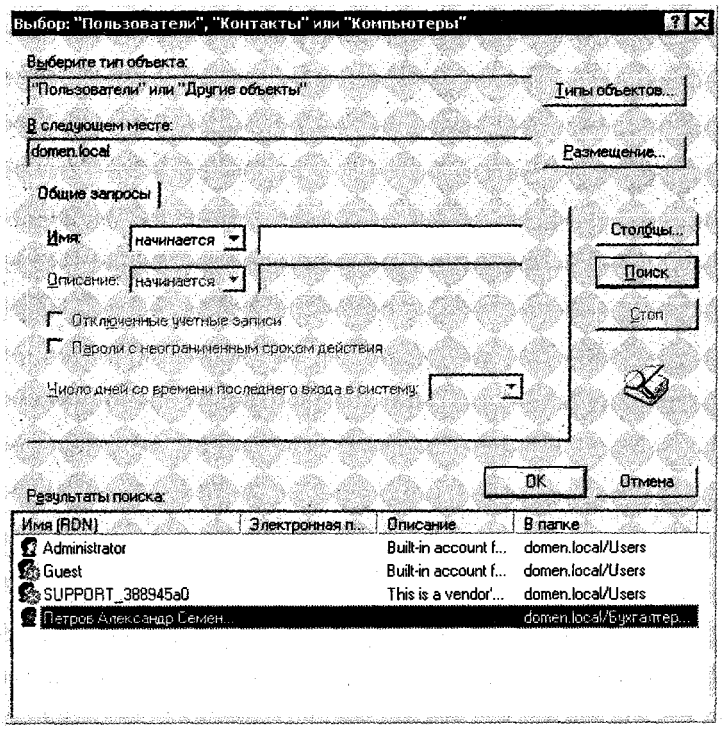


Рис. 16.15. Дополненное окно выбора пользователей

В результате в окне, показанном на рис. 16.14, появятся выбранные пользователи. Нажав кнопку **ОК**, вы добавите указанных пользователей в группу **Пользователи 1С:Предприятие**. Операция завершена.

16.6. Настройка общего доступа

Основное преимущество локальной сети заключается в использовании общих ресурсов — файлов, приложений, принтеров и т. п. Поэтому сейчас речь пойдет о том, каким образом создавать ресурсы и распределять доступ к ним.

Общие ресурсы могут быть на любом компьютере, в том числе и на домене. В последнем случае, чтобы оптимизировать доступ к этим ресурсам, дополнительно производится настройка домена до уровня файлового сервера. Хотя ничто не мешает просто создать общий ресурс и настроить необходимый доступ.

ПРИМЕЧАНИЕ

Из видеоурока «Урок 16.3. Настройка общего доступа в Windows 2003 Server», который находится на компакт-диске, прилагаемом к книге, вы узнаете, как настроить общий доступ к ресурсам.

Чтобы организовать доступ к папке, нужно в любой из оболочек **Проводника** выделить ее и щелкнуть правой кнопкой мыши. Далее в появившемся меню выбрать пункт **Общий доступ и безопасность**.

В результате откроется окно (рис. 16.16), где нужно указать сетевое имя, под которым этот ресурс будет виден в сети, и добавить пользователей, которые с ним смогут работать.

Прежде всего установите переключатель в положение **Открыть общий доступ к этой папке**. Указав название ресурса, определите, нужно ли обеспечить доступ к ресурсам одновременно многим пользователям или лучше поставить ограничение на количество подключений. Это зависит от типа ресурса. Если в папке находится база данных, с которой работают многие пользователи, придется сделать неограниченный доступ многих пользователей. Если же это папка с дистрибутивами или фильмами, доступ к ней можно ограничить, например, пятью одновременно подключенными пользователями. Выбирать вам, однако не забывайте, что каждое лишнее подключение не только отнимает ресурсы компьютера, но и увеличивает трафик в сети.

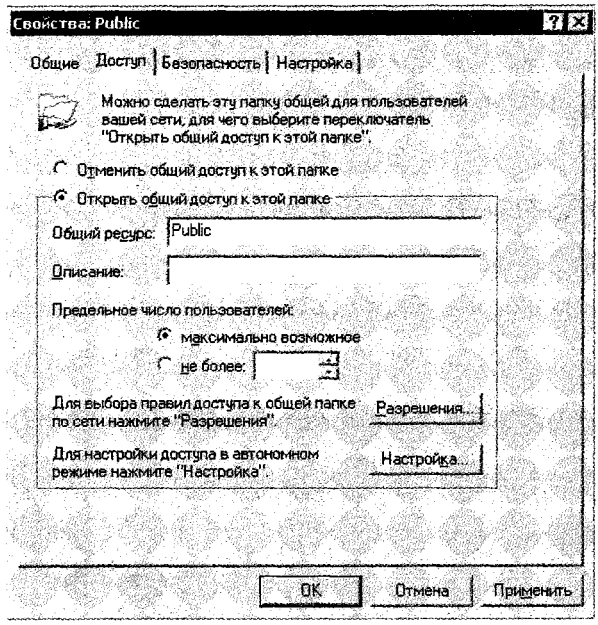


Рис. 16.16. Указываем имя общего ресурса и добавляем пользователей

Следующий шаг — распределение прав пользователей.

После нажатия кнопки **Разрешения** открывается окно, показанное на рис. 16.17. По умолчанию к ресурсу могут подключиться все пользователи, о чем свидетельствует группа с названием **Все**. Однако доступ ограничен лишь возможностью чтения. Для того чтобы тонко настроить разрешения, например одним пользователям предоставить доступ только на чтение, а другим — и на чтение, и на изменения, необходимо сначала добавить нужных пользователей и группы и затем устанавливать или снимать флажки **Разрешить** и **Запретить**.

Для того чтобы добавить объект, используйте кнопку **Добавить**.

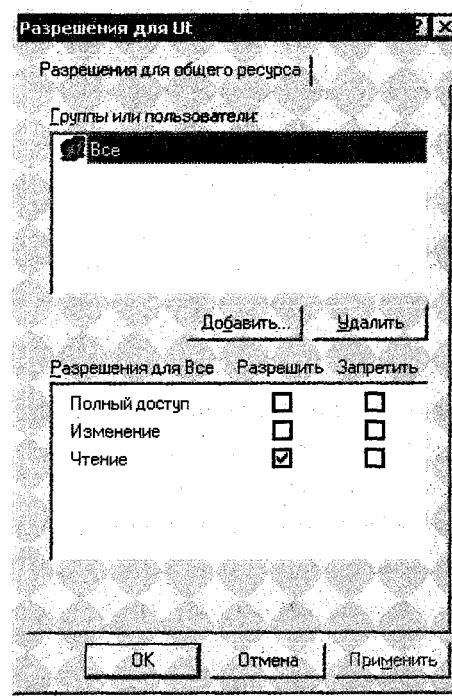


Рис. 16.17. Список пользователей ресурса

В результате откроется окно, заполнение которого мы уже рассматривали ранее (см. материал о добавлении учетных записей пользователей).

После того как пользователи будут добавлены и настроены их права доступа к ресурсу, нажмите кнопку **ОК**. Далее система произведет все необходимые изменения в реестре операционной системы и общий ресурс станет доступным выбранным пользователям.

В среде **Проводника** папка с общим доступом будет отображаться как папка с изображением держащей ее руки (рис. 16.18).

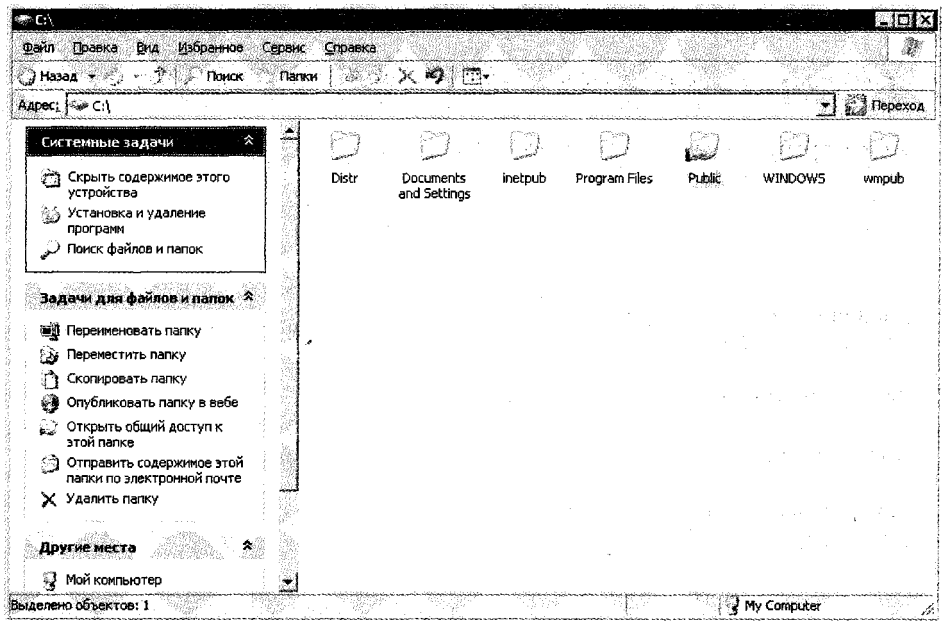


Рис. 16.18. Общий ресурс создан

Аналогичным образом можно и отменить общий доступ. Для этого в окне, представленном на рис. 16.16, нужно установить переключатель в положение **Отменить общий доступ к этой папке**.

Определение общего доступа к принтеру происходит аналогичным способом.

Количество общих ресурсов может быть разным, но следует помнить: чем больше доступ к компьютеру, тем сложнее его контролировать. Кроме того, не забывайте, что доступ к ресурсу должен быть постоянным (не нужно без причины перегружать компьютер), в противном случае все это теряет смысл...

Глава 17

Установка и подключение сетевого оборудования

- Подключение концентратора или коммутатора
- Подключение точки доступа
- Подключение маршрутизатора
- Установка сетевого адаптера и драйверов

Итак, сеть спроектирована, выбраны топология и стандарт, проложена проводка. Мало того, на управляющем компьютере уже установлена и настроена сетевая операционная система. Осталось дело за малым — за расстановкой и подключением необходимого сетевого оборудования и проверкой связи с сервером и другими компьютерами.

Порядок подключения сетевых устройств особого значения не имеет. Однако лучше сначала подключить точку доступа, маршрутизатор, модем, концентратор и в последнюю очередь — компьютеры. Такая последовательность позволяет подсоединять машины к уже функционирующей сети, что значительно облегчит их настройку и выявление неисправностей при подключении.

17.1. Подключение концентратора или коммутатора

Концентратор — первое устройство, которое отвечает за соединение группы компьютеров в некоторую проводную мини-сеть (рабочую группу).

ПРИМЕЧАНИЕ

Основная функция концентратора — получение сигнала через один порт, восстановление его и передача на остальные порты. Таким образом, имея концентратор, уже можно организовать локальную сеть.

Концентраторы могут иметь от 8 до 36 портов, один из которых служит для подключения к другому концентратору или маршрутизатору. Этот порт называется uplink-порт и отличается от других тем, что для соединения через него используют кроссовер-кабель. Многие современные концентраторы сами производят перенаправление контактов на аппаратном уровне, что позволяет использовать обычный кабель.

Особенностью действия концентраторов является их чрезмерная активность, приводящая к засорению трафика ненужными пакетами. Поэтому использование лишь одного концентратора при большом количестве подключенных компьютеров сопряжено с определенными трудностями. Для того чтобы избавиться от подобного эффекта, часто вместо концентраторов используют коммутаторы.

Если планируется подключить всего несколько компьютеров, вам с лихвой хватит одного восьмипортового концентратора. Поскольку количество компью-

теров небольшое, создаваемый концентратором шум не будет настолько сильным, чтобы использовать дополнительное сетевое оборудование.

Со временем количество подключаемых компьютеров, возможно, будет увеличиваться. Это заставит вас использовать еще один концентратор, соединив его с предыдущим через uplink-порт, или заменить предыдущий на концентратор с большим количеством портов.

Таким образом, если сеть разрастается, то нужно только заботиться о расширении количества концентраторов или использовать более мощные устройства. Однако как только она достигнет критических размеров — около 15–20 компьютеров, следует задуматься о введении в действие маршрутизатора или коммутатора, иначе за счет возникающего трафика производительность сети заметно уменьшится.

Установка и подключение коммутатора не должны вызвать каких-либо затруднений. Главное — найти место, где устройство будет расположено, и хорошо его закрепить. Особенно это касается случаев, когда коммутатор крепится на стену. Если используется монтажный шкаф, устройство просто фиксируется винтами к корпусу.

Подключение кабелей к концентратору или коммутатору осуществляется с таким расчетом, чтобы можно было легко отключить или подключить нужный кабель. Поэтому, если имеется такая возможность, подключайте кабели через одно гнездо.

ПРИМЕЧАНИЕ

Из видеоурока «Урок 17.1. Подключение кабеля на основе витой пары к коммутатору», который находится на компакт-диске, прилагаемом к книге, вы узнаете, как подключить готовые кабели, например, на основе витой пары к коммутатору.

После того как блок питания устройства подключен к сети переменного напряжения, оно готово к работе. Что касается концентратора, он способен сразу же начать работу без предварительной настройки. В случае же с коммутатором вам можете потребоваться предварительная настройка. Как минимум желательно установить ему зарезервированный в Active Directory IP-адрес, чтобы можно было в дальнейшем осуществлять удаленное управление устройством.

Чтобы настроить коммутатор, вам потребуется прямое подключение. Именно поэтому чаще всего коммутатор настраивается до его установки в монтажный шкаф или на стену. Хотя для этих целей можно использовать ноутбук.

Коммутатор программируется с использованием идущего в комплекте COM-шнура и соответствующего программного обеспечения. В случае отсутствия такового можно использовать системную утилиту **telnet**. Более детально параметры программирования должны быть описаны в документации к коммутатору.

17.2. Подключение точки доступа

Подключение точки доступа не вызывает никаких трудностей: достаточно подключить блок питания и вкрутить антенну. При этом ее можно расположить в любом месте, которое наилучшим образом подходит для организации надежной и быстрой связи с компьютерами сети (рис. 17.1).

Рис. 17.1. Примеры расположения точки доступа

По умолчанию точка доступа запрограммирована на работу в беспроводной сети. В любой момент пользователь может эти параметры просмотреть или поменять с помощью веб-браузера. Для этого достаточно подключить к компьютеру устройство и ввести в адресной строке браузера **http://192.168.0.50**. Но лучше всего при изменении параметров точки доступа подключить ее к маршрутизатору или даже к Ethernet-карте компьютера. Это позволит в любой момент получить доступ к ней, даже в случае, когда установлены такие параметры, при которых она не функционирует и, соответственно, не функционирует беспроводная сеть.

Поскольку адрес точки доступа может конфликтовать с адресацией в вашем домене, обязательно перепрограммируйте ее должным образом, присвоив ей заранее зарезервированный IP-адрес.

17.3. Подключение маршрутизатора

Маршрутизатор — это устройство, которое рангом выше концентратора или коммутатора. Он имеет мощнейшие механизмы фильтрации создаваемого всеми сетевыми устройствами трафика, а также средства управления пакетами. Маршрутизатор является незаменимым устройством в сети, насчитывающей более 20–30 компьютеров. Маршрутизатор также позволяет организовывать виртуальные сети и осуществляет маршрутизацию пакетов между ними.

Маршрутизатор имеет мощный анализатор трафика и взаимодействует с маршрутными протоколами, поэтому он всегда знает, что и кому предназначается. Это позволяет ему минимизировать трафик, направляя пакеты только между выбранными устройствами. Кроме того, в маршрутизаторе имеется возможность программной коррекции взаимосвязей подключенных к нему устройств.

Это устройство становится необходимым, когда сеть достигает критических размеров и грозит стать неуправляемой.

Принцип подсоединения маршрутизатора очень прост. Как правило, данное устройство имеет всего несколько портов, к которым подключают точки доступа, концентраторы или коммутаторы, отвечающие за работу отдельных веток сети или групп компьютеров.

Как и коммутатор или точка доступа, маршрутизатор также поддается программированию. Мало того, это обязательно следует сделать, если вы хотите иметь полный контроль над сетью.

Программирование маршрутизатора — достаточно сложный процесс. Как минимум требуется изменить IP-адрес устройства, добавить IP-адреса всех коммутаторов и точек доступа, чтобы можно было организовать эффективное взаимодействие между ними.

Поскольку маршрутизатор — одно из самых дорогостоящих устройств, он всегда устанавливается в изолированный монтажный шкаф или отдельное помещение, доступ к которому имеется только у определенных лиц. Кроме того, для подключения подобного рода устройств обязательно используйте блок бесперебойного питания.

17.4. Установка сетевого адаптера и драйверов

Сетевой адаптер — устройство, которое инициирует передачу или прием пакетов. Иначе говоря, это окно, через которое компьютер взаимодействует с другими машинами и устройствами сети.

Как вы уже знаете, сетевые адаптеры бывают внешние и внутренние (интегрированные в материнскую плату).

Внешние сетевые карты изготавливают в виде плат расширения, вставляющихся в слот на материнской плате (наиболее распространены), или устройств, подключаемых к USB-порту.

Основным слотом для подключения устройств такого рода является PCI. Он может работать на частотах 33 и 66 МГц и, согласно спецификациям, в широком диапазоне скоростей: начиная с 132 и заканчивая 528 Мбайт/с, чего вполне достаточно для работы в любой сети, будь то 10 или 1000 Мбит.

В последнее время практически все материнские платы имеют интегрированный сетевой адаптер. Это достаточно удобное решение, которое к тому же позволяет сэкономить немного денег. Однако большинство встроенных сетевых плат невысокого уровня, что не позволяет использовать их для организации работы серверов и других функциональных компьютеров. Поэтому многие пользователи предпочитают устанавливать дополнительную сетевую карту, тем более что она необходима в разного рода серверах, например в интернет-шлюзах.

Скорость работы адаптера зависит от сетевого оборудования, которое используют для организации сети. Если оно функционирует на скорости 100 Мбит/с, нет смысла приобретать сетевые карты, работающие со скоростью 10 Мбит/с. В крайнем случае можно использовать адаптер, работающий со скоростью и 10, и 100 Мбит/с.

Что касается беспроводных сетевых адаптеров, то к их выбору следует подходить очень аккуратно — можно получить сеть, в которой половина компьютеров не сможет общаться с другими.

Если вы используете коаксиальный кабель, то вам нужно также учесть, что сетевые карты должны иметь BNC-разъем. Как правило, в этом случае приобретают комбинированные сетевые карты с двумя разъемами: BNC и RJ-45. Такие карты обычно работают на скорости как 10, так и 100 Мбит/с.

Для проводной сети на основе витой пары лучше всего приобретать сетевые адаптеры, рассчитанные на работу в сети со скоростью 100 Мбит/с или даже 1 Гбит/с.

Опять же, дабы избежать неприятных моментов при работе в беспроводной сети, лучше использовать сетевые адаптеры одного стандарта, к примеру IEEE 802.11b. Еще лучше — оборудование стандарта IEEE 802.11g, которое имеет совместимость со всеми предыдущими беспроводными стандартами.

ПРИМЕЧАНИЕ

Из видеоурока «Урок 17.2. Установка сетевой карты в компьютер», который находится на компакт-диске, прилагаемом к книге, вы узнаете, как установить сетевую карту в корпус компьютера.

Для установки сетевого адаптера в компьютер снимите с системного блока прикрывающую его образную крышку (или левую боковину), открутив сзади корпуса несколько винтов.

Затем выберите PCI-слот, в который вы планируете установить сетевую карту, и открутите или выломайте соответствующую планку в задней стенке корпуса (рис. 17.2).

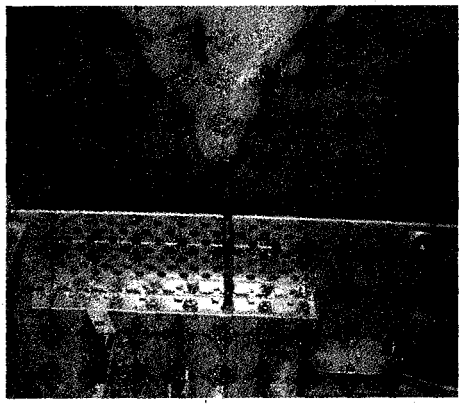


Рис. 17.2. Выкручиваем заглушку

ВНИМАНИЕ

Перед тем как выкручивать и тем более выламывать планку, приложите сетевую карту к PCI-слоту, чтобы определить, какую из прорезей на задней стенке корпуса нужно освободить. Дело в том, что сетевые карты могут быть как в левом исполнении, когда сама плата находится слева от слота, так и в правом. От этого зависит, какую из планок нужно снимать.

После этого возьмите сетевую плату в руки таким образом, чтобы ее выход оказался повернутым к задней стенке. Далее несильным, но настойчивым нажатием на плату с двух сторон вставьте ее в слот (рис. 17.3).

После этого проверьте плотность контактов и при необходимости еще раз нажмите с двух сторон, чтобы металлическая планка, к которой прикручена сетевая плата, плотно прижалась к шасси корпуса. Затем прикрутите металлическую планку к шасси с помощью винта.

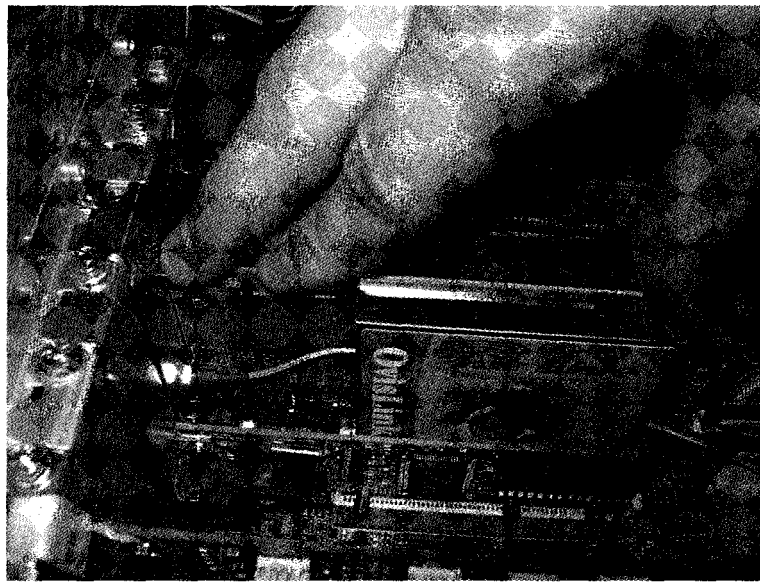


Рис. 17.3. Вставляем сетевой адаптер

После этого можно установить крышку корпуса обратно и подключить к выходу сетевой карты кабель или, в случае с беспроводной сетевой картой, прикрутить антенну (рис. 17.4).

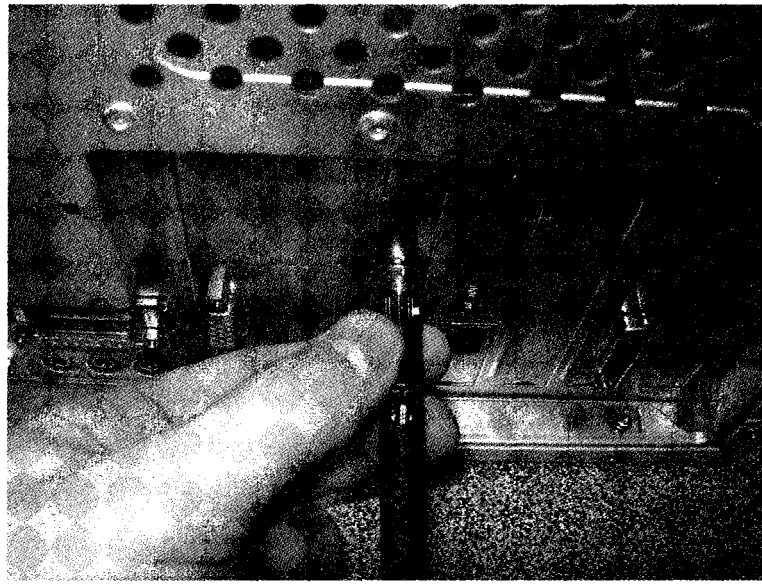


Рис. 17.4. Установка завершена, прикручиваем антенну

После того как сетевой адаптер установлен, можно включить компьютер и заняться установкой и настройкой драйверов.

После установки сетевой карты в слот материнской платы нужно загрузить ее драйверы. Такие операционные системы, как Windows 2000/XP/Server 2003, имеют большую базу драйверов разнообразных устройств, поэтому сетевая карта, скорее всего, определится автоматически и система сама установит сетевые драйверы. Если система не распознала тип сетевой карты, вам придется установить их самостоятельно.

Итак, подключив к компьютеру новое устройство и загрузив операционную систему, вы через несколько секунд увидите, что ваше устройство не только опознано (рис. 17.5), но уже установлено и используется системой.

При этом вы можете сразу же настроить его (рис. 17.6).

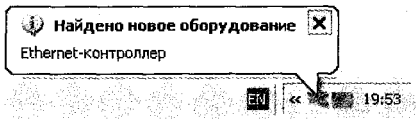


Рис. 17.5. Обнаружено новое устройство — сетевая плата

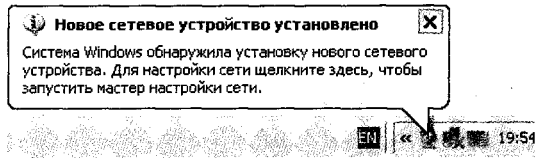


Рис. 17.6. Предложение настроить установленное устройство

Если вы не доверяете появляющимся сообщениям, проверить их правдивость можно, запустив **Диспетчер устройств**. Для этого щелкните правой кнопкой мыши на значке **Мой компьютер** и в контекстном меню выберите пункт **Свойства**.

После этого появится окно **Свойства системы**, содержащее несколько вкладок с разнообразной справочной информацией. Некоторые из них также можно использовать для вызова определенных системных утилит. В частности, можно запустить автоматическое обновление компонентов операционной системы через Интернет или восстановление системы и наблюдение за дисками.

На данный момент нас интересует вкладка **Оборудование** (рис. 17.7). Она позволяет не только просматривать информацию о подключенных устройствах и драйверах, но и устанавливать новое оборудование и настраивать профили для разных конфигураций системы.

В данном случае нас интересует информация об установленных устройствах, поэтому нажмите кнопку **Диспетчер устройств**.

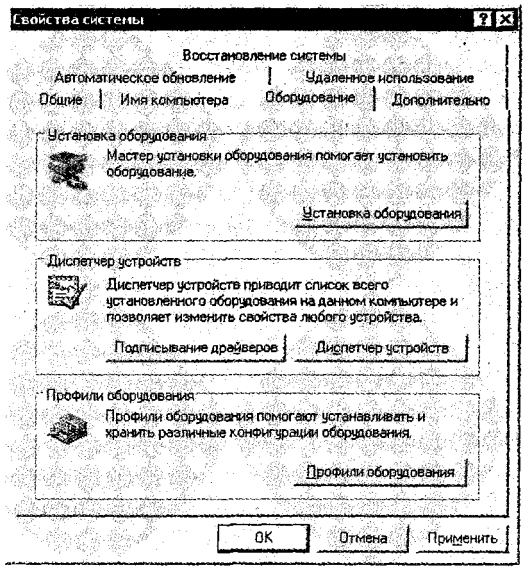


Рис. 17.7. Окно Свойства системы, вкладка Оборудование

В открывшемся окне можно увидеть информацию о любом установленном в системе устройстве. Для этого нужно выбрать соответствующий пункт, развернуть его и дважды щелкнуть на названии нужного устройства.

На рис. 17.8 видно, что сетевая карта установлена.

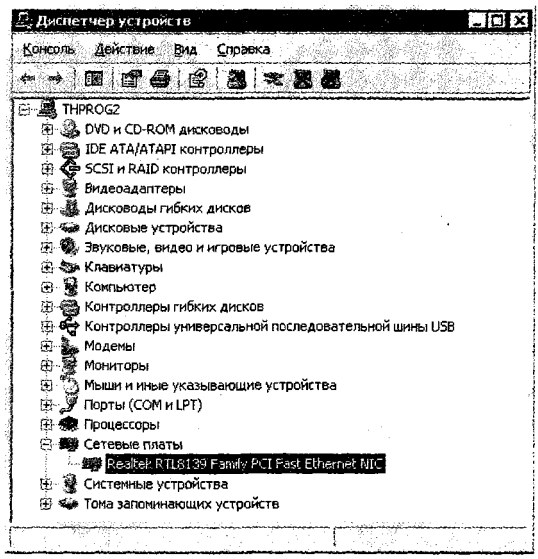


Рис. 17.8. Окно Диспетчер устройств

Если система не смогла найти сетевую плату после включения компьютера или, обнаружив ее, не установила нужный драйвер, вам придется сделать это вручную.

Для этого в диалоговом окне, показанном на рис. 17.7, нажмите кнопку **Установка оборудования**.

После этого загрузится **Мастер установки оборудования**. Принцип его действия такой же, как в предыдущих версиях операционной системы. Прочитав полезную информацию о том, что он умеет и для чего предназначен, нажмите кнопку **Далее**.

Как обычно, мастер предложит два варианта дальнейших действий.

- Автоматический поиск и установка. Этот механизм запускается сразу после загрузки операционной системы, поэтому, если начальная установка сетевой карты не дала никаких результатов, повторный поиск, скорее всего, не поможет.
- Установка вручную. Этот вариант подразумевает, что пользователь знает, где находится драйвер устройства, и сам укажет его расположение (рис. 17.9).

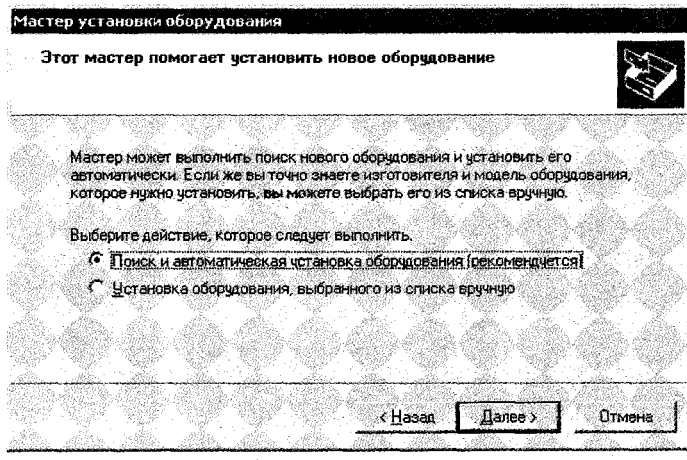


Рис. 17.9. Выбор варианта действий

Если вы все-таки решили использовать первый вариант, установите соответствующий переключатель и нажмите кнопку **Далее**.

После этого мастер начнет искать устройство по всем категориям.

Если мастер не сможет обнаружить устройство, то в появившемся окне нужно нажать кнопку **Далее**, чтобы указать модель сетевой карты вручную.

На этом же этапе вы бы оказались, если бы выбрали второй вариант действий в окне, показанном на рис. 17.9.

Чтобы установить драйвер для сетевой карты вручную, в открывшемся окне (рис. 17.10) выберите пункт **Сетевые платы** и нажмите кнопку **Далее**.

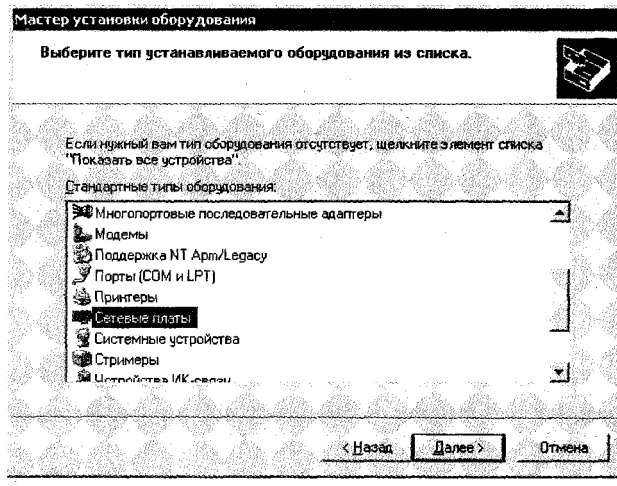


Рис. 17.10. Выбираем нужный тип оборудования — сетевую плату

После этого вам предстоит выбрать производителя сетевой карты и ее название (рис. 17.11). Если у вас есть диск с драйверами к устройству, то нажмите кнопку **Установить с диска** и укажите путь к драйверу.

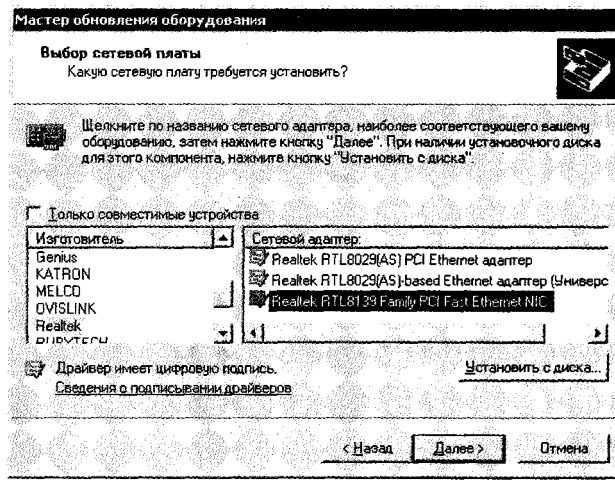


Рис. 17.11. Выбор производителя сетевой карты

После подтверждения выбора мастер начнет копировать нужные файлы. При этом он проверит наличие цифровой подписи у драйвера сетевой карты. Делается это для обеспечения максимальной защиты операционной системы от непредвиденных сбоев.

Если подпись у драйвера отсутствует, то есть драйвер сетевой карты может каким-либо образом нарушить работоспособность системы, то мастер установки сообщит об этом и предложит выбрать вариант дальнейших действий: продолжить установку драйвера или установить другой. Если вы уверены, что драйвер работоспособен, продолжите установку, иначе придется искать новый.

После завершения установки мастер выдаст окно с сообщением об этом.

Чтобы убедиться, что сетевая карта уже установлена, запустите **Диспетчер устройств**.

Беспроводное оборудование никогда не устанавливается самостоятельно. Поэтому вам придется осуществить подобные действия для любого беспроводного адаптера. Единственное, что может облегчить вам задачу, — более или менее интеллектуальная программа установки, которая находится на идущем в комплекте с устройством диске.

Глава 18

Настройка беспроводного оборудования

- Настройка точки доступа
- Настройка беспроводного адаптера

Поскольку для настройки беспроводного оборудования используется программа производителя и она не зависит от типа операционной системы, эту тему будем рассматривать отдельно.

В поставку с беспроводными устройствами, как правило, входят утилиты управления их работой. После установки драйвера они используются для настройки режима сети, уровня ее безопасности, SSID, протокола безопасности и многого другого.

Данные настройки обязательно нужно сделать независимо от того, в каком режиме будет работать сеть. В любом случае следует назначить одинаковый SSID всем устройствам и тем более необходимо обеспечить нормальный уровень безопасности сети.

18.1. Настройка точки доступа

В качестве образца будем использовать точку доступа D-Link DWL-2100AP, которая достаточно популярна среди организаторов беспроводных сетей и характеризуется относительной дешевизной и большим количеством технических возможностей. В частности, она может выступать не только в роли точки доступа, но и служить мостом, повторителем, клиентом с проводным подключением и т. п.

Для конфигурирования данной точки доступа можно пойти несколькими путями. В частности, можно использовать веб-интерфейс, доступный по адресу 192.168.0.50, утилиту конфигурирования или системную утилиту telnet. В любом случае количество параметров, изменяемых с их помощью, впечатляет и даже шокирует.

Использование утилиты конфигурирования, поставляемой вместе с устройством, возможно только при Ethernet-подключении к точке доступа или при беспроводном подключении с помощью беспроводного адаптера. Это означает, что, не имея подключенного беспроводного адаптера, вы сможете подключиться к точке доступа, только используя проводное подключение. Наилучшим и наиболее безопасным способом управления точкой доступа, конечно же, является непосредственное подключение ее к управляющему компьютеру посредством кабеля, хотя это и не всегда возможно. При этом IP-адрес и маска подсети соединения, с помощью которого производится подключение, должны быть настроены соответствующим образом. В частности, IP-адрес должен быть, например, 192.168.0.51, а маска подсети — 255.255.255.0.

Сделать это можно, если вызвать окно свойств беспроводного соединения (**Пуск ▸ Настройка ▸ Сетевые подключения**), а затем щелкнуть на соединении правой кнопкой мыши и в появившемся меню выбрать пункт **Свойства**.

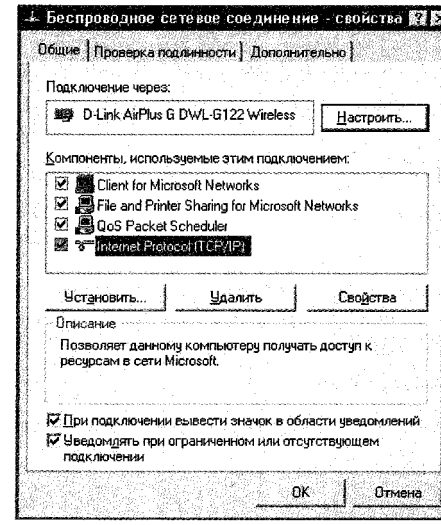


Рис. 18.1. Свойства соединения

В результате откроется окно свойств выбранного соединения (рис. 18.1), в котором отображается подключенный адаптер и набор протоколов и служб, используемых для организации соединения. Нас интересует протокол TCP/IP. Выделяем позицию **Internet Protocol (TCP/IP)** и нажимаем кнопку **Свойства**.

В появившемся окне (рис. 18.2) устанавливаем переключатель **Использовать следующий IP-адрес** и в поля **IP-адрес** и **Маска подсети** вводим нужные значения. После этого можно нажать кнопку **ОК** и попытаться запустить утилиту конфигурирования точки доступа.

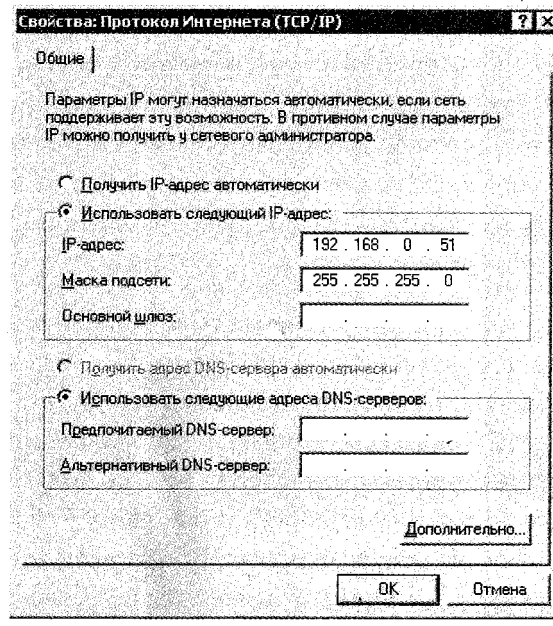


Рис. 18.2. Указываем IP-адрес и маску подсети

Предположим, для конфигурирования точки доступа вы решили использовать утилиту конфигурирования AP Manager, которая находится на прилагаемом к устройству компакт-диске.

После запуска программы появляется окно, показанное на рис. 18.3. В верхней его части находится восемь кнопок, вызывающих разные окна настроек устройства или окна со сведениями.

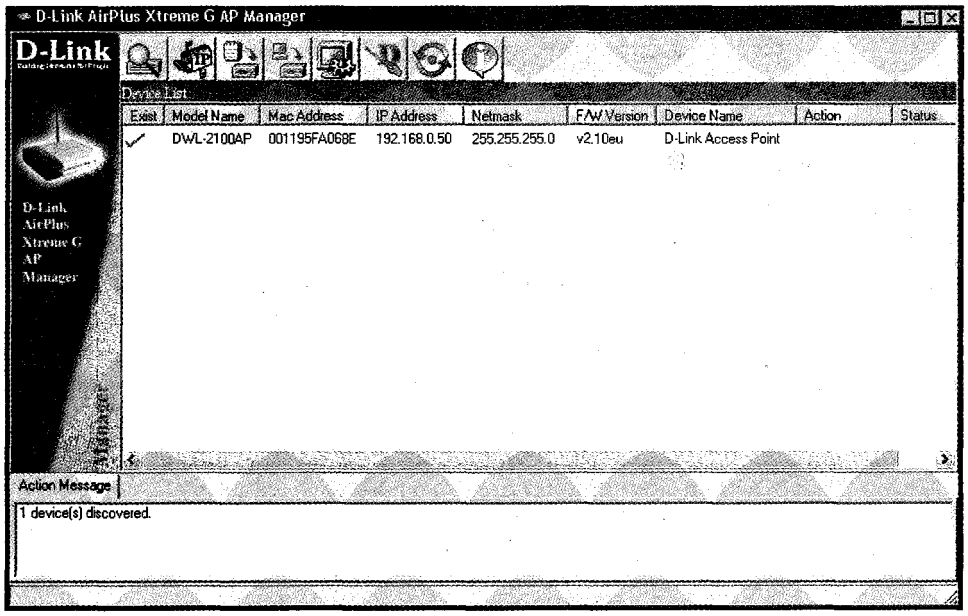


Рис. 18.3. Главное окно программы конфигурирования

В центральной части окна программы находится список всех найденный точек доступа D-Link DWL-2100AP с кратким описанием их параметров.

В нижней части отображаются все события, происходящие с точкой доступа, например сообщения конфигурирования или сообщения об ошибках.

Итак, начнем с самого простого. Нажимаем первую кнопку, имеющую подсказку **Discover devices** (Поиск устройств). В результате программа произведет поиск доступных точек доступа и выведет их в центральной части окна. В нашем случае обнаружена только одна точка доступа.

По умолчанию точка доступа имеет IP-адрес 192.168.0.50 и маску подсети 255.255.255.0. Естественно, с целью безопасности данный адрес лучше всего

сменить на другой, поскольку любой, кто знает адрес точки доступа, может попробовать к ней подключиться или применить методы взлома. Чтобы поменять адрес, нужно нажать вторую слева кнопку, которая имеет подсказку **Set IP** (Установить IP). В результате появляется окно, содержащее всего два параметра — **IP Address** (IP-адрес) и **IP Netmask** (IP-маска сети). Изменив адресацию согласно принятой в сети[1], нажимаем кнопку **OK**.

Следующий шаг — установка начальных параметров работы точки доступа. Для этого нажимаем шестую кнопку с подсказкой **Wizard** (Мастер).

В результате появится окно мастера настройки точки доступа, в котором сообщается, что в процессе работы будут настроены следующие параметры: пароль доступа к точке доступа, SSID, канал передачи данных и режим безопасности (рис. 18.4).

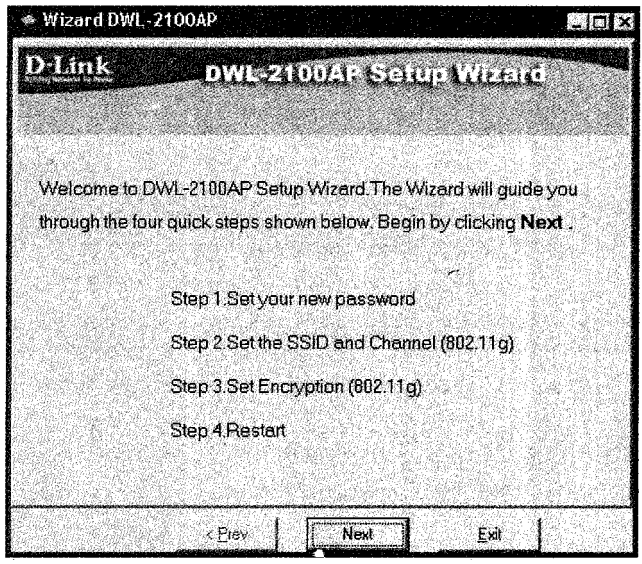


Рис. 18.4. Окно мастера настройки точки доступа

Чтобы начать настройку точки доступа, нажимаем кнопку **Next** (Далее).

В следующем окне вам предложат ввести пароль, который утилита станет запрашивать в случае, если будет производиться какая-либо настройка парамет-

[1] Часто используется зарезервированный или статичный IP-адрес.

ров точки доступа. Естественно, данный пароль должен знать только человек, отвечающий за администрирование сети. Установив новый пароль и введя его подтверждение, нажимаем кнопку **Next** (Далее).

В следующем окне вам предложат выбрать канал, по которому будут передаваться данные (рис. 18.5). В идеале канал должен выбираться таким образом, чтобы он не мешал работе другой точки доступа, хотя теоретически каналы не пересекаются.

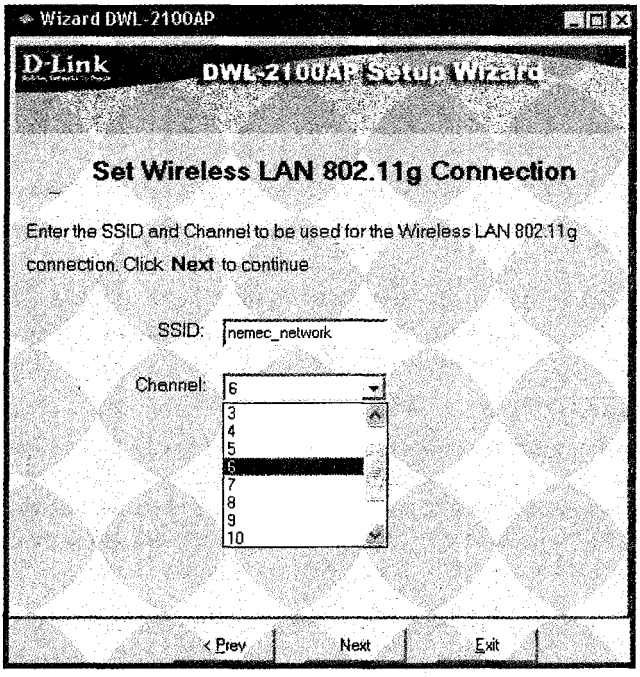


Рис. 18.5. Выбираем канал передачи данных

В принципе, многие «умные» точки доступа могут при необходимости изменять номер канала автоматически. Однако, как бы там ни было, начальный канал указать придется. По умолчанию используется шестой канал, его и оставляем. Для продолжения установки нажимаем кнопку **Next** (Далее).

В следующем окне (рис. 18.6) вам предложат выбрать начальный режим безопасности, включающий в себя использование протокола WEP с определенной длиной ключа шифрования. Если вы не хотите применять шифрование (а зря!), оставляйте значение **Disable** (Заблокировано) и нажимайте **Next** (Далее) для перехода в следующее окно.

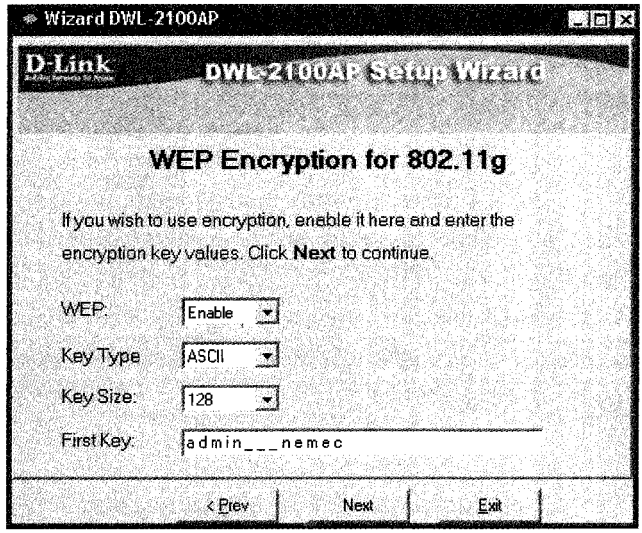


Рис. 18.6. Указываем параметры шифрования и ключ шифрования

В противном случае выбираем значение **Enable** (Разрешено). Далее необходимо указать тип ключа — **HEX** или **ASCII**, длину ключа (**64**, **128**, **152**) и сам ключ.

ВНИМАНИЕ

При выборе длины ключа обязательно убедитесь в том, что все беспроводные устройства сети смогут работать с ним. Часто бывает так, что точка доступа поддерживает длину ключа, например, 104 бит, в то время как беспроводный адаптер его не поддерживает. В итоге, беспроводное устройство не может подключиться к точке доступа.

При выборе ключа не рекомендуется использовать какие-либо личные данные, например фамилию, дату рождения или номер телефона, поскольку они могут стать причиной взлома сети злоумышленниками. Лучше всего подобрать несвязное символьное выражение или смесь знаков.

После нажатия кнопки **Next** (Далее) появляется итоговое окно, которое сообщает, что настройка начальных параметров точки доступа завершена. Если вы хотите что-либо изменить, воспользуйтесь кнопкой **Prev** (Предыдущее). Если все данные указаны верно, подтверждаем их нажатием кнопки **Finish** (Готово).

Поскольку подключение к точке доступа с помощью утилиты конфигурирования также использует пароль доступа к ней, то перед внесением изменений программа обязательно предупредит вас, что после применения параметров необходимо сделать соответствующие настройки в системной части программы.

После этого программа конфигурирования начнет запись новых параметров в постоянную память точки доступа, что может занять некоторое время.

Следующий шаг — настройка нового пароля для доступа к точке доступа с помощью программы. Для этого нажимаем пятую кнопку — с подсказкой **System Settings** (Системные установки). Откроется окно, которое показано на рис. 18.7. В самой верхней его части находится поле ввода **Access Password** (Пароль доступа), в котором и нужно прописать введенный при настройке точки доступа пароль. После этого нажимаем кнопку **OK** и начинаем более детально настраивать параметры.

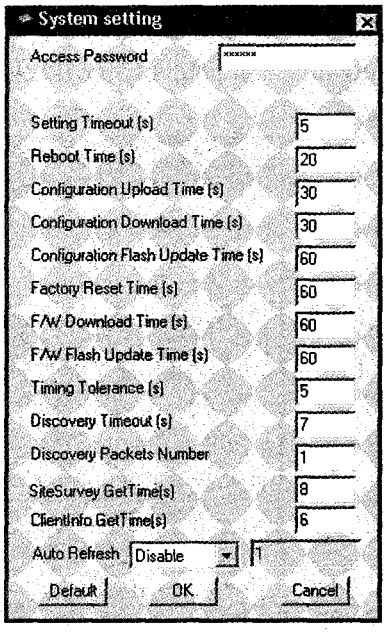


Рис. 18.7. Системные установки утилиты конфигурирования

Итак, чтобы зайти в расширенные параметры точки доступа, достаточно дважды щелкнуть кнопкой мыши на позиции с информацией о точке доступа или нажать третью кнопку с подсказкой **Devices Settings** (Установки устройства).

ПРИМЕЧАНИЕ

Любые изменения, вносимые в конфигурацию точки доступа, начинают работать лишь после нажатия кнопки Apply (Применить).

Окно настройки точки доступа состоит из семи вкладок, каждая из которых содержит свой набор параметров. Ниже описаны все находящиеся на вкладках параметры и их возможные значения.

СОВЕТ

На каждой вкладке присутствует набор из семи кнопок, каждая из которых выполняет свою функцию. Обратите особое внимание на кнопки Check All (Отметить все) и Clear Checks (Очистить отмеченное). С их помощью можно отметить все параметры или снять выделение с них на всех вкладках. Исходя из этого, советую ни в коем случае не пользоваться этими кнопками, поскольку это может привести к трудноисправимым последствиям. Лучше внимательно просмотреть все вкладки и аккуратно внести все необходимые изменения, нежели потом отлавливать причины отказа работы точки доступа или беспроводных адаптеров вашей сети.

Вкладка General

По умолчанию первой открывается вкладка **General** (Общие) (рис. 18.8).

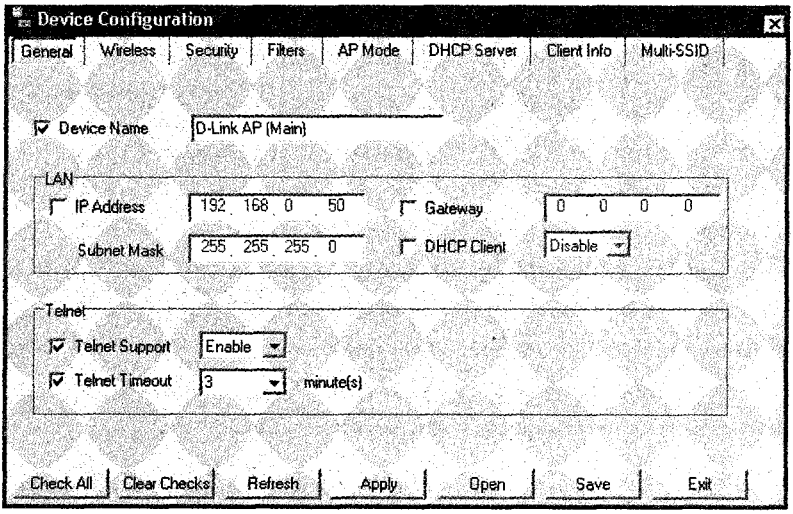


Рис. 18.8. Содержимое вкладки General (Общие)

На ней вы найдете следующие параметры.

- **Device Name** — дает возможность изменить название точки доступа, тем самым позволяя отличать точки доступа между собой. С помощью данного названия, например, можно описать местоположение точки или ее роль в сети. Чтобы ввести название, необходимо активизировать параметр установкой флажка.
- **LAN** — данная область отвечает за конфигурирование точки доступа в плане настройки IP-адреса, маски подсети, шлюза и DHCP-клиента.
  - **IP Address** (IP-адрес) — параметр, содержащий текущий IP-адрес, которым пользуется точка доступа. По умолчанию он использует IP-адрес 192.168.0.50 и его изменение заблокировано. Если по какой-либо причине этот адрес использовать в сети не рекомендуется (например, с целью безопасности), тогда можно установить флажок напротив параметра **IP Address** и ввести новое значение.
  - **Subnet Mask** (Маска подсети) — параметр, работающий в паре с **IP Address** и отвечающий за маску подсети. При изменении IP-адреса (когда установлен флажок **IP Address**) параметр **Subnet Mask** активизируется и можно

ввести требуемую маску подсети. При этом маска сети вычисляется автоматически в зависимости от введенного IP-адреса.

- **Gateway** (Шлюз) — параметр, содержащий IP-адрес шлюза, который, например, может использоваться для подключения к интернет-серверу, любому другому маршрутизатору или точке доступа. Чтобы активизировать данный параметр, установите соответствующий флажок и введите в поле ввода данных нужный адрес.
- **DHCP Client** (DHCP-клиент) — если планируется использовать статический IP-адрес, необходимо выбрать позицию **Disable** (Запрещено). При этом автоматически отключаются параметры **IP Address** и **Subnet Mask.** Если же в сети установлен DHCP-сервер и точке доступа назначается автоматическая адресация, тогда необходимо установить значение **Enable** (Разрешено).

➢ **Telnet** — данная область содержит параметры, которые отвечают за настройку точки доступа с использованием системной утилиты telnet.

- **Telnet Support** (Поддержка telnet) — параметр может принимать всего два значения: **Enable** (Разрешено) и **Disable** (Запрещено). В зависимости от этого вы сможете или не сможете использовать утилиту telnet для конфигурирования устройства[1]. По умолчанию установлен флажок **Enable** (Разрешено).
- **Telnet Timeout** (Задержка отключения telnet) — в целях безопасности, если при использовании программы возникают значительные перерывы, имеется возможность отключения точки доступа. Чтобы задействовать этот механизм, достаточно установить соответствующий флажок и ввести в поле промежуток времени, через который будет произведено отключение. По умолчанию он составляет 3 минуты. Оптимальным же является вариант 10 минут.

Вкладка Wireless

Вкладку **Wireless** (Беспроводная сеть) используют для настройки таких основных параметров беспроводной сети, как SSID, канал передачи данных, скорость передачи данных и др. (рис. 18.9).

---

[1] При использовании утилиты telnet, как правило, имеется возможность конфигурировать намного больше параметров устройства, нежели при использовании стандартной утилиты конфигурирования.

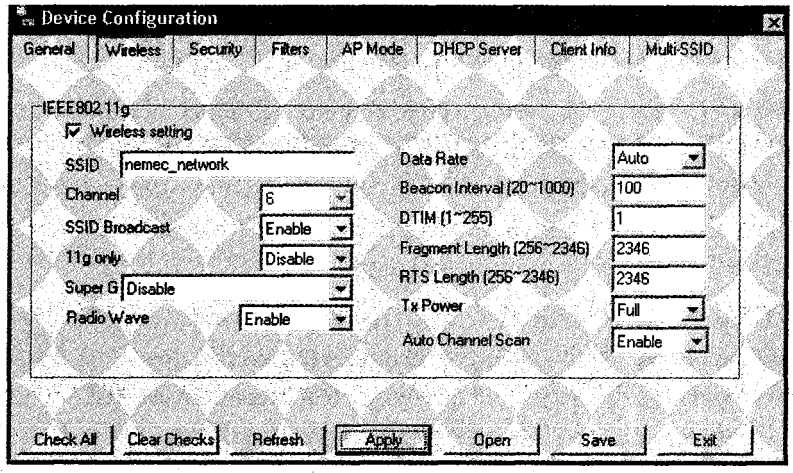


Рис. 18.9. Содержимое вкладки Wireless (Беспроводная сеть)

На вкладке имеются следующие параметры.

- **Wireless setting** (Настройка беспроводной сети) — данная область содержит основные параметры, коренным образом влияющие на организацию работы сети.
  - **SSID** — описывает уникальный идентификатор сети, который выступает в качестве связующего звена всех участвующих в работе беспроводных устройств. По умолчанию для точки доступа D-Link DWL-2100AP установлено значение **default**. Естественно, как минимум в целях безопасности, данный идентификатор следует изменить на что-то более уникальное. В нашем случае параметру **SSID** присвоено значение `nemec_network`.
  - **Channel** (Канал передачи данных) — параметр отвечает за номер канала, который будет использоваться для передачи данных в сети. По умолчанию выбирается шестой канал, хотя это фактически не несет никакой практической нагрузки. В случае использования параметра **Auto Channel Scan** (Автоматическое сканирование каналов) данный канал выбирает автоматически сама точка доступа и сведение об этом сообщается каждому беспроводному устройству сети, что заставляет их менять канал передачи данных автоматически. На практике выбирают канал, который не используется другими точками доступа, с целью уменьшения взаимных помех.
  - **SSID Broadcast** (Транслирование SSID) — параметр играет важную роль в организации безопасной передачи данных в сети. По умолчанию точка доступа производит радиовещание своего SSID всем радиоустройствам

в радиусе ее действия, что, естественно, делает защиту сети более сильной. С целью максимально обезопасить себя от посягательств извне рекомендуется вещание SSID отключить. В любом случае пользователям, которые законно подключают свои компьютеры к сети, данный идентификатор все равно сообщается. Так почему же не усложнить жизнь злоумышленнику?

- **11g only** (Только 11g-устройства) — поскольку в работе сети не обязательно участвуют устройства единого стандарта, этот факт следует учитывать. Если вы планируете использовать устройства любого совместимого типа, то, естественно, данному параметру следует задать значение **Disable** (Запрещено). В противном случае, если все устройства поддерживают, например, стандарт IEEE 802.11g, можно установить значение **Enable** (Разрешено).

ПРИМЕЧАНИЕ

Кстати, используя этот параметр, можно достичь дополнительной защищенности сети, исключая нежелательные возможные подключения с помощью устройств другого стандарта. Правда, при этом нужно обеспечить использование устройств обязательно поддерживающих стандарт IEEE 802.11g.

- **Super G** (Режим «Супер G») — каждая точка доступа имеет свои технические особенности, тем или иным образом отличающие ее от множества устройств подобного типа. Особенностью точки доступа D-Link DWL-2100AP является механизм передачи данных, при котором достигается удвоенная скорость, составляющая 108 Мбит/с. Данный параметр может принимать четыре значение: **Disable** (Запрещено), **Super G without Turbo** (Режим «Супер G» без дополнительного ускорения), **Super G with Static Turbo** (Режим «Супер G» со статическим ускорением) и **Super G with Dynamic Turbo** (Режим «Супер G» с динамическим ускорением). Экспериментировать с использованием этих режимов (кроме режима **Disable** (Запрещено)) нужно очень осторожно, поскольку точка доступа может повести себя непредсказуемо. Обязательным условием использования этого режима в сети является практическая поддержка его всеми устройствами.
- **Radio Wave** (Радиоволны) — режим фактически используют для включения и отключения радиоустройства.
- **Data Rate** (Скорость данных) — данный параметр указывает, с какой скоростью будет производиться передача данных в сети, если только параметр **Super G** (Режим «Супер G») имеет значение **Disable** (Запрещено).

Доступны значения **Auto**, **1**, **2**, **5**, **6**, **9**, **11**, **12**, **18**, **24**, **36**, **48** и **54** Мбит/с. По умолчанию установлено значение **Auto**, и это правильно, поскольку скорость передачи данных может автоматически изменяться в зависимости от условий среды.

- **Beacon Interval (20-1000)** (Интервал сигналов (20–1000)) — отвечает за частоту отсылки пакетов, призванных синхронизировать устройства сети. По умолчанию установлено значение **100**, чего вполне достаточно для поставленной задачи. Если наблюдаются сбои в работе устройств или качество сигнала оставляет желать лучшего, данный показатель можно уменьшать до **20**, и наоборот, если сеть работает устойчиво, частоту отсылки таких пакетов можно уменьшить путем повышения интервала вплоть до **1000**. При этом не забывайте, что чрезмерное уменьшение интервала отсылки пакетов синхронизации приводит к увеличению трафика сети и, как следствие, к уменьшению скорости передачи полезной информации.
- **DTIM (1-255)** — параметр отвечает за количество отсылаемых пакетов подтверждения того, когда будет доступно следующее окно для передачи данных. Данные пакеты отсылаются всем клиентам сети, чтобы они знали, когда можно начинать вещание. Доступные значения — от **1** до **255**, по умолчанию установлено значение **1**.
- **Fragment Length (256-2346)** (Объем пакетов данных (256–2346)) — данный параметр описывает максимальный размер пакета данных, при достижении которого происходит разбивка информации на более мелкие пакеты. По умолчанию, чтобы максимально увеличить пропускную способность сети, установлено значение **2346**, которое в случае надобности можно уменьшать до **256**.
- **RTS Length (256-2346)** (Объем пакета RTS (256–2346)). RTS-пакеты служат для отсылки коротких сообщений в сеть о том, что один из компьютеров хочет передать данные другому. При этом в пакете содержится информация об отправителе и получателе, а также любая другая информация, которая востребована на данный момент. По умолчанию размер RTS-пакета составляет 2346 бит, но может быть уменьшен вплоть до 256 бит.
- **Tx Power** (Мощность сигнала) — данный параметр описывает показатель мощности, с которой передатчик данного устройства производит передачу данных. Этот параметр может принимать значения **Full** (Полная мощность), **Half** (Половина мощности), **Quarter** (Четверть мощности), **Eighth** (Восьмая часть мощности) и **Min** (Минимальная мощность). Для пере-

носных устройств потребляемая мощность играет достаточно важную роль, поэтому в сети небольшого радиуса разумно будет уменьшить мощность передатчика до уровня, необходимого для досягаемости всех ее устройств. Кроме того, с помощью регулировки мощности сигнала можно обеспечить дополнительный уровень безопасности сети, отсекая возможных удаленных клиентов.

- **Auto Channel Scan** (Автоматическое сканирование каналов) — очень полезный параметр, отвечающий за использование механизма автоматического сканирования частотного диапазона с целью выявления наименее зашумленного канала. Доступны два значения — **Enable** (Разрешить) и **Disable** (Запретить). По понятным причинам рекомендуется использовать первый.

Вкладка Security

Вкладку **Security** (Безопасность) (рис. 18.10) используют для настройки параметров безопасности беспроводной сети, без чего она представляет собой легкую цель для любителей покопаться в чужих данных и украсть что-то ценное.

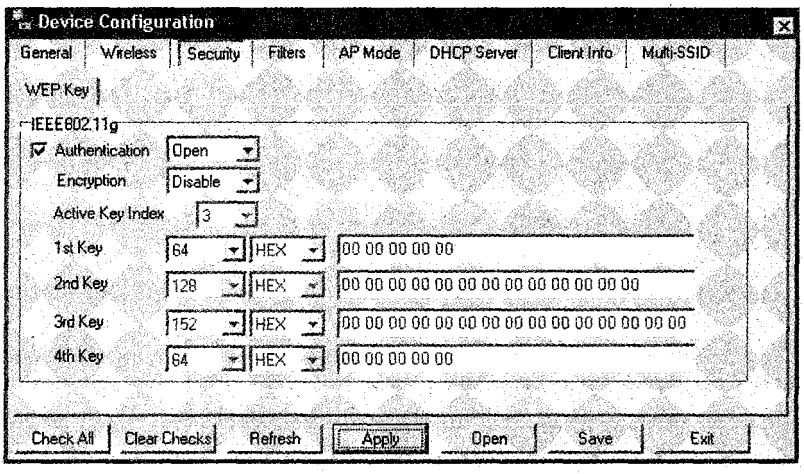


Рис. 18.10. Вкладка Security (Безопасность)

Содержимое вкладки изменяется в зависимости от выбранных ранее параметров. Фактически на ней могут быть две разные вкладки — **WEP Key** (WEP-ключи) и **IEEE.11g WPA**. Рассмотрим вкладку подробнее.

- **IEEE802.11g** — данная область содержит параметры, связанные с настройкой протокола безопасности WEP.

- **Authentication** (Аутентификация) — отвечает за включение или отключение режима аутентификации. Чтобы задействовать его, достаточно установить соответствующий флажок и выбрать значение из списка: **Open** (Открытый), **Shared** (Разделенный), **Both** (Оба режима), **WPA-EAP**, **WPA-PSK**. В случае двух последних вариантов появляется дополнительная вкладка **IEEE.11g WPA** с настройками данного метода аутентификации.
- **Encryption** (Шифрование) — параметр активизирует или деактивизирует метод шифрования с помощью установки значений **Enable** (Разрешить) и **Disable** (Запретить) соответственно. При этом сам параметр доступен лишь в случае, когда параметр **Authentication** (Аутентификация) имеет значения **Open** (Открытый) или **Both** (Оба режима). В любом случае, будь то протокол безопасности WEP или WPA, использовать шифрование очень желательно, чтобы в один прекрасный день не обнаружить, что у вас пропадают важные документы или кто-то ворует интернет-трафик.
- **Active Key Index** (Индекс активного ключа) — параметр указывает на то, какой из ключей в данный момент времени активен. Вообще, протокол WEP может использовать до четырех разных ключей шифрования разной длины. Однако одновременно может использоваться только один из них. Поэтому с помощью параметра **Active Key Index** (Индекс активного ключа) можно указать, какой из этих ключей будет использоваться. В зависимости от указанного номера, активизируется конкретный (по номеру ключа) параметр, отвечающий за настройку длины ключа и выбора самого ключа.
- **1st Key** (Первый ключ) — параметр описывает первый ключ шифрования. При этом можно выбрать длину ключа (**64**, **128**, **152** бит), его символьный тип (**HEX** или **ASCII**) и указать сам ключ (строку символов выбранного типа).
- **2nd Key** (Второй ключ) — параметр описывает второй ключ шифрования. При этом можно выбрать длину ключа (**64**, **128**, **152** бит), символьный тип (**HEX** или **ASCII**) и сам ключ (строку символов выбранного типа).
- **3rd Key** (Третий ключ) — параметр описывает третий ключ шифрования. Характеристики соответствуют предыдущим.
- **4th Key** (Четвертый ключ) — параметр описывает четвертый ключ шифрования и имеет описанные выше характеристики.

➢ **WPA Setting** (Настройки WPA) — данная область содержит параметры, влияющие на работу протокола безопасности WPA.

- **Cipher Type** (Тип шифра) — параметр указывает точке доступа, какой из типов шифрования использовать. Доступны значения **Auto** (Автоматический выбор), **AES** и **TKIP**.
- **Group Key Update Interval** (Интервал обновления группового ключа) — параметр указывает интервал времени, через который произойдет автоматическая замена ключа шифрования. По умолчанию установлено значение **1800**, но можно устанавливать интервал **300–9999999**. Установка слишком малого интервала нежелательна, поскольку это увеличит частоту следования служебных пакетов, что сразу уменьшит полезную пропускную способность сети. Установка слишком большого интервала не так критична, но это дает больше времени злоумышленнику для попытки проникновения в сеть.
- **PassPhrase** (Пароль) — параметр содержит пароль, применяемый при типе шифрования TKIP. Длина пароля может колебаться от 8 до 63 символов. Понятно, что чем длиннее пароль, тем тяжелее его взломать. Обязательно учтите это при выборе.

➢ **Security Server** (Сервер безопасности) — область параметров содержит настройки RADIUS-сервера аутентификации и появляется лишь тогда, когда параметру **Authentication** (Аутентификация) присвоено значение.

- **RADIUS Server** (Адрес RADIUS-сервера) — если в сети установлен RADIUS-сервер, то здесь следует прописать его IP-адрес.
- **RADIUS Port** (Порт RADIUS-сервера) — если в сети установлен RADIUS-сервер, то здесь следует прописать порт сервера, через который происходит аутентификация.
- **RADIUS Secret** (Пароль RADIUS-сервера) — если в сети установлен RADIUS-сервер, то здесь следует прописать пароль доступа к нему.

Вкладка Filters

Вкладка **Filters** (Фильтры) используется для предоставления возможности управлять точкой доступа из Ethernet-сети или возможности настройки параметров точки доступа клиентами беспроводной сети (рис. 18.11).

На вкладке имеются следующие параметры.

➢ **WLAN Partition** (WLAN разделение) — данная область содержит параметры настройки доступа из Ethernet-сети в беспроводную сеть.

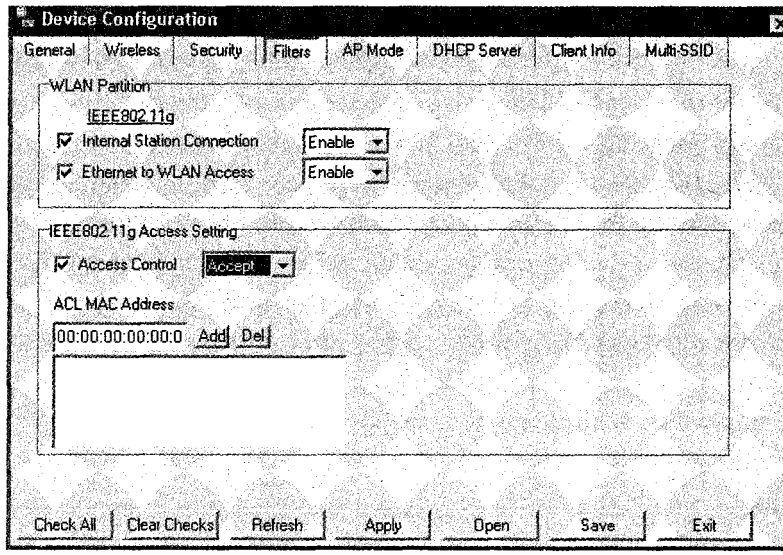


Рис. 18.11. Содержимое вкладки Filters (Фильтры)

- **Internal Station Connection** (Подключение внутренних станций) — отвечает за возможность подключения к точке доступа беспроводных устройств с целью обмена информацией между ними. Если установлено значение **Disable** (Запретить), беспроводные станции не смогут подключиться к точке доступа и, соответственно, не смогут общаться между собой. По умолчанию данный параметр имеет значение **Enable** (Разрешить), и таковым он должен оставаться постоянно, разве что происходит важное администрирование, на время которого беспроводные устройства не должны мешать.
- **Ethernet to WLAN Access** (Доступ из сети Ethernet в сеть WLAN) — с помощью данного параметра регулируют отношения между клиентами беспроводной сети и ее проводного сегмента Ethernet. Доступны два значения — **Enable** (Разрешить) и **Disable** (Запретить). Если параметр принимает значение **Disable** (Запретить), Ethernet-клиенты не могут обмениваться информацией с клиентами беспроводной сети. В то же время клиенты беспроводной сети могут обмениваться информацией с клиентами проводной сети. По умолчанию установлено значение **Enable** (Разрешить), поскольку очень часто точка доступа подключается к маршрутизатору и, соответственно, должен происходить обмен в обе стороны.

➢ **IEEE802.11g Access Setting** (Настройка доступа для устройств IEEE802.11g) — данная область содержит параметры настройки доступа к точке доступа с использованием списка доступа. С помощью параметра **Access Control** (Кон-

троль доступа) организуют списки доступа к точке доступа, ориентированные на MAC-адрес устройств, которые подключаются. Например, введя список MAC-адресов и выбрав значение параметра **Accept** (Принимать), вы тем самым позволяете этим устройствам подключаться к точке доступа. Если же установить значение **Reject** (Отклонять), устройства с указанным MAC-адресом не смогут подключиться к сети. По умолчанию установлено значение **Disable** (Запретить), что отключает использование этого параметра и позволяет всем устройствам без исключения (если не действуют другие правила) подключаться к точке доступа.

Вкладка AP Mode

Вкладку **AP Mode** (Режим точки доступа) используют для настройки режима, в котором будет работать точка доступа (рис. 18.12).

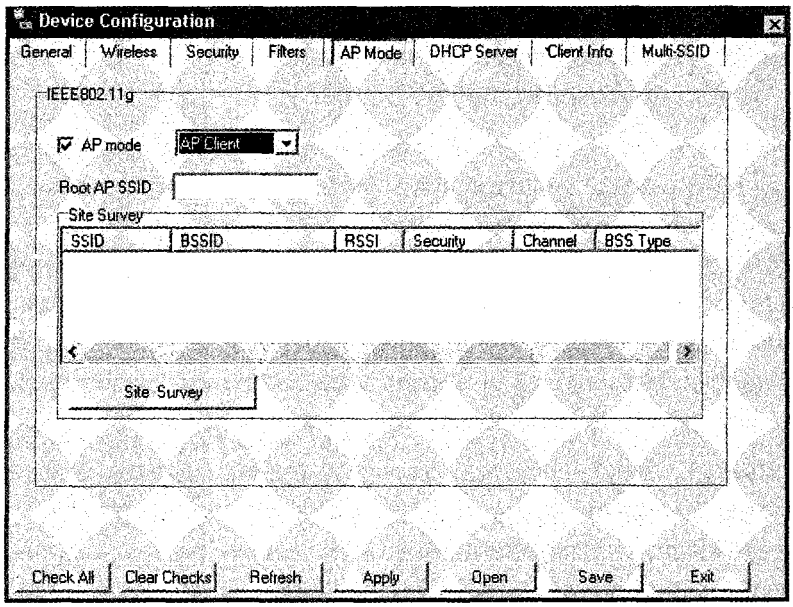


Рис. 18.12. Содержимое вкладки AP Mode (Режим точки доступа)

На вкладке присутствует всего один параметр — **AP Mode** (Режим точки доступа), однако при его изменении могут появляться дополнительные элементы управления. Возможна настройка следующих параметров этой вкладки.

- **AP Mode** (Режим точки доступа) — отвечает за режим, в котором работает данное устройство. Доступны следующие значения.

- **Access Point** (Точка доступа) — устройство выполняет свои прямые обязанности — обязанности точки доступа. По умолчанию используется именно он.
- **WDS with AP** — данный режим используют, когда необходимо соединить несколько существующих сетей в одну. При этом данная точка доступа является главной. При его активизации появляется дополнительный параметр — **Remote AP MAC Address** (MAC-адреса подключаемых точек доступа), с помощью которого нужно составить список MAC-адресов всех соединяемых точек доступа. При использовании этого режима все соединяемые точки доступа должны быть D-Link DWL-2100AP.
- **WDS** — используют, когда необходимо соединить несколько существующих сетей в одну (данная точка доступа может быть и не главной). При активизации на вкладке появляется дополнительный параметр — **Remote AP MAC Address** (MAC-адреса подключаемых точек доступа), с помощью которого нужно составить список MAC-адресов всех соединяемых точек доступа. При использовании этого режима все соединяемые точки доступа должны быть D-Link DWL-2100AP.
- **AP Repeater** (Повторитель) — режим используют в том случае, когда нужно увеличить радиус существующей сети путем ретрансляции сигнала от главной точки доступа. При активизации этого режима на вкладке появляется дополнительный параметр — **Remote AP MAC Address** (MAC-адреса подключаемых точек доступа), с помощью которого нужно указать MAC-адрес главной точки доступа. Для облегчения настройки этого параметра можно воспользоваться механизмом обзора существующих точек доступа, который запускается нажатием кнопки **Site Survey** (Обзор узлов).
- **AP Client** (Клиент) — режим используют, когда к беспроводной сети необходимо подключить одно из Ethernet-устройств, например компьютер или принтер. При активизации на вкладке появляется дополнительный параметр — **Remote AP SSID** (SSID точки доступа), для которого нужно указать SSID-устройство, которое выполняет функции точки доступа. При использовании этого режима указываемая точка доступа должна быть D-Link DWL-2100AP. Для облегчения поиска нужного SSID можно воспользоваться механизмом обзора существующих точек доступа, который запускают нажатием кнопки **Site Survey** (Обзор узлов).

➢ **Remote AP MAC Address** (MAC-адреса подключаемых точек доступа) — с помощью данного параметра можно создавать списки из MAC-адресов.

Вкладка DHCP Server

Вкладку **DHCP Server** (Сервер DHCP) (рис. 18.13) используют для настройки параметров DHCP-сервера, механизм которого встроен в точку доступа D-Link DWL-2100AP.

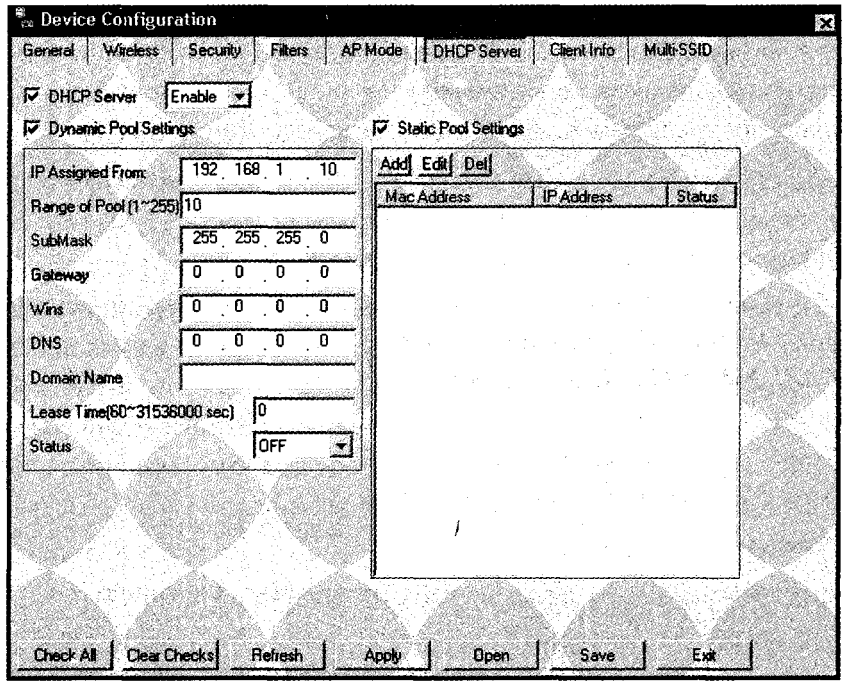


Рис. 18.13. Вкладка DHCP Server (Сервер DHCP)

На вкладке имеются следующие параметры.

- **DHCP Server** (Сервер DHCP) — параметр содержит всего два возможных значения — **Enable** (Разрешить) и **Disable** (Запретить). Первый из них активизирует встроенный сервер DHCP, а второй его отключает. По умолчанию установлено значение **Disable** (Запретить). В сети должен быть только один сервер DHCP, который чаще всего устанавливают на главной точке доступа. Поэтому, прежде чем включить этот механизм, убедитесь, что в сети не существует активного сервера DHCP. После выбора значения **Enable** (Разрешить) сразу активизируются параметры **Dynamic Pool Settings** (Динамические установки пула адресов) и **Static Pool Settings** (Статичные установки пула адресов), с помощью которых вам необходимо будет настроить пул адресов, выдаваемых устройствам беспроводной сети.

- **Dynamic Pool Settings** (Динамические установки пула адресов) — динамическая установка пула доступных адресов подразумевает автоматическую раздачу адресов устройствам сети, при которой адреса генерируются динамически, основываясь на интервальных данных, введенных пользователем. Чтобы активизировать данный механизм раздачи адресов, достаточно присвоить параметру **Dynamic Pool Settings** (Динамические установки пула адресов) значение **Enable** (Разрешить). Конечно, параллельно можно использовать и статичные IP-адреса, но в этом случае они не должны лежать в интервале адресов, предназначенных для динамической выдачи.
- **IP Assigned From** (Назначенный IP-адрес) — параметр содержит IP-адрес, назначаемый серверу DHCP. Он же является и первым из пула адресов, выделенных для динамической раздачи адресов.
- **Range of Pool (1-255)** (Интервала пула адресов (1–255)) — параметр описывает количество адресов и начальный адрес, которые отводятся для динамического распределения. Например, в качестве значения этого параметра можно ввести 10. Это означает, что адрес, заканчивающийся на 10 (например, 192.168.1.10) будет присвоен серверу DHCP, а адреса, заканчивающиеся на 11, 12, 13, 14, 15, 16, 17, 18, 19 и 20, будут динамически распределены между беспроводными устройствами.
- **SubMask** (Маска подсети) — параметр содержит маску подсети.
- **Gateway** (Шлюз) — параметр содержит IP-адрес шлюза, если таковой используют. В качестве шлюза может быть, например, маршрутизатор или точка доступа с подключением к Интернету.
- **Wins** (Системный сервис Wins) — системный сервис призван определять реальный IP-адрес сети или устройства, используя его динамический адрес. По умолчанию этот параметр не используется, а если и используется, то крайне редко.
- **DNS** — параметр содержит адрес существующего в сети сервера DNS, который может быть необходим в случае использования общего Интернета или доменной системы построения сети.
- **Domain Name** (Имя домена) — параметр содержит доменное имя, присваиваемое одной из точек доступа с целью организации доменной системы сети.
- **Lease Time (60-31536000 sec)** (Продолжительность использования) — параметр описывает временной интервал, в течение которого беспроводные клиенты могут использовать назначенные им динамические адреса. По умол-

чанию установлено значение **0**, что говорит о том, что адрес может использоваться бесконечно долго.

- **Status** (Состояние) — назначение параметра достаточно туманно, поскольку присвоение ему значения **OFF** (Отключен) приводит к отключению созданного пула адресов, что аналогично отключению сервера DHCP. По умолчанию параметр имеет значение **ON** (Включен).
- **Static Pool Settings** (Статичные установки пула адресов) — статичный набор адресов используют с целью назначения статичного адреса важным устройствам сети. Таковыми могут быть, например, серверы или сетевые принтеры. В этом случае нужно установить данный флажок и с помощью кнопок **Add** (Добавить), **Edit** (Редактировать) и **Del** (Удалить) настроить список статичных адресов. При этом имейте в виду, что данные адреса не должны лежать в интервале адресов, указанных в параметре **Range of Pool** (Интервал пула адресов).

Вкладка Client Info

Вкладка **Client Info** (Сведения о клиентах) не содержит никаких настраиваемых параметров и служит информационным целям (рис. 18.14).

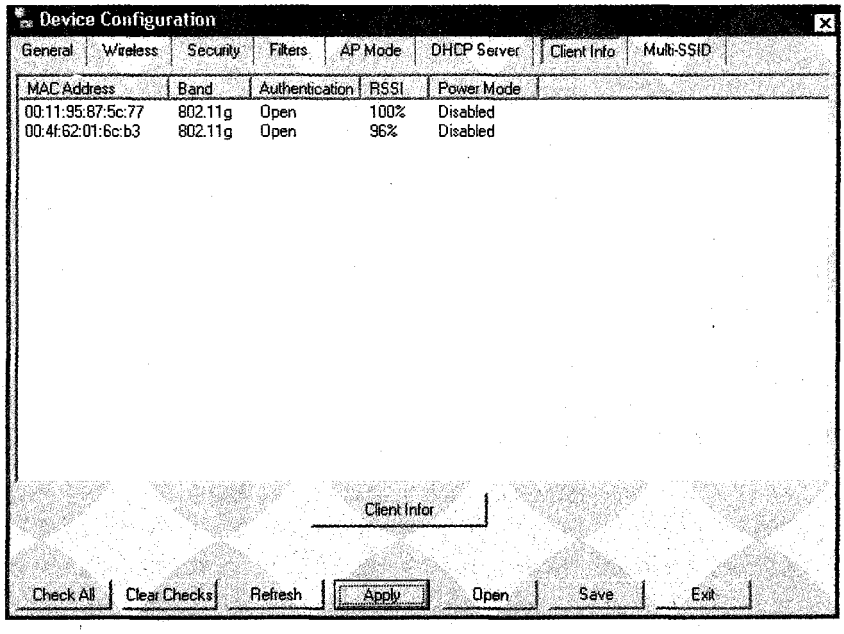


Рис. 18.14. Содержимое вкладки Client Info (Сведения о клиентах)

На ней можно увидеть информацию о беспроводных клиентах, подключенных к данной точке доступа. Чтобы произвести опрос клиентов, нужно нажать кнопку **Client Infor** (Информатор клиентов). В результате таблица на вкладке заполняется данными о MAC-адресе, беспроводном стандарте устройства, режиме аутентификации, мощности сигнала и режиме энергосбережения. В нашем примере видно, что к точке доступа в данный момент подключено два беспроводных клиента.

Вкладка Multi-SSID

Вкладку **Multi-SSID** (Мульти-SSID) используют для настройки дополнительных SSID, с помощью которых можно организовывать виртуальные сети и разграничивать подключения к точке доступа на уровне гостевых SSID. Это можно осуществлять благодаря наличию в D-Link DWL-2100AP соответствующего механизма, чем может похвастаться не каждое подобное устройство (рис. 18.15).

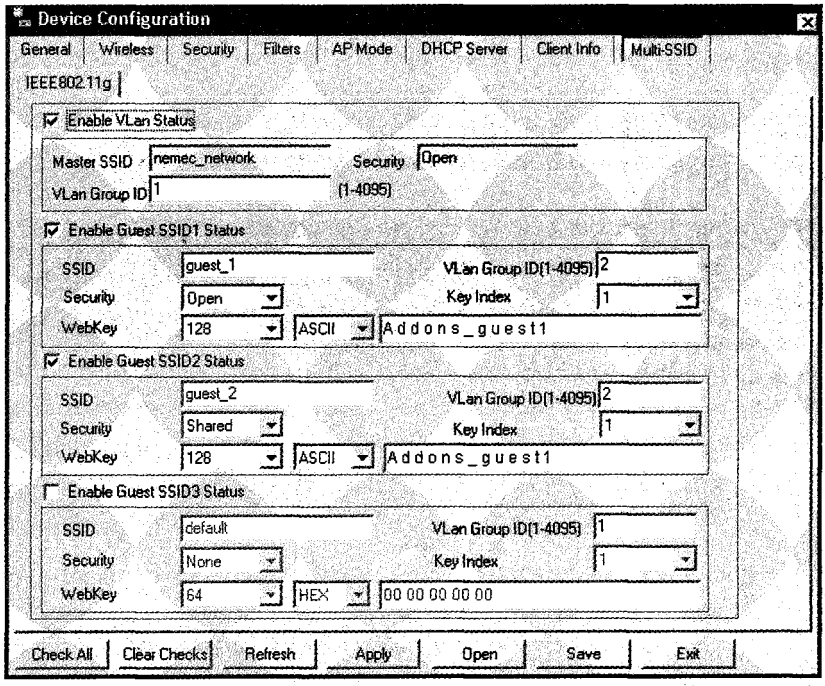


Рис. 18.15. Вкладка Multi-SSID (Мульти-SSID)

На вкладке присутствует группа параметров, которая повторяется три раза, но для разных SSID. Таким образом, есть возможность настройки до трех разных гостевых SSID. Это делается с помощью следующих параметров.

- **Enable VLan Status** (Разрешить виртуальные сети) — по умолчанию возможность использования нескольких SSID отключена. Чтобы ее задействовать, необходимо установить данный флажок.
  - **Master SSID** (Главный SSID) — параметр не изменяется, поскольку используется значение SSID точки доступа, которое настраивалось ранее. По сути, в данном поле отображается текущий SSID, присвоенный точке доступа.
  - **Security** (Безопасность) — параметр также не подлежит редактированию и отображает лишь текущий механизм безопасности, например **Open** (Открытый) или **Shared** (Разделенный).
  - **VLan Group ID** (Идентификатор виртуальной группы) — создаваемые виртуальные группы отличаются номерами. Для них доступно более 4000 номеров, начиная с единицы. Как правило, основной группе, то есть той, которая содержит главный SSID, присваивают единицу, как и показано на рис. 18.15.
- **Enable Guest SSID1 Status** (Разрешить гостевой SSID1) — область содержит параметры, описывающие дополнительный SSID, в частности SSID1. Чтобы активизировать такую возможность, необходимо установить данный флажок.
  - **SSID** — параметр содержит уникальный идентификатор, в частности SSID1. При выборе этого идентификатора необходимо придерживаться тех же правил, что и при выборе главного SSID. Особенно это важно, если вещание SSID отключено и для подключения к сети обязательно нужно точно знать этот SSID. В этом случае можно легко отсеять нежелательные подключения извне.
  - **Security** (Безопасность) — параметр описывает метод аутентификации. При этом дополнительная его настройка возможна лишь в том случае, если в области параметров **Enable VLan Status** (Разрешить виртуальные сети) параметр **Security** (Безопасность) имеет значения **Open** (Открытый) или **Shared** (Разделенный). При этом становятся доступными значения **None** (Никакой), **Open** (Открытый) или **Shared** (Разделенный).
  - **Webkey** (Ключ) — можно выбрать длину ключа шифрования данных, передаваемых в сети между устройствами, использующими гостевой SSID1. Длина ключа может составлять **64**, **128** и **152** бит. Также необходимо сразу же выбрать тип символьной строки (**HEX** или **ASCII**), представляющей ключ, и сам ключ.

- **VLan Group ID** (Идентификатор виртуальной группы) — как и в случае с главной виртуальной группой, дополнительная также должна иметь свой уникальный номер из интервала 1–4095, отличный от номера главной виртуальной группы. В нашем примере главная виртуальная группа под номером **1**, а группа с гостевым SSID1 — **2**.

➢ **Key Index** (Номер ключа) — как обычно, для шифрования данных может использоваться до четырех ключей разной или одинаковой длины. Для переключения между ними предназначен параметр **Key Index** (Номер ключа).

Подобным образом можно настроить еще два гостевых SSID, если, конечно, есть такая необходимость.

18.2. Настройка беспроводного адаптера

Ниже описаны параметры настройки популярного беспроводного USB-адаптера D-Link DWL-G122, который используется для работы в беспроводных сетях стандарта IEEE 802.11g. Даже если у вас установлен другой беспроводный адаптер, принципы его настройки не должны сильно отличаться от описываемых ниже.

После установки драйвера для беспроводного адаптера D-Link DWL-G122, в области уведомлений **Панели задач** появляется значок в виде буквы D.

В дальнейшем настройку адаптера можно будет производить, щелкнув на нем правой кнопкой мыши и выбрав в меню пункт **Wireless Network** (Беспроводная сеть), или просто дважды щелкнув на нем кнопкой мыши.

В результате появится окно программы настройки, содержащее пять вкладок. По умолчанию открывается вкладка **Link Info** (Сведения о соединении), содержащая информацию о текущем соединении: режим сети, используемый беспроводной стандарт, текущая скорость соединения, SSID и др. (рис. 18.16).

Непосредственно параметрами работы устройства управляют на вкладках **Configuration** (Конфигурация) и **Advanced** (Расширенные настройки). Кроме того, настройку параметров подключения ко всем найденным точкам доступа можно осуществлять на вкладке **Site Survey** (Обзор узлов). Рассмотрим их более внимательно.

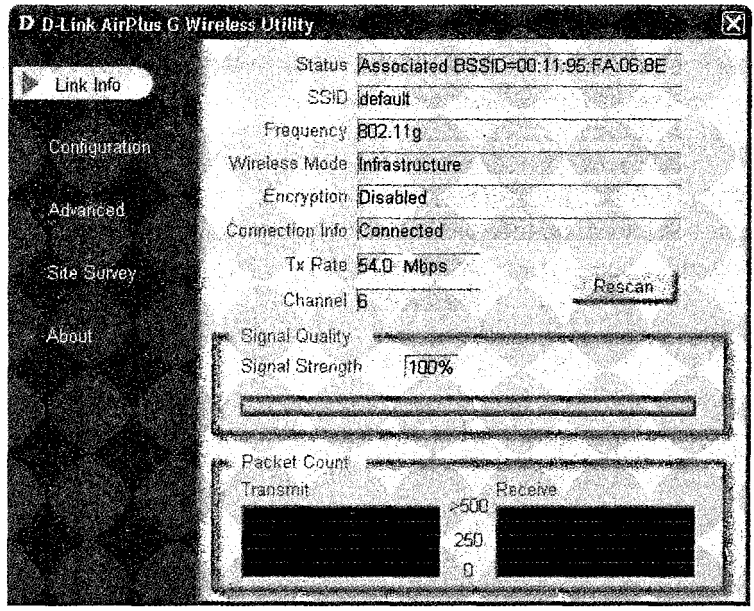


Рис. 18.16. Окно программы конфигурирования, вкладка Link Info (Сведения о соединении)

Выбираем вкладку **Configuration** (Конфигурация) (рис. 18.17). На ней присутствуют следующие параметры.

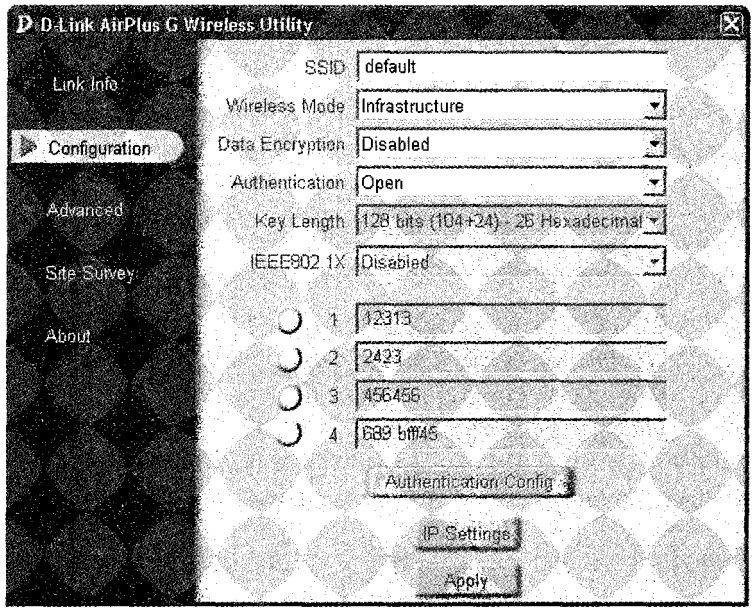


Рис. 18.17. Окно программы конфигурирования, вкладка Configuration (Конфигурация)

- **SSID** — уникальный идентификатор сети. По умолчанию любое беспроводное устройство в качестве SSID имеет слово **default**. Однако если в сети уже настроена точка доступа, данный параметр должен содержать указанный при ее настройке идентификатор.
- **Wireless Mode** (Беспроводной режим) — режим, в котором планируется использовать данное беспроводное устройство. Доступны два варианта: **Infrastructure** (Режим инфраструктуры) и **Ad-Hoc** (Режим «точка-точка»).
- **Data Encryption** (Шифрование данных) — способ шифрования данных, ориентирующийся на существующие технологии и протоколы безопасности. Шифрование данных может быть включено и выключено (варианты **Enabled** (Разрешить) или **Disabled** (Запретить)). Чтобы обеспечить приемлемую защиту сети, естественно, шифрование должно быть разрешено.
- **Authentication** (Аутентификация) — способ прохождения аутентификации при подключении к выбранному устройству. От нее будет зависеть используемый в дальнейшем протокол безопасности. Возможны следующие варианты: **Open** (Открытая), **Shared** (Разделенная), **WPA** и **WPA-PSK**.
- **Key Length** (Длина ключа) — описывает длину ключа, которая будет использоваться при шифровании данных. Доступны варианты:
  - **64 bits (40+24) — 10 Hexadecimal digits** — в этом режиме в качестве ключа может использоваться комбинация из 10 шестнадцатеричных символов (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F);
  - **128 bits (104+24) — 26 Hexadecimal digits** — в этом режиме в качестве ключа может использоваться комбинация из 26 шестнадцатеричных символов (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F);
  - **64 bits (40+24) — 5 Ascii digits** — в качестве ключа может использоваться комбинация из пяти букв, цифр и знаков латинского алфавита;
  - **128 bits (104+24) — 13 Ascii digits** — может использоваться комбинация из 13 букв, цифр и знаков латинского алфавита.
- **IEEE802.1X** — при использовании данного режима будет осуществляться аутентификация по стандарту IEEE 802.1x, которая на сегодняшний день обеспечивает наибольшую защиту сети, хоть и уменьшает ее пропускную способность.

Если выбран режим шифрования данных, предоставляется возможность ввести четыре разных ключа шифрования, которые можно использовать по некоторому графику, выбираемому пользователем. При этом программа проверя-

ет длину и символы вводимых знаков, которые должны соответствовать одному из выбранных правил (только шестнадцатеричные символы или любые латинские символы и знаки).

На вкладке **Advanced** (Расширенные настройки) (рис. 18.18) можно настроить следующие параметры.

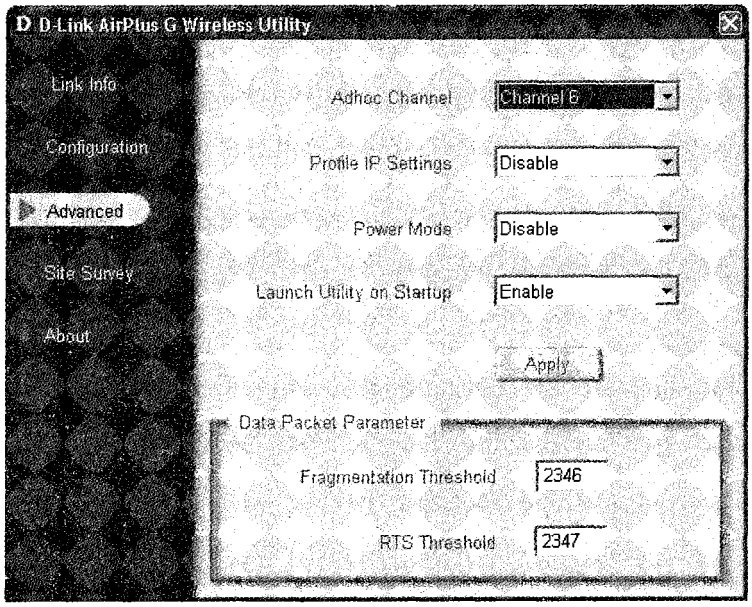


Рис. 18.18. Окно программы конфигурирования, вкладка Advanced (Расширенные настройки)

- **Adhoc Channel** (Канал передачи данных) — используемый для передачи данных канал. Согласно сетевому стандарту IEEE 802.11g весь диапазон частот разбит на 13 каналов, любой из которых может использоваться для нужд передатчика. В данном параметре вы можете указать любой из этих каналов. Иногда полезно бывает использовать конкретный канал, когда знаешь, что он не занят одной из возможных близкорасположенных точек доступа или маршрутизатором. Это позволяет обеспечить минимальную зашумленность эфира и, как следствие, повысить стабильность работы сети и ее высокую пропускную способность.
- **Profile IP Settings** (Использование IP-шаблонов) — с помощью этой утилиты конфигурирования адаптера D-Link DWL-G122 можно настраивать несколько шаблонов с параметрами подключения к разным точкам доступа. Поэтому, чтобы эти шаблоны можно было автоматически использовать, нужно

назначить данному параметру значение **Enable** (Разрешить). Если использование шаблонов не планируется, лучше установить значение **Disable** (Запретить).

- **Power Mode** (Режим энергопотребления) — поскольку при работе передатчика беспроводного адаптера используется достаточно много энергии, что критично для пользователей переносных и наладонных компьютеров, то стандартами предусмотрен режим энергосбережения. Данный параметр может принимать три значения: **Disable** (Запретить), **Min Saving** (Минимальное сбережение энергии), **Max Saving** (Максимальное сбережение энергии). Исходя из потребностей и конкретной ситуации, данный параметр можно менять на свое усмотрение.
- **Launch Utility on Startup** (Запускать утилиту при старте) — данный параметр говорит сам за себя: значение **Enable** (Разрешить) запускает утилиту конфигурирования адаптера вместе со стартом системы. В дальнейшем, когда все параметры адаптера будут настроены и опробованы, данный параметр лучше установить в положение **Disable** (Запретить).
- **Data Packet Parameter** (Параметры пакетов данных) — отвечает за настройку параметров формирования пакетов с данными. Поскольку для шифрования могут использоваться разные методы и ключи, то размер служебной части пакета с данными может значительно изменяться. Если он будет слишком большим, то меньше места останется для полезных данных. В этом параметре имеются две составляющие, подбирая значения которых можно искусственно поднять производительность сети.

Переходим на вкладку **Site Survey** (Обзор узлов) (рис. 18.19). Она содержит очень важную информацию касательно найденных точек доступа, а также шаблоны с настройками, которые можно использовать при подключении к ним. В любой момент вы можете узнать SSID точки доступа, ее MAC-адрес, мощность сигнала, а также посмотреть, к какой из точек доступа в данный момент подключен ваш адаптер. Кроме всего прочего, можно конфигурировать параметры подключения к точкам доступа, добавлять новые, производить фильтрацию по выбранным параметрам и т. д.

Например, чтобы изменить параметры подключения к существующей точке доступа, нужно в области **Available Network** (Доступные сети) выделить нужный пункт и нажать на кнопку **Configure** (Конфигурировать).

В результате откроется окно, в котором можно будет изменить метод шифрования, вариант аутентификации и указать ключи шифрования, которые вы должны заранее узнать у администратора сети (рис. 18.20).

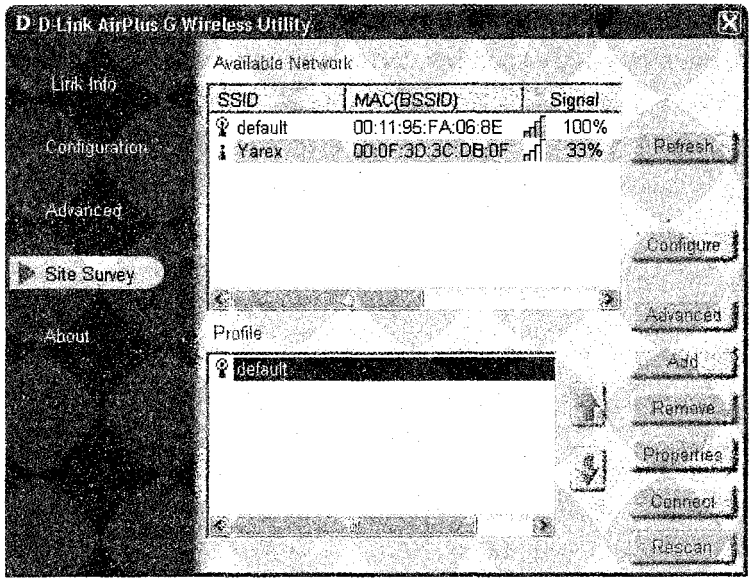


Рис. 18.19. Окно программы конфигурирования, вкладка Site Survey (Обзор узлов)

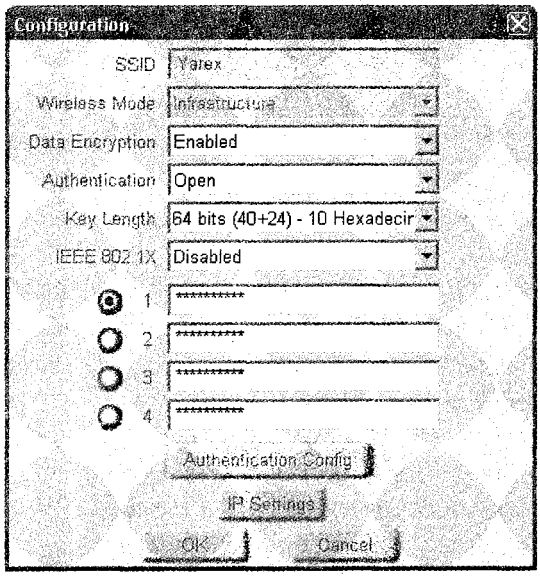


Рис. 18.20. Изменение параметров подключения к сети

Здесь сразу можно будет настроить IP-адрес, маску подсети и другие конфигурационные параметры, чтобы можно было подключиться к точке доступа с правильными параметрами (рис. 18.21). Чтобы это сделать, достаточно нажать на кнопку **IP Settings** (Настройки IP) в нижней части окна (см. рис. 18.20).

При этом появится окно настройки, очень напоминающее окно настройки аналогичных параметров с помощью стандартного механизма Windows (рис. 18.22). Так, здесь можно указать IP-адрес, маску подсети, адрес шлюза, адреса предпочитаемого и дополнительного DNS-серверов, настроить адрес прокси-сервера и многое другое, что обязательно вам пригодится, когда вы будете использовать общий Интернет.

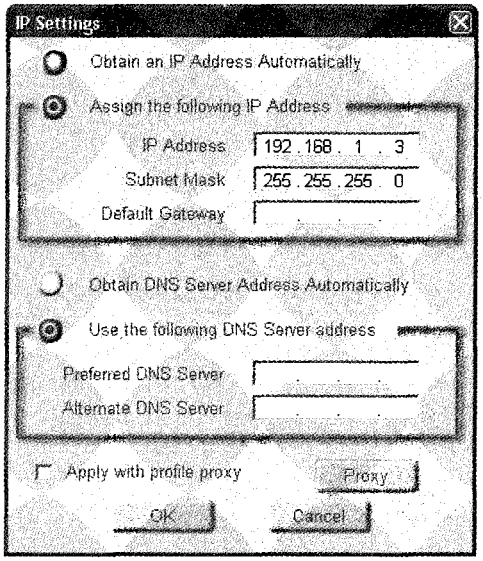


Рис. 18.21. Настраиваем IP-адрес, маску подсети и другие параметры

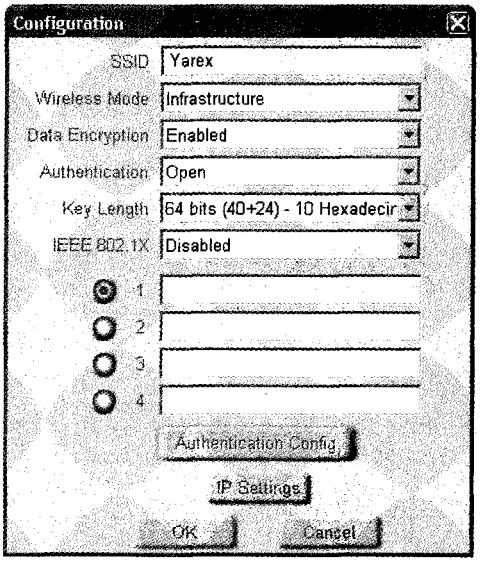


Рис. 18.22. Настройка шаблона с параметрами для подключения к точке доступа

Вместо того чтобы постоянно изменять параметры подключения к точке доступа, вы можете просто использовать разные шаблоны с параметрами, которые очень легко создать. Для этого нужно нажать кнопку **Add** (Добавить) в окне, изображенном на рис. 18.19.

При этом откроется окно, аналогичное окну редактирования параметров точки доступа, только многие поля ввода будут пустыми. Их нужно будет заполнить самостоятельно. Например, чтобы создать шаблон для подключения к точке доступа **Yarex**, введите имя шаблона `Yarex` и настройте все остальные известные вам параметры. После этого нажмите кнопку **OK** и проверьте созданный шаблон на практике: попробуйте подключиться к сети **Yarex**, выделив соответствующий шаблон и нажав кнопку **Connect** (Подключиться).

Глава 19

Настройка компьютера в Windows XP

- Настройка параметров сети и проверка связи с сервером
- Работа с общими ресурсами

Microsoft Windows XP заслуженно заняла свое место среди применяемых операционных систем. Хорошая защищенность и отказоустойчивость, легкость в эксплуатации, широкие возможности и многое другое — все это нравится пользователям. Очень многие предпочитают работать в данной операционной системе как на рабочем, так и на домашнем компьютере. Поэтому, если вы хотите использовать ее для работы в локальной сети, нужно знать, как правильно устанавливать и настраивать сетевой клиент, протокол, службу и т. д. Также необходимо уметь создавать общие ресурсы, подключаться и пользоваться ими.

19.1. Настройка параметров сети и проверка связи с сервером

Итак, придерживаясь первоначального алгоритма, нам осталось лишь подключить компьютер к уже созданной сети, воспользовавшись для этого уже установленным сервером. Имея в сети сервер, можно легко проверить правильность подключения сетевого компьютера. Именно поэтому мы первым делом настроили сервер.

Если вы создали домашнюю сеть, не расстраивайтесь по поводу отсутствия сервера: проверить связь вы сможете с помощью любого из коммутаторов или маршрутизатора. Однако об этом позже.

Подключение к домену или рабочей группе

Первым делом нам необходимо настроить на компьютере параметры сети, используя для этого данные об адресации и имени (именах) рабочей группы или домена.

ПРИМЕЧАНИЕ

Из видеоурока «Урок 19.1. Подключение к домену в Microsoft Windows XP», который находится на компакт-диске, прилагаемом к книге, вы узнаете, как происходит подключение к домену.

Итак, начнем. Для начала настроим домен или рабочую группу. Для этого щелкните правой кнопкой мыши на значке **Мой компьютер** и в появившемся меню выберите пункт **Свойства**.

Откроется окно свойств системы, содержащее несколько вкладок. В данный момент нас интересует вкладка **Имя компьютера** (рис. 19.1). Первым делом на ней

вы можете изменить описание компьютера, которое будет отображаться в окне проводника рядом с именем вашего компьютера в сети. Для этого используйте поле **Описание**.

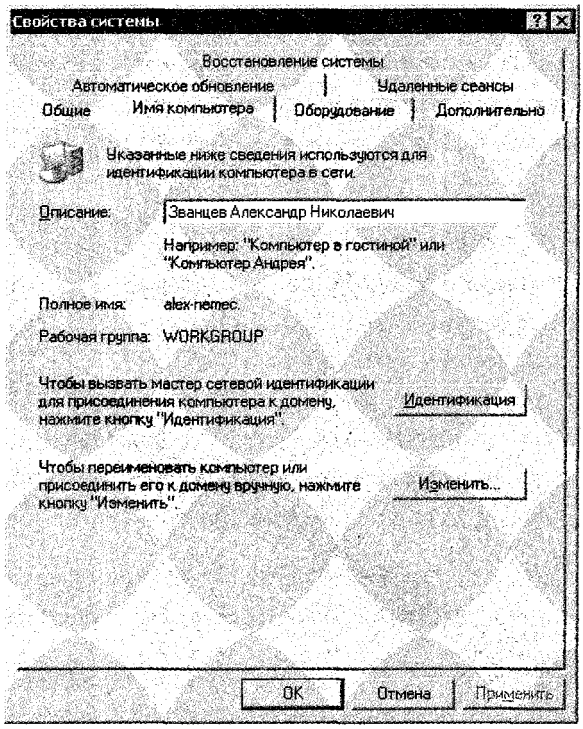


Рис. 19.1. Содержимое вкладки Имя компьютера

Подсоединить компьютер к домену или рабочей группе можно двумя способами — простым и сложным. При этом простой путь подойдет пользователям, которые уже не раз сталкивались с подобного рода действием. Сложный же более информативный[1] и, наверное, подойдет неподготовленному пользователю. С другой стороны, если у вас на руках уже имеются все необходимые данные для регистрации в сети, тогда лучше выбрать именно первый вариант, поскольку он более понятен. Так мы и сделаем.

Чтобы пойти простым путем, нажимаем кнопку **Изменить**. В результате появится окно (рис. 19.2), в котором нужно будет указать имя домена или группы.

[1] Данный путь изобилует достаточно путаными шагами и непонятными словами, поэтому начинающие пользователи часто применяют упрощенный способ настройки.

Так, если в сети имеется домен, вам необходимо будет указать, что компьютер является членом домена, и ввести его имя. В противном случае укажите, что компьютер принадлежит рабочей группе, и укажите ее имя. Здесь же можно изменить имя компьютера, под которым он будет отображаться в сети.

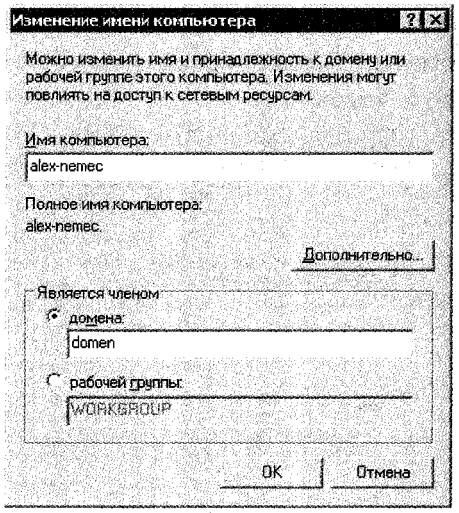


Рис. 19.2. Указываем имя домена или группы

Если вы используете доменную систему, после нажатия кнопки **OK** появится окно с требованием ввести логин и пароль доступа пользователя, который имеет право подсоединиться к домену. Это означает, что данный пользователь должен уже быть зарегистрирован в Active Directory. Если вы еще не зарегистрированы, подключиться к домену можно под любой другой учетной записью, например попросить об этой услуге администратора сети.

Если введенные данные верны, после нескольких секунд вы окажетесь в домене, о чем будет свидетельствовать соответствующее сообщение.

Если вы подключаетесь к рабочей группе, появится сообщение о том, что вы подключились к группе с указанным названием.

Теперь, чтобы полноценно войти в домен или группу, необходимо перезапустить компьютер, о чем и сообщит вам надпись в нижней части окна, показанного на рис. 19.1.

Настройка протокола

Настроив подключение к домену или группе, вы подготовили компьютер к вхождению в сетевую рабочую группу, но не более того. Если в сети имеется статическая адресация, вы не сможете в нее полноценно войти и работать. Чтобы это сделать, вам придется еще выполнить настройку IP-протокола.

Прежде всего необходимо открыть свойства IP-протокола используемого сетевого подключения. Для этого найдите на **Рабочем столе** значок **Сетевое окружение**, щелкните на нем правой кнопкой мыши и в появившемся меню выберите

пункт **Свойства**. В результате должно появиться окно со списком сетевых подключений (рис. 19.3).

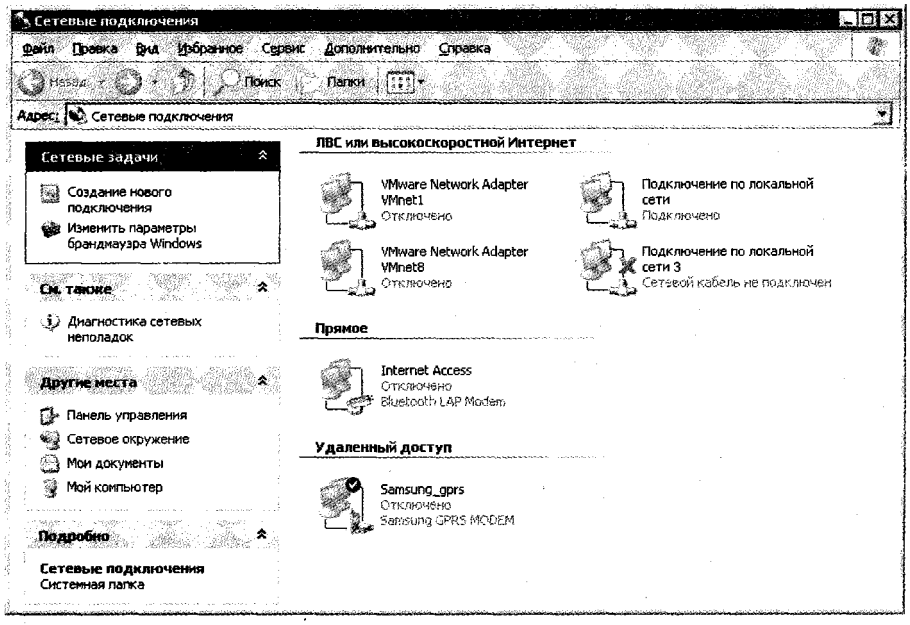


Рис. 19.3. *Список сетевых подключений*

ПРИМЕЧАНИЕ

Если на Рабочем столе значка Сетевое окружение нет, то он обязательно будет на Панели управления или в меню Пуск.

Количество сетевых подключений может быть разным. Ведь они создаются автоматически в случае, если вы подключаете Bluetooth-адаптер, используете выход в Интернет через модем или подключаетесь к другому компьютеру с помощью любого вида связи. Поэтому не удивляйтесь, если в открывшемся окне вы увидите несколько неактивных сетевых подключений.

В случае если к компьютеру никаких устройств не подключалось и к другим машинам он не подсоединялся, открыв окно, вы обнаружите всего одно сетевое подключение.

Как бы там ни было, щелкнув правой кнопкой мыши на активном сетевом подключении и выбрав в появившемся меню пункт **Свойства**, вы увидите окно, показанное на рис. 19.4.

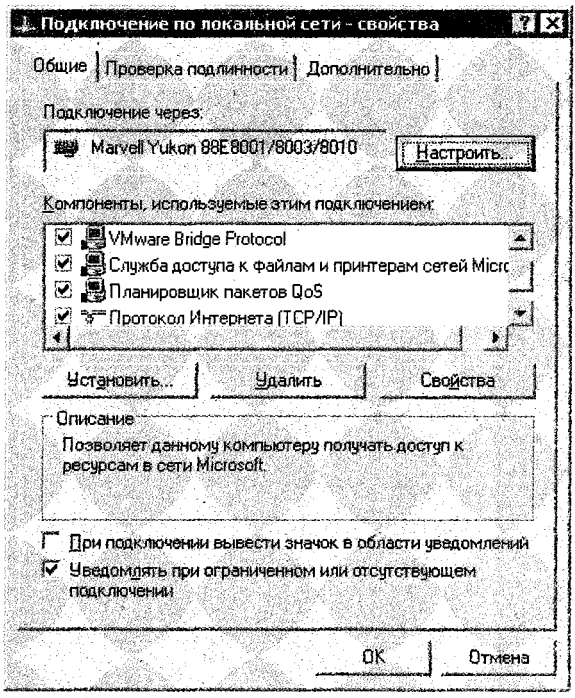


Рис. 19.4. Свойства выбранного сетевого подключения

Теперь, чтобы настроить IP-протокол, найдите его (**Протокол Интернета (TCP/IP)**) в списке среди других протоколов и служб подключения и дважды щелкните на нем кнопкой мыши или нажмите кнопку **Свойства**. Для ввода IP-адреса и маски подсети используются поля **IP-адрес** и **Маска подсети** (рис. 19.5).

Если в сети настроен DNS-сервер, необходимо установить переключатель в положение **Использовать следующие адреса DNS-серверов** и в поле **Предпочитаемый DNS-сервер** ввести его IP-адрес.

Если в сети с доменом настроен DHCP-сервер и выдача адресов производится автоматически, необходимо установить переключатель в положение **Получить IP-адрес автоматически**.

В принципе, на этом настройку протокола можно закончить, поскольку этого вполне хватает для нормальной работы в локальной сети. Здесь также можно добавить и адреса шлюзов (маршрутизаторов), если таковые имеются, что позволит получить доступ к сегментам сети с другой адресацией. Для этого нажмите кнопку **Дополнительно** и введите нужные IP-адреса с помощью кнопки **Добавить**.

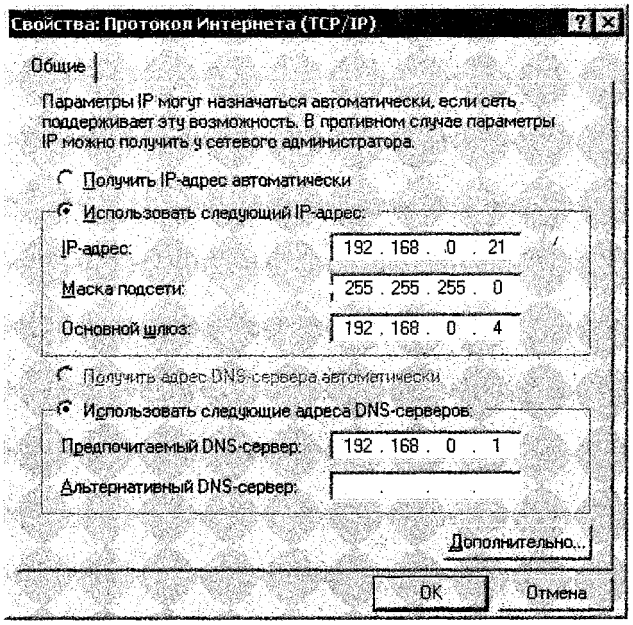


Рис. 19.5. Настраиваем IP-адрес, маску подсети и другие параметры

Проверка связи

После подключения компьютера к сети и настройки ее параметров может так оказаться, что, перезагрузив компьютер, вы не сумеете подключиться к этой сети. Причиной может быть ошибка при настройке или физическая ошибка сети, например неправильно обжатый кабель, обрыв кабеля, неисправный порт на концентраторе или коммутаторе и т. д.

Самый простой способ проверить связь — использовать системную утилиту ping.

Первым делом необходимо открыть командную строку. Для этого выберите **Пуск ▸ Программы ▸ Стандартные ▸ Командная строка**. Далее наберите в строке следующее: `ping 192.168.0.1`.

ВНИМАНИЕ

В качестве адреса в примере указан адрес домена сети. Вы же можете вводить любой другой, используемый в вашей сети, например адрес коммутатора, к которому вы подключены.

В случае если физическая связь с указанным адресом существует, то есть кабель не поврежден и оборудование исправно, вы увидите результат, показанный на рис. 19.6. По умолчанию программа посылает по указанному IP-адресу

всего четыре пакета, чего вполне достаточно для проверки связи. При наличии связи вы видите время ответа, которое в нашем случае составляет менее 1 мс. Также возможна ситуация, когда этот показатель колеблется в широком диапазоне. Это значит, что связь есть, но она далеко не самая устойчивая и быстрая, что, в свою очередь, означает слишком большую длину сегмента или наличие коллизий в сети. В этом случае можно попробовать подключить кабель к другому порту на концентраторе или коммутаторе.

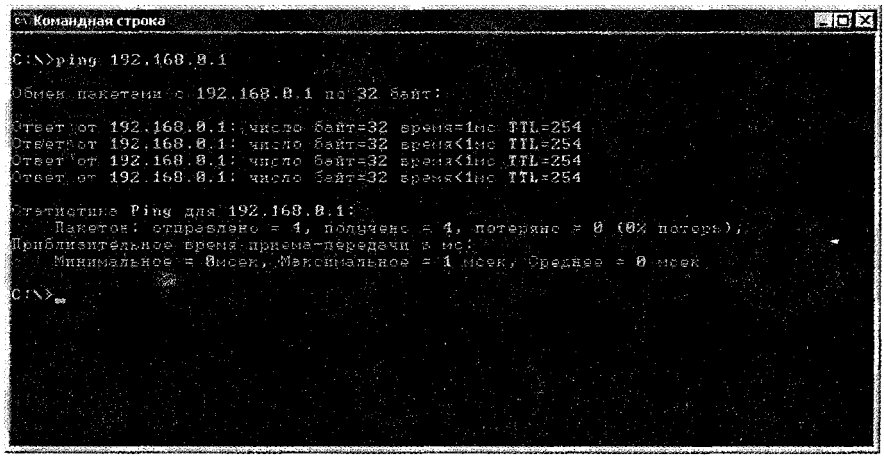


Рис. 19.6. Удачное выполнение команды

Если связи с указанным устройством не существует, вы увидите результат, показанный на рис. 19.7. В этом случае необходимо проверить следующее:

Рис. 19.7. Неудачное выполнение команды

- IP-адрес;
- маску подсети;
- рабочую группу или домен;
- корректность установки сетевой карты (используйте **Диспетчер устройств**);
- если сетевая карта неинтегрированная, контакт в слоте с адаптером или портом (если используется USB-адаптер);
- работоспособность адаптера (должен гореть индикатор связи на задней панели);
- правильность обжима коннекторов на кабеле;
- состояние всех портов, которые задействованы для подключения вашего компьютера.

19.2. Работа с общими ресурсами

Главный плюс сети — доступ к ресурсам. И если вы работаете в Windows XP, вам нужно уметь правильно использовать чужие и раздавать свои.

Предоставление доступа к дискам и их содержимому

ПРИМЕЧАНИЕ

Из видеоурока «Урок 19.2. Настройка общего доступа к файловым ресурсам в Microsoft Windows XP», который находится на компакт-диске, прилагаемом к книге, вы узнаете, как настроить общий доступ к файловым ресурсам.

Для начала откройте окно **Проводника**. В Windows XP общий доступ устанавливается отдельно на каждую папку, поэтому первым делом определитесь с папками, которые вы хотите отдать «на растерзание» сетевым пользователям.

Далее выполните следующие действия. Выделите папку, которую вы хотите отдать в общее пользование, и щелкните на ней правой кнопкой мыши. Затем в появившемся меню выберите пункт **Общий доступ и безопасность**.

В результате появится окно, содержащее несколько вкладок. Для управления доступом перейдите на вкладку **Доступ**. В зависимости от того, подключены вы к домену или нет, содержимое этой вкладки может быть разным. Рассмотрим оба случая.

Без использования домена

В этом случае вы увидите окно, показанное на рис. 19.8.

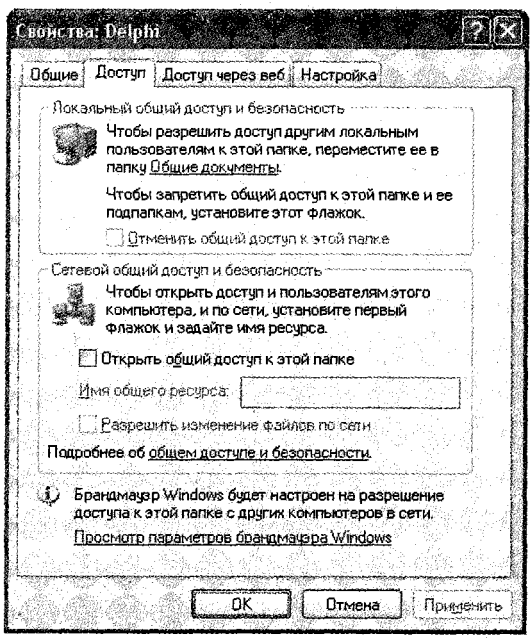


Рис. 19.8. Настраиваем доступ к файловому ресурсу в сети без домена

Для управления доступом в сети используется область **Сетевой общий доступ и безопасность**. Теперь, чтобы открыть доступ к папке, установите переключатель в положение **Открыть общий доступ к этой папке**. Если вы хотите, чтобы другие пользователи могли вносить изменения в документы, установите флажок **Разрешить изменение файлов по сети**. Нажмите кнопку **OK**, операционная система начнет изменять права доступа к папке, о чем будет свидетельствовать появление небольшого окна с анимированным содержимым.

С использованием домена

В этом случае вы увидите окно, показанное на рис. 19.9.

На открытой по умолчанию вкладке **Доступ** установите переключатель в положение **Открыть общий доступ к этой папке**. Затем нужно указать права доступа к этому ресурсу. Для этого нажмите кнопку **Разрешения**. По умолчанию доступ к папке открыт для всех пользователей на одинаковых правах — только для чтения.

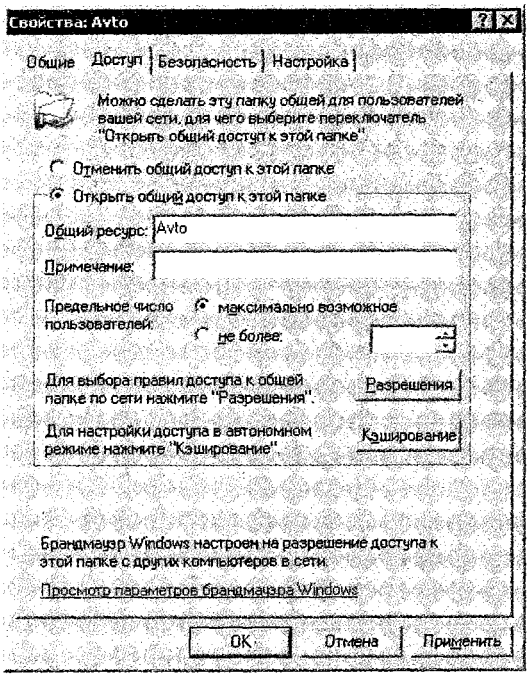


Рис. 19.9. Настраиваем доступ к файловому ресурсу в сети с доменом

Если вас это устаивает, больше никаких действий производить не нужно. Если вы хотите настроить разные права для разных пользователей, нажмите кнопку **Добавить**. Далее вы увидите уже знакомое окно добавления пользователей из домена (см. рис. 16.14). Об этом читайте в разделе 16.6 «Настройка общего доступа».

Чтобы отменить общий доступ к ресурсу, в окнах, представленных на рис. 19.8 и 19.9, установите переключатель в положение **Отменить общий доступ к этой папке** соответственно.

Описанным образом можно установить общий доступ на произвольное количество папок.

Предоставление доступа к принтерам

ПРИМЕЧАНИЕ

Из видеоурока «Урок 19.3. Настройка общего доступа к принтеру в Microsoft Windows XP», который находится на компакт-диске, прилагаемом к книге, вы узнаете, как настроить общий доступ к принтеру.

Часто бывает так, что кому-то нужно распечатать информацию, а принтера у него под рукой нет. Если вы подключены к сети и у вас есть принтер, вы можете стать настоящим спасителем, если предоставите его в общее пользование. Тем более что сделать это не составляет особого труда. Главное, не переборщить с разрешениями.

Итак, прежде всего откройте группу **Принтеры и факсы**, для чего выберите **Пуск ▸ Настройка ▸ Принтеры и факсы**. Далее щелкните правой кнопкой мыши на принтере и в появившемся меню выберите пункт **Общий доступ**.

Откроется окно с несколькими вкладками. Чтобы настроить доступ к принтеру, перейдите на вкладку **Доступ**. Опять же ее содержимое может отличаться в зависимости от того, подключены вы к домену или нет.

Так, если доменная система не используется, вам достаточно установить переключатель в положение **Общий доступ к данному принтеру** и ввести его сетевое имя.

Если же в сети используется домен, установите переключатель в положение **Общий доступ к данному принтеру** и введите название, под которым этот принтер будет отображаться в сетевом окружении (рис. 19.10). Здесь же можно указать, что сведения о принтере необходимо добавить в Active Directory. Для этого установите флажок **Внести в Active Directory**.

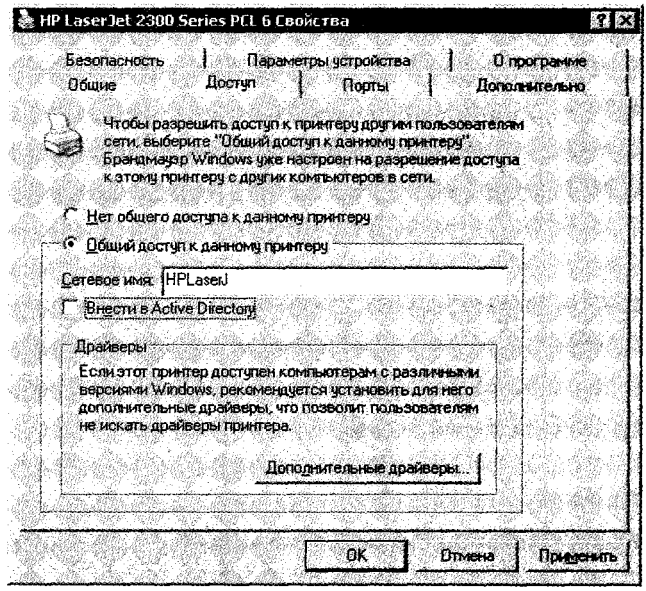


Рис. 19.10. Открываем общий доступ к принтеру

ПРИМЕЧАНИЕ

Информация из Active Directory иногда бывает нужна при подключении сетевого принтера. Однако наиболее часто используется возможность прямого подключения к компьютеру, поэтому установка флажка Внести в Active Directory не столь важна.

После этого, если вы хотите настроить права доступа к принтеру, перейдите на вкладку **Безопасность**.

По умолчанию к вашему принтеру получат доступ все участники сети, с ограничением, что они не смогут управлять чужими заданиями печати. Вы также можете назначить каждому разные права, предварительно добавив их в группу пользователей принтера. О том, как это сделать, подробно рассказано в разделе 16.6 «Настройка общего доступа».

На этом настройку общего доступа к принтеру можно считать законченной.

Подключение сетевой папки

ПРИМЕЧАНИЕ

Из видеоурока «Урок 19.4. Подключение к общим ресурсам в Microsoft Windows XP», который находится на компакт-диске, прилагаемом к книге, вы узнаете, как подключиться к сетевой папке.

Предположим, недавно вы узнали, что в вашей сети — корпоративной, офисной или домашней — есть компьютер, на котором существует общая папки с партией новых фильмов, и вам очень хочется их пересмотреть. Так в чем же дело?

Откройте **Проводник** и выберите в левой его части **Сетевое окружение**. Зная название нужного компьютера, найдите его в сетевом окружении и выделите.

При этом в правой части окна **Проводника** отобразятся все ресурсы, которые данный компьютер отдает в общее пользование.

Вот и заветная папка **Video**. Щелкните на ней правой кнопкой мыши и в появившемся меню выберите команду **Подключить сетевой диск**.

Откроется окно подключения сетевого диска (рис. 19.11). В нем вам нужно указать диск, на котором будет отображаться содержимое выбранной вами папки **Video**. Если вы хотите, чтобы этот диск подключался каждый раз, когда вы заходите в Windows, установите флажок **Восстанавливать при входе в систему**.

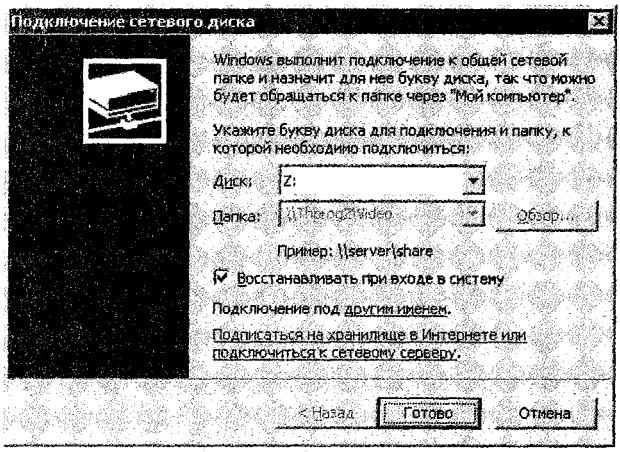


Рис. 19.11. Подключаем сетевой диск

Вот и все — наслаждайтесь просмотром любимых фильмов!

Подключение сетевого принтера

ПРИМЕЧАНИЕ

Из видеоурока «Урок 19.4. Подключение к общим ресурсам в Microsoft Windows XP», который находится на компакт-диске, прилагаемом к книге, вы узнаете, как настроить общий доступ к принтеру.

Если нужно распечатать какую-либо информацию, а принтер к компьютеру не подключен, не обязательно бежать с диском к соседу, если между вашими компьютерами установлена сеть. Достаточно подключить его принтер в качестве сетевого. Конечно, при условии, что на соседский принтер установлен общий доступ (см. подраздел «Предоставление доступа к принтерам»).

Самый простой способ подключить сетевой принтер следующий. Откройте в **Проводнике** сетевое окружение и выделите компьютер, который предоставляет доступ к принтеру. Затем дважды щелкните кнопкой мыши на принтере в правой части окна либо нажмите правую кнопку мыши на нем и в появившемся меню выберите пункт **Подключить**.

Теперь можно печатать.

Глава 20

Настройка компьютера в Windows Vista

- Подключение к сети
- Работа с общими ресурсами

Операционная система Windows Vista начинает свое наступление на компьютеры пользователей, и остановить его уже невозможно. Любой, кто обладает достаточно мощным компьютером, даже просто ради интереса ставит эту систему и пробует с ней работать. Ну а тот, кто уже пользуется ею давно, привык и расставаться с ней не собирается.

Поэтому, если вы обладатель операционной системы Windows Vista в любом исполнении, вам необходимо уметь подключить компьютер к сети и научиться использовать общие ресурсы и предоставлять свои ресурсы соседям.

20.1. Подключение к сети

Как только вы подсоединяете к компьютеру сетевой кабель и включаете компьютер, Vista сразу же обнаруживает сеть и сохраняет о ней информацию. Однако подключиться к сети система сразу не захочет и предложит пройти некий путь подключения.

ПРИМЕЧАНИЕ

Видеоурок «Урок 20.1. Подключение к сети в Microsoft Windows Vista», который находится на компакт-диске, прилагаемом к книге, демонстрирует подключение к сети в Microsoft Windows Vista.

Теперь обо всем по порядку.

Первым делом откройте **Панель управления**. Найдите и перейдите по ссылке **Сеть и Интернет** (рис. 20.1).

В результате откроется окно (рис. 20.2), в котором отображается текущее состояние подключения к найденной сети. Также здесь находятся механизмы настройки доступа к файловым ресурсам компьютера и его принтерам.

Настройка протокола

Наша задача — настроить IP-протокол, указав IP-адрес компьютера, маску подсети, IP-адрес DNS-сервера и т. д. Чтобы иметь возможность настройки указанных параметров, в окне **Центр управления сетями и общим доступом** (см. рис. 20.2) перейдите по ссылке **Управление сетевыми подключениями**.

Откроется окно со списком сетевых подключений. Щелкнув на нужном подключении правой кнопкой мыши, выберите в появившемся меню пункт **Свойства**.

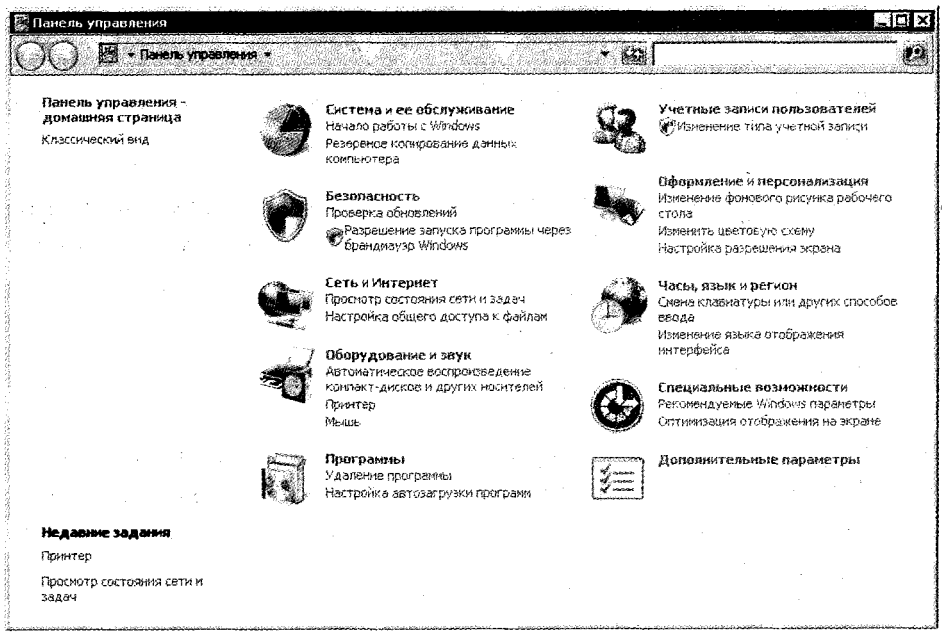


Рис. 20.1. Находим и запускаем ссылку Сеть и Интернет

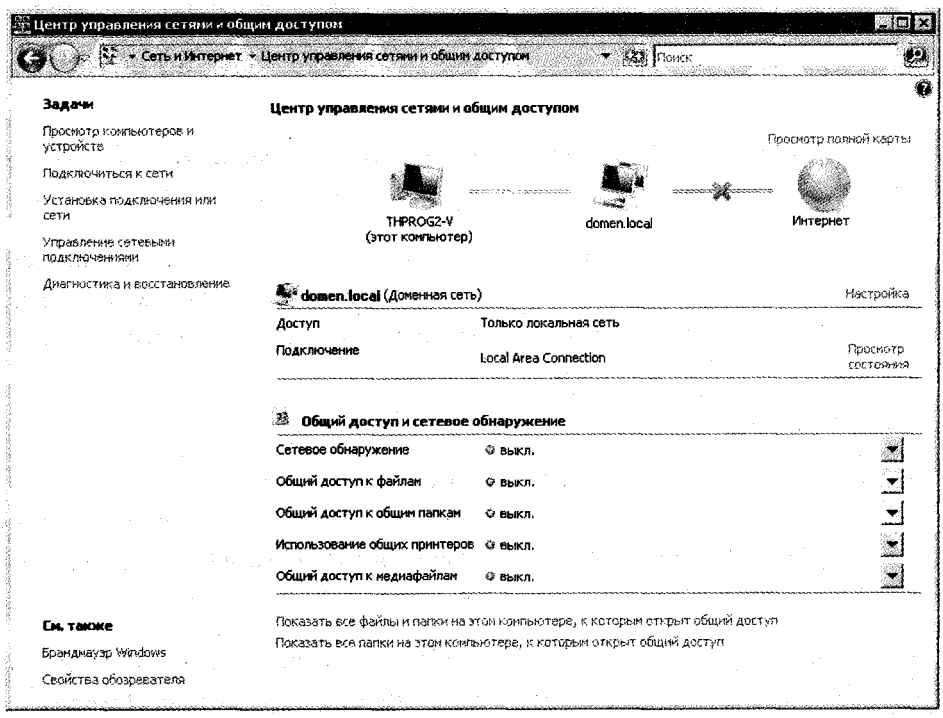


Рис. 20.2. Центр управления сетями и общим доступом

После этого появится окно свойств выбранного сетевого подключения (рис. 20.3). В отличие от аналогичного окна в Windows XP, здесь находится гораздо больше протоколов и служб, однако сути дела это не меняет.

Нас интересует позиция **Протокол Интернета версия 4 (TCP/Ipv4)**. Двойным щелчком кнопки мыши вы инициируете появление окна настройки IP-протокола (рис. 20.4).

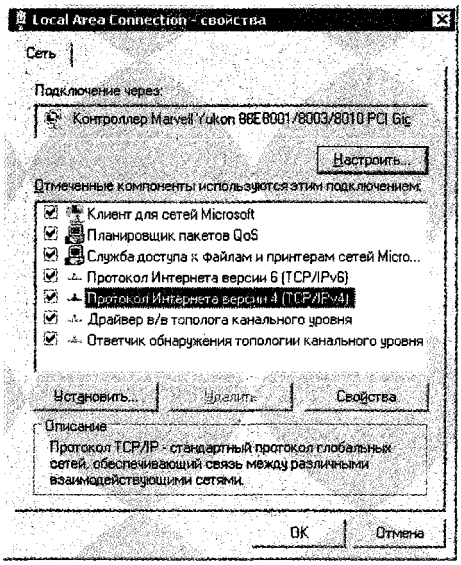


Рис. 20.3. Свойства выбранного сетевого подключения

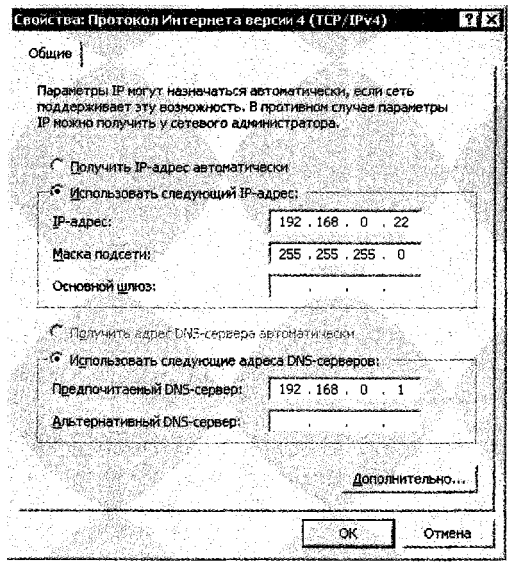


Рис. 20.4. Вводим необходимые данные

Имея на руках все необходимые данные, вводим их в соответствующие позиции.

После того как будет нажата кнопка **OK**, вы сможете полноправно присоединиться к домену или рабочей группе.

Настройка сетевого обнаружения

Хотя подсоединение к сети уже настроено, вы все равно не сможете видеть ее компьютеры. Для того чтобы это стало возможным, вам необходимо произвести дополнительные настройки сетевого окружения.

Для этого вернитесь к окну, показанному на рис. 20.2, и нажмите кнопку со стрелкой напротив надписи **Сетевое обнаружение**. В результате эта позиция расширится и появятся два параметра. Чтобы позволить компьютеру видеть дру-

гие машины сети и обозначить себя, установите переключатель в положение **Включить сетевое обнаружение** (рис. 20.5). После этого нажмите кнопку **Применить**. В результате служба начнет свою работу, о чем будет свидетельствовать зеленый индикатор **вкл.** напротив надписи **Сетевое обнаружение**.

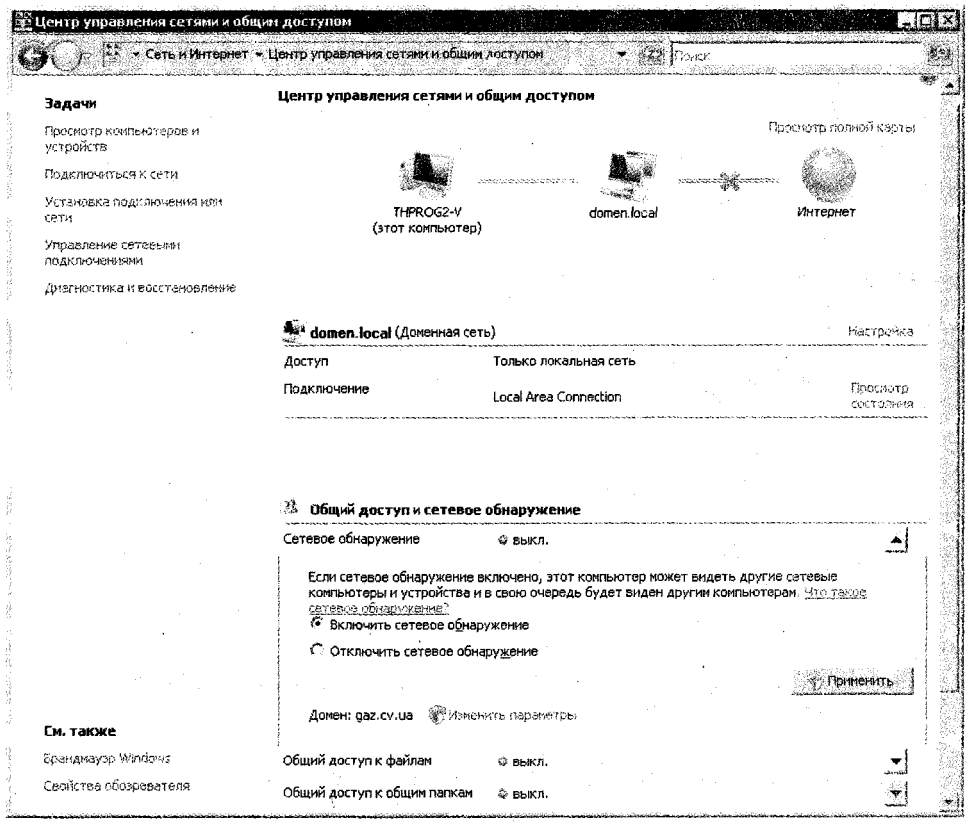


Рис. 20.5. Активизируем службу сетевого обнаружения

На этом настройка сети завершена.

Проверка связи

Если после настройки операционной системы вы не можете попасть в сеть, значит, вы ввели неправильные данные при настройке протокола или имеется какое-то физическое повреждение сетевого оборудования.

Проверка связи с сервером или другим устройством сети осуществляется по принципу, описанному для операционной системы Windows XP (см. главу 19).

20.2. Работа с общими ресурсами

Локальная сеть, как вы понимаете, подразумевает наличие для ее участников общих ресурсов, то есть вы должны уметь использовать чужие и предоставлять свои. Ниже описана последовательность действий, которые необходимо выполнить в Windows Vista для комфортной работы в сети.

В данной операционной системе предоставление ресурса для общего использования происходит в два этапа. Прежде всего необходимо активизировать соответствующую возможность и только потом можно добавлять права на использование ресурса.

Предоставление файлового ресурса

По умолчанию, даже если вы уже подключены к сети, возможность доступа к вашим ресурсам заблокирована, что сделано в угоду повышенной безопасности системы.

ПРИМЕЧАНИЕ

Из видеоурока «Урок 20.2. Настройка общего доступа к файловым ресурсам в Microsoft Windows Vista», который находится на компакт-диске, прилагаемом к книге, вы узнаете, как настроить общий доступ к файловым ресурсам.

Прежде всего откройте **Пуск ▸ Панель управления ▸ Сеть и Интернет ▸ Центр управления сетями и общим доступом**.

Далее в появившемся окне (рис. 20.6) нажмите кнопку со стрелкой напротив надписи **Общий доступ к файлам**. В результате требуемая секция расширится, появятся два переключателя. Для того чтобы активизировать функцию общего доступа к файлам, установите переключатель в положение **Включить общий доступ к файлам**.

После нажатия кнопки **Применить** данная функция активизируется, о чем будет свидетельствовать зеленый цвет индикатора рядом с надписью **Общий доступ к файлам**.

Теперь рассмотрим, как можно настроить общий доступ к конкретной папке.

Используя **Проводник**, найдите папку, которую вы планируете предоставить в общее пользование. Щелкнув на ней правой кнопкой мыши, в появившемся меню выберите пункт **Общий доступ**.

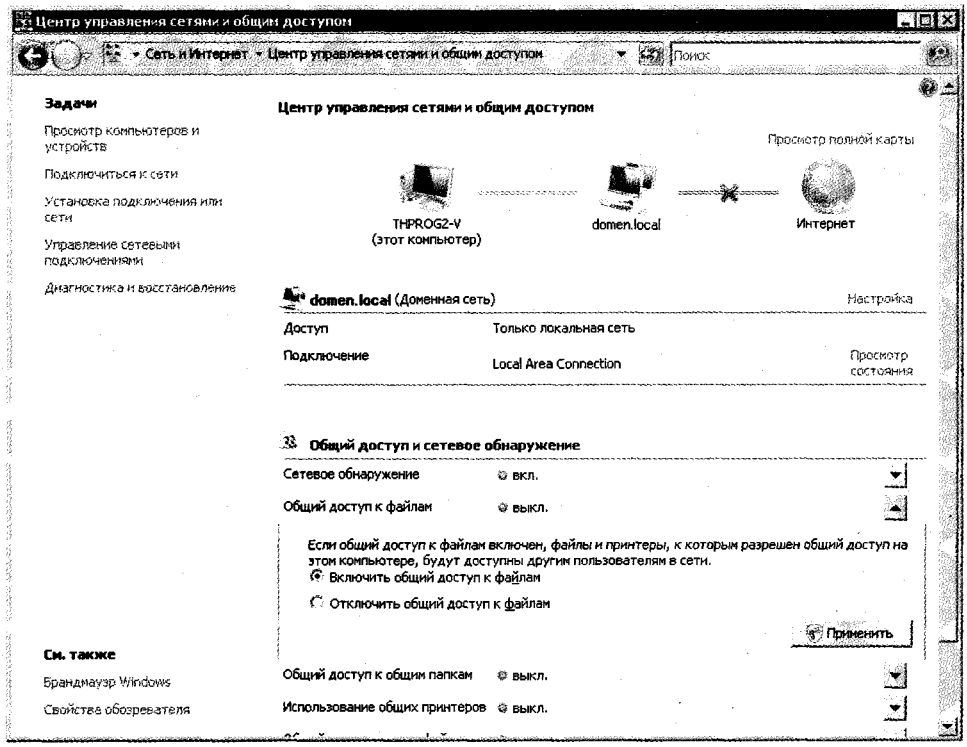


Рис. 20.6. Настраиваем общий доступ к файлам

Откроется окно (рис. 20.7), отображающее пользователей и группы, которые имеют доступ к вашему ресурсу. По умолчанию, кроме владельца компьютера, доступа никто не имеет, но это очень легко исправить. Например, открыв список, можно выбрать группу **Все**, что позволит всем видеть вашу папку. Для добавления этой группы в список используйте кнопку **Добавить**.

Непонятно почему, но создатели Windows Vista не позволяют в этом окне настраивать права более прозрачно, нежели выбором одного из вариантов доступа: **Читатель**, **Соавтор** или **Совладелец**. Тем не менее это можно сделать позже. По умолчанию группа или пользователь добавляется с правами **Читатель**. Если вы уже знаете более детально, что означает каждый из вариантов, то можете сменить права доступа прямо здесь, щелкнув правой кнопкой мыши на группе или пользователе.

Как бы там ни было, после нажатия кнопки **Общий доступ** система произведет некоторые манипуляции, в результате которых будет открыт общий доступ к папке (рис. 20.8).

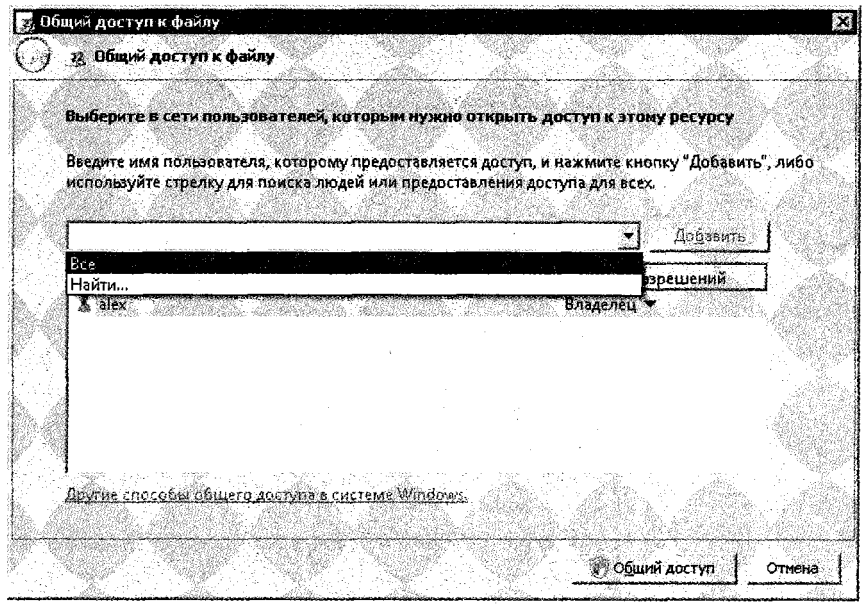


Рис. 20.7. Добавляем права доступа

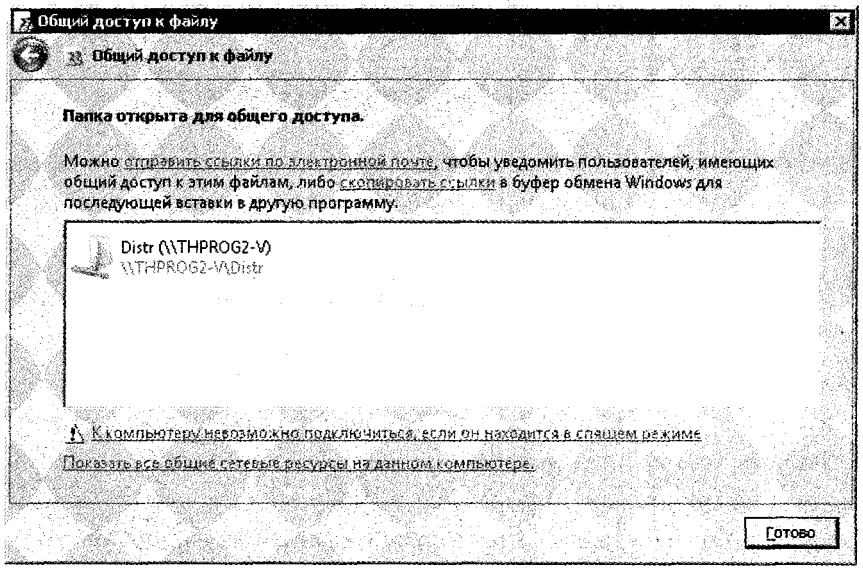


Рис. 20.8. Общий доступ к папке открыт

Теперь, если вы хотите настроить права некоторым пользователям более точно, сделайте следующее. Опять используйте **Проводник**, щелкните правой кнопкой мыши на нужной папке и выберите в появившемся меню пункт **Свойства**.

В появившемся окне (рис. 20.9) нажмите кнопку **Дополнительный доступ**.

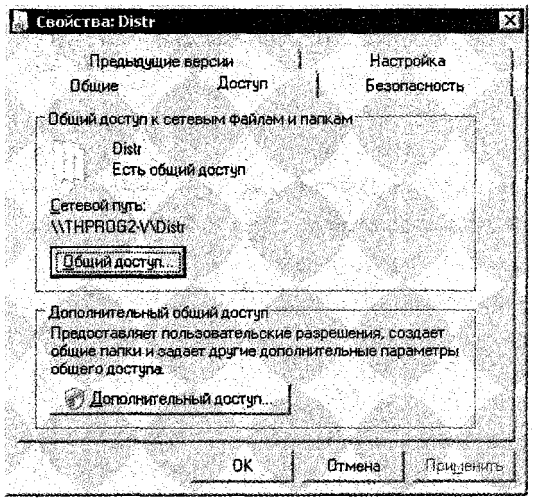


Рис. 20.9. Настраиваем дополнительный доступ

В результате откроется окно (рис. 20.10), в котором можно настраивать разрешения для каждого из пользователей и групп, у которых есть доступ к этой папке. Прежде чем перейти к настройке этих прав, обратите внимание на то, что здесь можно ограничить количество одновременных подключений. Об этом вы вспомните, когда ощутите заметное торможение компьютера из-за злоупотребления ресурсом. В этом случае просто уменьшите количество одновременных подключений до минимума, например до 2–3 человек.

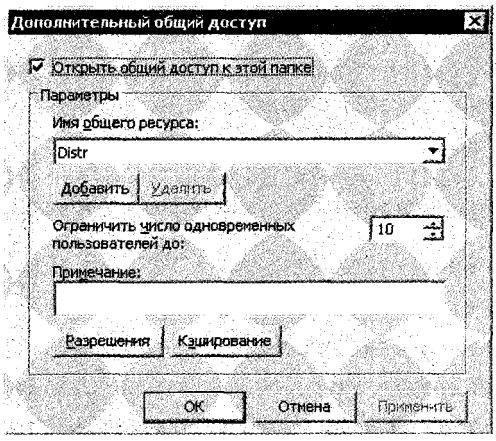


Рис. 20.10. Окно Дополнительный общий доступ

Чтобы настроить разрешения для конкретных пользователей или групп, нажмите кнопку **Разрешения**. В появившемся окне (рис. 20.11) вы увидите список всех пользователей, которым разрешен доступ к данному ресурсу. Чтобы добавить новых, нажмите кнопку **Добавить**. Процесс добавления пользователей уже был описан ранее, поэтому можете обратиться за помощью к разделу 16.6.

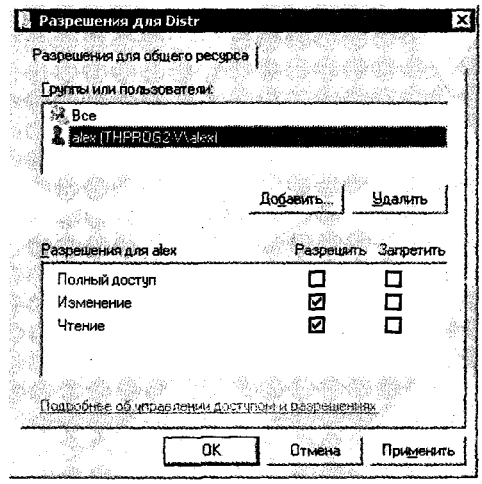


Рис. 20.11. Настраиваем разрешения для каждой позиции

Что касается отключения доступа к общей папке, то это можно сделать несколькими способами. Например, можно снять флажок **Открыть общий доступ к этой папке** в окне, показанном на рис. 20.10. Второй вариант — нажать кнопку **Общий доступ** в окне **Свойства папки** (см. рис. 20.9) и в появившемся окне выбрать позицию **Прекратить доступ**.

Предоставление принтера

ПРИМЕЧАНИЕ

Из видеоурока «Урок 20.3. Настройка общего доступа к принтеру в Microsoft Windows Vista», который находится на компакт-диске, прилагаемом к книге, вы узнаете, как настроить общий доступ к принтеру.

Как и в случае с файловыми ресурсами, предоставление общего доступа к принтеру также происходит в два этапа. Прежде всего необходимо активизировать соответствующую возможность и только потом можно добавлять права на использование принтера.

Выберите **Пуск ▸ Панель управления ▸ Сеть и Интернет ▸ Центр управления сетями и общим доступом**.

Далее в появившемся окне (рис. 20.12) нажмите кнопку со стрелкой напротив надписи **Использование общих принтеров**. Затем установите переключатель в положение **Включить общий доступ к принтерам** и нажмите кнопку **Применить**. В результате система осуществит необходимые настройки и активизирует общий доступ к принтерам, о чем сообщит зеленый индикатор радом с надписью **Использование общих принтеров**.

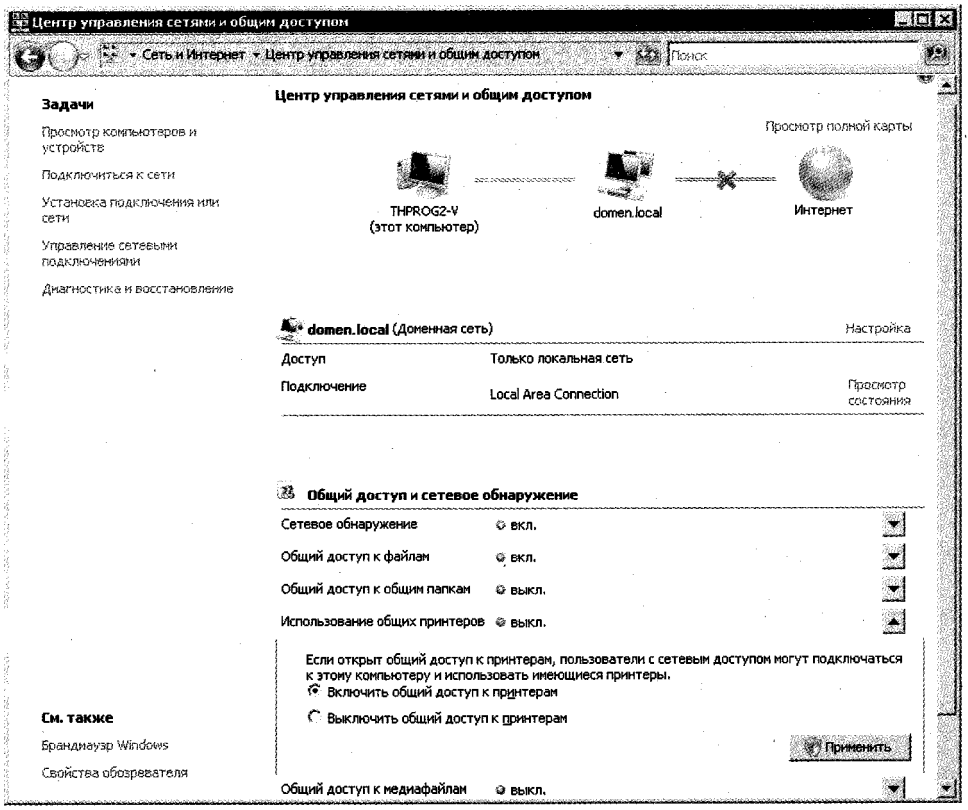


Рис. 20.12. Открываем доступ к принтеру

Следующий шаг — настройка прав доступа. Для этого откройте в **Проводнике** группу **Принтеры**, щелкните правой кнопкой мыши на названии нужного устройства и в появившемся меню выберите пункт **Общий доступ**.

Откроется окно с настройками принтера на вкладке **Доступ** (рис. 20.13). После активизации возможности использования общих принтеров содержимое этой вкладки блокируется и может быть изменено только после нажатия кнопки **Настройка общего доступа**.

После этого вы получаете возможность изменения сетевого имени принтера. Если вы перейдете на вкладку **Безопасность** (рис. 20.14), можно также добавлять или удалять машины, которые могут использовать принтер, а также настраивать их права.

Процесс добавления пользователей уже был описан ранее, поэтому можете обратиться за помощью к разделу 16.6 «Настройка общего доступа».

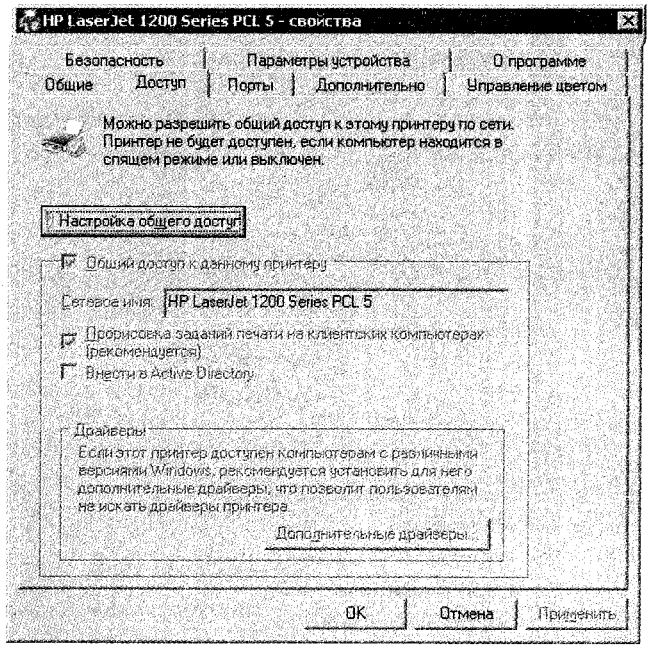


Рис. 20.13. Нажимаем кнопку Настройка общего доступа

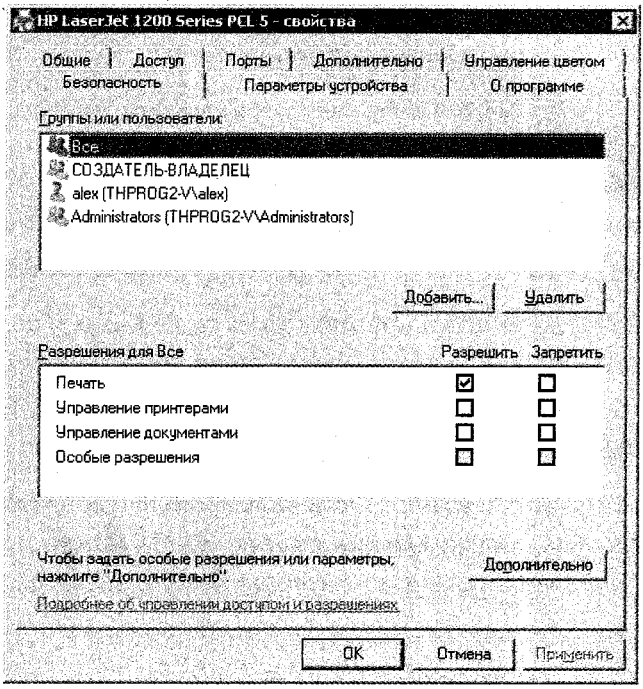


Рис. 20.14. Настраиваем права пользователей и групп

Подключение сетевой папки

ПРИМЕЧАНИЕ

Из видеоурока «Урок 20.4. Подключение к общим ресурсам в Microsoft Windows Vista», который находится на компакт-диске, прилагаемом к книге, вы узнаете, как подключиться к общим ресурсам.

Процесс подключения к общему файловому ресурсу очень прост и имеет несколько вариантов. Для этого, например, можно использовать **Проводник**.

Так, если вы хотите временно подключиться к сетевой папке, чтобы открыть файл или переписать фильм, для этого достаточно в левой части **Проводника** открыть группу **Сеть** и отметить нужный компьютер. Далее в правой части окна выберите нужный объект и просто перетяните его мышью, удерживая клавишу **Alt**.

Если вы планируете использовать этот файловый ресурс постоянно, проще подключить его как сетевой диск, чтобы каждый раз не искать компьютер и папку.

Для этого щелкните правой кнопкой мыши на нужной папке и в появившемся меню выберите пункт **Подключить сетевой диск**.

В результате появится окно, где необходимо указать букву диска, которая будет использоваться для подключения сетевого ресурса. Также для постоянного автоматического подключения диска при входе в систему установите флажок **Восстанавливать при входе в систему**.

Подключение сетевого принтера

Подключиться к сетевому принтеру, если у вас на то имеется право, очень легко. Убедит вас в этом видеоурок 20.4 «Подключение к общим ресурсам в Microsoft Windows Vista».

Подключение сетевого принтера осуществляется аналогично подобному процессу в Windows XP.

Для этого просто откройте нужный компьютер через **Проводник**, щелкните правой кнопкой мыши на принтере и в появившемся меню выберите команду **Подключить** или просто дважды щелкните кнопкой мыши на названии принтера.

Однако следует заметить, что доля компьютеров с установленной операционной системой Windows Vista пока еще слишком мала, поэтому может так случиться, что для подключения принтера вам придется где-то найти и вручную установить его драйверы.

Глава 21

Подключение сети к Интернету

- Некоторые сведения об Интернете
- Варианты доступа в Интернет
- Организация общего доступа в Интернет

Вряд ли можно представить современную жизнь без Интернета, который предоставляет пользователям неограниченные возможности и ресурсы. Только от вас самих зависит, как и для каких целей вы будете их использовать.

Интернет — это глобальная сеть, которая начиналась с объединения нескольких компьютеров, а закончилась миллионами и достигла вершины успеха развития, поэтому рассмотреть ее организацию и возможности — одна из обязательных задач данной книги.

21.1. Некоторые сведения об Интернете

Что же такое Интернет? Более двух десятков лет назад была начата работа над созданием экспериментальной сети ARPAnet. Идея принадлежала Министерству обороны США. Основная задача, которая ставилась перед разработчиками, — достижение устойчивости сети к любым повреждениям.

В то время велась холодная война между США и Советским Союзом, которая в любой момент могла перерасти в третью мировую войну. Учитывая, что авиационная бомбардировка может затронуть и уничтожить обширные промышленные (и не только) районы, разрабатываемая научными сотрудниками сеть должна была обеспечить беспрерывную работу. Предполагалось достичь этого путем сохранения работоспособности хотя бы одного из компьютеров, с которым можно было бы соединиться с помощью другого.

На соединяющиеся компьютеры (не только на саму сеть) также была возложена обязанность обеспечивать установку и поддержание связи. Принцип состоял в том, чтобы любой компьютер мог связаться с другим как равный с равным. Разработкой стандарта такой сети занялась Международная организация по стандартизации (ISO).

Идея сети была ясна, и за ее разработку принялись все, в том числе и многие из компьютерных любителей, что было возможно из-за длительных задержек в принятии стандарта. Постепенно программное обеспечение, которое обслуживало сеть, совершенствовалось и распространялось. Его стали применять многие пользователи. Со временем над сетью был взят контроль и все стало строго стандартизировано.

Чуть позже появилась World Wide Web (WWW) — Всемирная паутина, и все ринулись покорять просторы Интернета.

Бесчисленное множество разнообразных по характеру ресурсов превратило Интернет в небывалый по мощности информационный механизм. Перспективы его развития носят непредвиденный характер, что еще больше привлекает.

Интеграция Интернета в жизнь происходит быстрыми темпами и рано или поздно достигнет 100%-ной отметки.

Чтобы стать участником клуба любителей Интернета, нужно очень мало — желание и деньги. Глобальная сеть настолько отлаженный механизм, что работать в ней может даже неопытный пользователь. Почему бы не попробовать и вам, может, понравится?

21.2. Варианты доступа в Интернет

Чтобы использовать Интернет, нужно к нему подключиться, то есть получить доступ. Для этого вам придется заключить договор с одним из провайдеров (организацией, которая имеет прямой выход в Сеть).

Провайдеры бывают первичные и вторичные.

Первичными провайдерами являются крупные организации, имеющие высокоскоростной наземный или спутниковый канал в Интернете. Такой канал позволяет получать и передавать данные со скоростью, намного превышающей скорость обычного модема, например более 100 Мбит/с. Доступ к такому каналу могут позволить себе лишь крупные компании, имеющие один или несколько серверов, обслуживающих их веб-сайты и базы данных.

Вторичные провайдеры — как правило, небольшие организации, заключившие договор об аренде канала у первичного провайдера. Скорость такого канала зависит от уровня и качества оборудования, которым владеет вторичный провайдер. Обычно она не превышает 10 Мбит/с. Доступ к каналу вторичного провайдера в несколько раз дешевле, нежели доступ к каналу первичного. Связано это с тем, что скорость канала быстро расходуется из-за большого количества подключений и, как правило, пользователю достается канал со скоростью 1–2 Мбит/с.

На сегодняшний день наиболее популярны следующие варианты подключения к Интернету:

- с помощью аналогово-цифрового модема;
- xDSL-модема;

- через беспроводный модем;
- выделенную линию;
- frame relay;
- кабельное телевидение.

Поскольку рано или поздно локальную сеть, какого бы она масштаба ни была, придется подключить к Интернету, следует хотя бы коротко рассмотреть каждый из этих вариантов.

Подключение с помощью аналогово-цифрового модема

Итак, как и следует из названия, для подключения к Интернету (читай «интернет-провайдеру») используется обычный аналогово-цифровой модем, который появился уже добрый десяток лет назад. Более подробно о модемах можно прочесть в разделе 4.6 «Модем» главы 4, посвященной сетевому оборудованию.

Некогда этот способ подключения был наиболее выгодным и простым, поскольку для выхода в Интернет достаточно было приобрести устройство и настроить свойства соединения. Сегодня этот способ также часто встречается, однако уже начинает сдавать свои позиции. Почему? Читайте далее.

Для соединения с интернет-провайдером используется имеющийся в каждом доме телефонный кабель. Для того чтобы принять ваш сигнал, провайдер вынужден держать на своей стороне подобный модем, который рассчитан, грубо говоря, на соединение «точка-точка» (именно поэтому часто встречается название «сеансовый способ подключения» или dial-up-доступ). А это означает, что для одновременного обслуживания сотни пользователей провайдеру приходится иметь в распоряжении сотню линий и модемов (пул-модемов). Главный недостаток соединения через модем — низкая скорость, которая при сегодняшних способах оформления ресурсов в Интернете не обеспечивает хорошей скорости их отображения. Кроме того, можно даже не думать о том, чтобы смотреть живое видео, слушать интернет-радио, общаться через веб-камеру по интернет-пейджеру и т. д.

Как уже упоминалось ранее, теоретическая скорость работы такого подключения составляет не более 56 Кбит/с. Тем не менее такой способ часто используется, когда существующая аналоговая телефонная линия не приспособлена к более «продвинутым» технологиям передачи данных.

Что касается организации выхода в Интернет с помощью аналогово-цифрового модема, то такой способ может подойти лишь для локальной сети с 2–3 компьютерами, не более. В противном случае вы только получите порцию адреналина от негодования по поводу низкой скорости.

Подключение с помощью xDSL-модема

Как и в случае с аналогово-цифровыми модемами, для организации выхода в Интернет с помощью xDSL-модема используется обычная телефонная линия. Однако благодаря абсолютно другой технологии передачи сигнала скорость передачи данных намного выше получаемой с помощью обычного аналогово-цифрового модема. Так, чаще всего в домашних условиях достигается скорость от 64 до 512 Кбит/с. При этом имеется возможность регулирования скорости в достаточно широких пределах, причем в обе стороны, то есть на передачу и прием информации.

На сегодняшний день наибольшее распространение получили ADSL-модемы. Главное их преимущество — высокая скорость передачи данных и телефонная линия, свободная для использования. Так, максимальная скорость получения данных для модемов ADSL 2+ составляет 24 Мбит/с, чего, согласитесь, хватает для любых нужд. Даже если скорость составляет всего 1 Мбит/с, вы уже спокойно можете слушать радио, смотреть фильмы и обмениваться информацией с большой скоростью.

Для организации выхода в Интернет xDSL-модемы достаточно часто используются в локальных сетях уровня предприятия или большого офиса. Ничто не мешает устанавливать их и в домашних сетях, однако в этом случае более популярными являются выделенные линии.

Подключение через выделенную линию

Выделенная линия, какого бы типа она ни была (телефонный или оптоволоконный кабель), непосредственно подключает машины сети к оборудованию провайдера. Так вы можете быть уверены в том, что линия используется в полном объеме и только вами.

Что касается скорости передачи данных, то все зависит от вашего оборудования: используемое в качестве носителя оптоволокно обеспечит скорость 10–100 Мбит/с.

Минусом подключения по выделенной линии является ее дороговизна. Тем не менее этот способ очень часто используется в домашних сетях, поскольку позволяет получить гарантированный доступ в Интернет вне зависимости от многих условий.

Подключение через Frame Relay

Соединение компьютеров через Frame Relay (примерный перевод «переменная структура») используется уже давно. Главный смысл такого подключения — динамическое изменение скорости в зависимости от потребностей пользователей, то есть изначально определяется минимальная скорость передачи данных, которая потом автоматический изменяется в различных условиях. Максимальная скорость может достигать 2 Мбит/с, все зависит от качества линии.

Подобный способ подключения достаточно часто используется на предприятиях для организации связи с удаленными участками. Для выхода в Интернет Frame Relay подходит не всегда. Так, в случае с домашними сетями загруженность линии практически всегда будет составлять 100 %. Поэтому выгоднее организовать выделенную линию с определенной скоростью передачи данных: пусть дороже, но качественнее.

Подключение через беспроводной модем

В последнее время все чаще для передачи данных используется радиоэфир. Преимущества очевидны: высокая скорость и, самое главное, мобильность.

Для того чтобы получить выход в Интернет, вам достаточно установить направленную антенну и радиомодем, подключив его к маршрутизатору. Скорость передачи/получения данных может достигать 2 Мбит/с. Недостаток в том, что скорость колеблется, поскольку напрямую зависит от расстояния до провайдера и погодных условий.

Не забывайте также о спутниковом Интернете, поскольку он тоже подразумевает использование радиоэфира, только на более высоких частотах. Подключение к Интернету через спутник имеет свои особенности, что не позволяет ему получить большую популярность. Первый, и самый главный недостаток — дороговизна подключения. Ведь для того, чтобы использовать такой Интернет, вам понадобится приобрести дорогостоящую спутниковую антенну и специальный модем.

Различают симметричный и асимметричный спутниковый Интернет.

Первый подразумевает использование более дешевого оборудования, однако требует еще и дополнительного наземного подключения к Интернету. Это связано с тем, что простая спутниковая антенна позволяет лишь получать данные, а для передачи необходим другой вид связи.

Подобного недостатка лишен асимметричный Интернет, однако стоимость спутникового оборудования в этом случае превышает все разумные пределы. Тем не менее использование асимметричного Интернета — единственный вариант подключения к Сети удаленных и отрезанных от цивилизации поселков.

Еще один недостаток спутникового Интернета — слишком большое время отклика. Это означает, что, даже имея подключение со скоростью, например, 2 Мбит/с, вы получаете информацию с задержкой.

Еще один вариант беспроводного подключения — использование существующих GSM-сетей, обслуживающих мобильные телефоны. В этом случае вы просто подключаете аппарат любым доступным способом к компьютеру (кабель, инфракрасный порт, Bluetooth), настраиваете соединение и используете его модем для выхода в Интернет. Что касается скорости передачи данных, то она не выдерживает никакой критики, поэтому подобное подключение к Интернету используется редко.

Использовать беспроводные технологии для подключения локальной сети к Интернету следует обдуманно и только в том случае, если другие варианты вас не устраивают.

Подключение через кабельное телевидение

Еще один бурно развивающийся способ подключения к Интернету — использование существующих телевизионных кабельных систем. Телевизор — устройство, которое есть в любом доме, и очень часто для просмотра программ используется кабельное вещание. Преимущества такого телевидения очевидны: большое количество каналов на любой вкус и на любого зрителя.

Использование существующего телевизионного кабеля для подключения к Интернету достаточно эффективно, поскольку не требует организации отдельных проводных линий. Скорость передачи данных может достигать 30 Мбит/с. Тем не менее использование кабельного подключения оправдано лишь в домашних

условиях, а для организации выхода в Интернет локальной сети даже небольшого размера подобный способ абсолютно нецелесообразен.

21.3. Организация общего доступа в Интернет

Если есть локальная сеть, рано или поздно появится необходимость подключения ее к Интернету. Для этого существуют несколько отработанных механизмов.

Общая идея проста — достаточно организовать подключение к Интернету одного из компьютеров сети и научить его «делиться» им с остальными. Использовать компьютер для этих целей очень удобно, поскольку можно настраивать разрешения визуально.

Можно также использовать и маршрутизатор, что более выгодно, поскольку исключает лишнее звено.

Реализацию этой идеи усложняет только то, что нужно организовывать контроль над использованием Интернета другими компьютерами и следить за безопасностью их подключения.

Для офисной сети, состоящей более чем из 20 компьютеров, обычно настраивают отдельную машину — интернет-шлюз, на который устанавливают необходимое программное обеспечение и который предназначен только для обслуживания подключенных к нему пользователей.

Если выделить отдельный компьютер нельзя, можно задействовать одну из рабочих машин. В этом случае к ней предъявляются дополнительные требования — как минимум она должна быть постоянно включена и работать без сбоев.

Ниже рассматривается вариант настройки общего Интернета на компьютере под управлением операционной системы Windows XP.

Использование стандартных компонентов Windows XP

Для организации общего доступа в Интернет в Windows XP Professional предназначена специальная служба ICS (Internet Connection Sharing).

Чтобы осуществить задуманное, главный компьютер уже должен иметь настроенное подключение к Интернету любого типа, через которое будет организован общий доступ в Глобальную сеть.

Итак, начнем. Выберем самый простой путь — мастер настройки сети. Чтобы его запустить, выполните команду **Пуск ▸ Настройка ▸ Сетевые подключения**. Затем в появившемся окне дважды щелкните кнопкой мыши на значке **Мастер настройки сети**.

В результате появится окно, сообщающее, для чего служит мастер настройки сети. В нем также говорится, что программу можно использовать для организации общего подключения к Интернету.

После нажатия кнопки **Далее** вы попадете в следующее окно, в котором даются советы по предварительной подготовке к выбранным действиям. В частности, предлагается проверить, установлены ли сетевая плата и модем и работают ли они. Кроме того, рекомендуется подключиться к Интернету, что совсем не обязательно, поскольку это можно сделать и позже, проверяя результат предоставления общего доступа.

После нажатия кнопки **Далее** мастер произведет проверку существующих сетевых подключений. Все обнаруженные подключения отобразятся в окне, показанном на рис. 21.1. В данном примере имеется одно проводное сетевое подключение, которое временно не работает, поскольку сетевая карта не подключена к сети. Это сделано с целью проверки мастера. Как видите, он обнаружил подключение и попросил проверить его или присоединить шнур. Это можно будет сделать позже, после создания общего доступа, поэтому установим флажок **Игнорировать отключенное сетевое оборудование**.

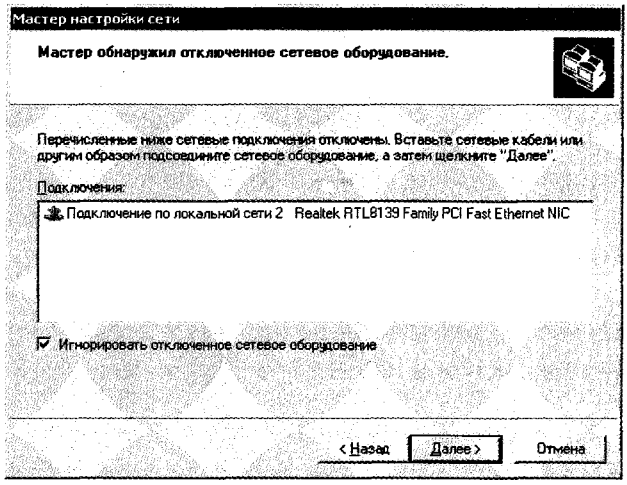


Рис. 21.1. Обнаружено сетевое подключение

Если бы в списке присутствовало больше одного подключения, мастер предложил бы вам выбрать одно из них, то, которое будет отвечать за соединение компьютера с локальной сетью.

В следующем окне мастер предложит выбрать метод подключения. Существует несколько возможных вариантов. Если необходимо сделать данный компьютер главным, то есть другие пользователи будут выходить в Интернет через него, то следует выбрать первый вариант.

Если в сети уже существует компьютер с выходом в Интернет и на нем уже настроен общий доступ, выбирайте второй вариант.

Третий вариант — это более сложный путь, поэтому в данной книге он рассматриваться не будет.

Предположим, вы выбрали первый вариант. В таком случае в следующем окне вам предложат указать подключение, которое отвечает за связь с Интернетом (рис. 21.2).

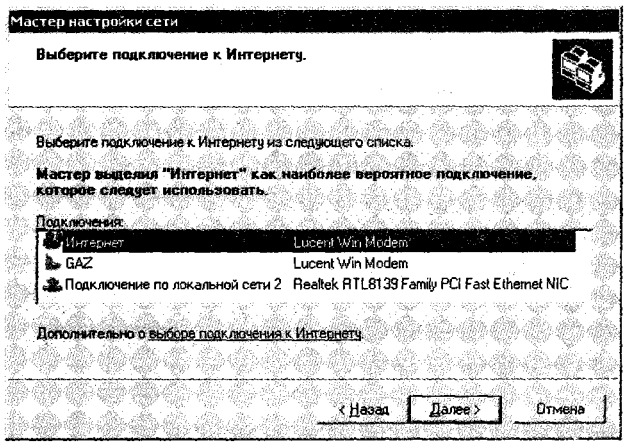


Рис. 21.2. Выбираем подключение

Выбрав соединение и нажав кнопку **Далее**, вы попадете в следующее окно, в котором нужно внести некоторые сведения о компьютере. Если нужно что-то исправить в предыдущем окне, воспользуйтесь кнопкой **Назад**.

В очередном окне вас попросят дать название группы. Чтобы компьютеры могли пользоваться доступом в Интернет, они должны принадлежать той группе, что и компьютер с настроенным общим доступом.

После нажатия кнопки **Далее** вы увидите окно с итоговой информацией о введенных вами данных. Если вы с ней не согласны, можно вернуться и изменить настройки, нажимая кнопку **Назад**.

Если все в порядке, нажмите кнопку **Далее**. После этого мастер попытается произвести все выбранные изменения и настройки системы. Данный процесс может занять некоторое время, поэтому будьте терпеливы.

После завершения настройки появится окно, в котором нужно установить переключатель в положение **Просто завершить работу мастера, нет нужды запускать его на других компьютерах**. Для настройки остальных компьютеров, то есть включения их в созданную группу, также используют мастер настройки сети.

После нажатия кнопки **Далее** появится окно, сообщающее об окончании настройки сети. После этого перезагрузите компьютер для сохранения изменений и обновления конфигурации системы.

Теперь, чтобы остальные компьютеры могли подключаться к Интернету, им необходимо будет немного настроить IP-протокол. Так, нужно будет прописать IP-адрес шлюза, в нашем случае это 192.168.0.1. Более детально о настройке протокола можно прочитать в главе 19.

Использование программы Kerio WinRoute

Использование вспомогательных программ для предоставления общего доступа в Интернет является оправданным шагом. Основное его достоинство — управляемость и контроль. Кроме того, эти программы содержат в себе все необходимые механизмы для обеспечения функционирования общего доступа в Интернет. Kerio WinRoute — одна из таких программ.

Прежде чем установить данную программу, вспомните, что для разделения трафика локальной сети и Интернета требуется настроенное соединение с ним. Как правило, это касается и офисных, и домашних сетей, для создания такого подключения используется дополнительная сетевая карта. Хотя вполне возможно, что будет использоваться и любого типа модем. При установке программы вам необходимо будет указать то устройство, которое используется для выхода в Интернет. В противном случае подсчет трафика будет вестись неверно.

Программа Kerio WinRoute небольшая по размеру, но тем не менее сочетает в себе мощные механизмы обеспечения общего доступа в Интернет и макси-

мального контроля. Использование всего одного IP-адреса (механизм NAT) для выхода в Интернет делает остальных клиентов максимально защищенными. Кроме того, имеется механизм, с помощью которого можно настраивать правила разного характера.

После запуска программы нужно произвести минимальные настройки, чтобы механизм начал работать. Дело в том, что WinRoute изначально настроена, а требуемые изменения касаются лишь указания нужного сетевого соединения, списка дозволенных протоколов и списка пользователей с паролями.

Со временем с появлением новых подключений и новых нюансов, возможно, придется произвести настройку встроенных механизмов DHCP и DNS, хотя это и не обязательно.

Количество параметров программы просто поражает. Вы можете настраивать разнообразнейшие фильтры, блокировать или разрешать выполнение программных модулей, ограничивать скорость, настраивать таблицы маршрутизации, правила использования трафика и многое другое. Все параметры поделены на группы, переход между которыми осуществляется с помощью древовидной структуры в левой части окна (рис. 21.3).

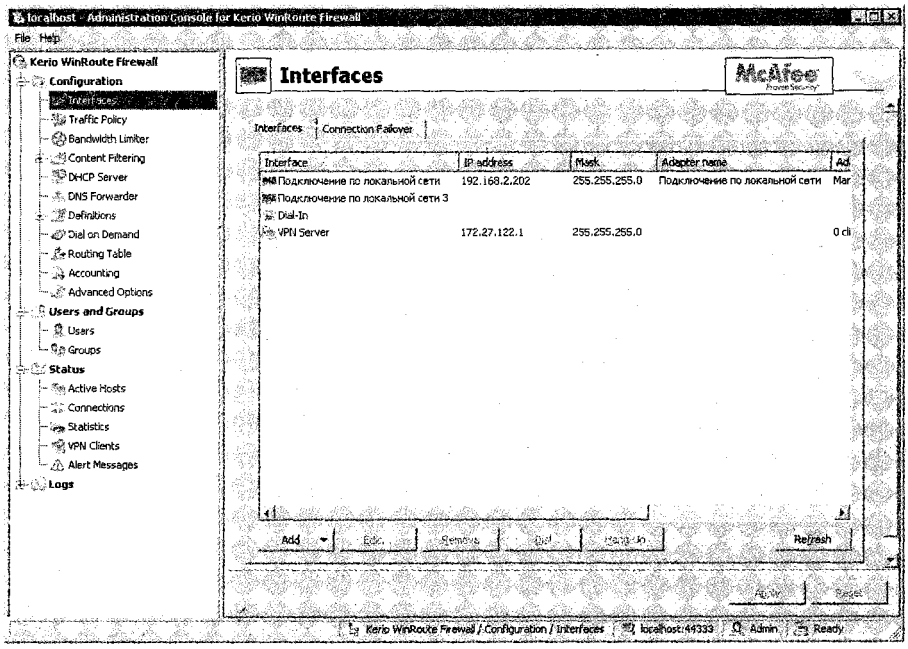


Рис. 21.3. Интерфейс программы Kerio WinRoute

Преимуществом WinRoute перед другими аналогичными программами является наличие встроенного брандмауэра и антивирусной защиты от McAfee. Также имеется подробнейшая статистика использования трафика, как доступная в самом интерфейсе программы (ветка **Status**), так и вызываемая с помощью браузера.

Настройка клиентских компьютеров заключается в том, чтобы прописать адрес прокси-сервера в настройках IP-протокола (в поле **Основной шлюз**).

Если вы хотите производить легкую тарификацию пользователей, обязательно добавьте всех их и пропишите им статичный IP-адрес. В этом случае никакой авторизации пользователей не потребуется. Если в сети настроен DHCP-сервер и адреса выдаются динамически, авторизация пользователя будет происходить каждый раз, когда он пытается загрузить любую веб-страницу.

Глава 22

Защита сети

- Отключение трансляции SSID
- Фильтрация MAC-адресов
- Настройка шифрования
- Снижение мощности передатчика

Защита данных, используемых и передаваемых по сети, всегда волнует и будет волновать тех, кто эту сеть создает или администрирует. В любом случае, какова бы ценность этих данных ни была, безопасность должна стоять на первом месте.

Поскольку специфика проводных и беспроводных сетей разная, организация защиты от несанкционированного доступа к ним также различается. Что касается проводного варианта, то здесь все проще, поскольку упирается в необходимый набор программного обеспечения — антивирусный пакет, сетевой экран и т. д. В беспроводной сети, кроме необходимого программного обеспечения, приходится настраивать оборудование, о чем и хотелось бы рассказать в этом разделе.

По умолчанию беспроводное оборудование не использует каких-либо механизмов защиты и является абсолютно открытым для атак извне. Поэтому после создания сети первым делом необходимо выполнить определенные действия, которые позволят максимально защитить вашу сеть.

Ниже рассмотрен пример настройки необходимого уровня безопасности точки доступа D-Link DWL-2100AP.

22.1. Отключение трансляции SSID

SSID является уникальным идентификатором, описывающим сеть. Фактически это имя сети, которое должны знать все, кто собирается к ней подключиться. Поэтому, прежде чем отключить транслирование идентификатора сети, обязательно сообщите его всем пользователям.

По умолчанию идентификатор сети сообщается точкой доступа всем беспроводным устройствам, лежащим в радиусе ее действия. Просканировав эфир и увидев точку доступа и ее SSID, беспроводной клиент может присоединиться к ней, если введет все правильные настройки подключения. Соответственно, не зная SSID точки доступа, подключиться к ней будет сложно, но возможно, если использовать специализированное программное обеспечение.

Данный способ защиты сети нельзя считать полноценным, но отсеять некоторую часть начинающих любителей бесплатного сыра вполне реально. Поэтому обязательно активизируйте эту возможность.

Практически все точки доступа позволяют отключить вещание SSID в сеть. Для этого необходимо зайти в настройки устройства и изменить один из параметров.

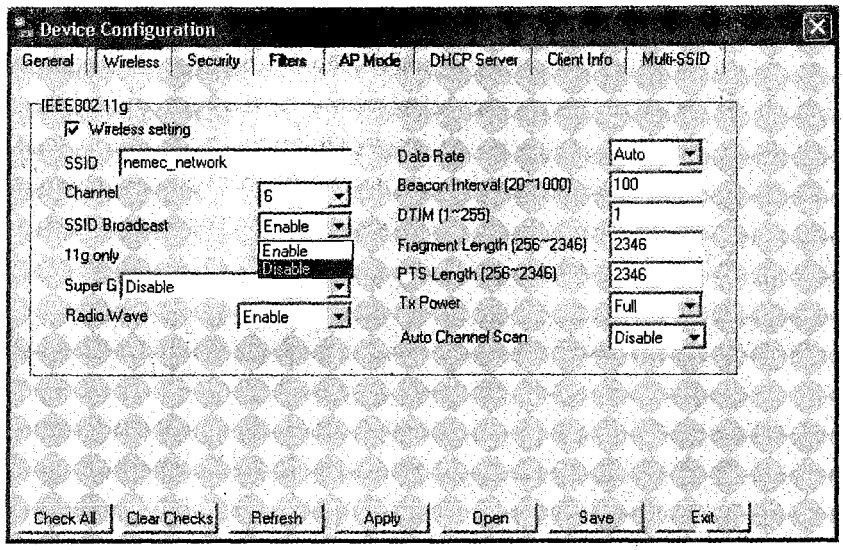


Рис. 22.1. Настраиваем параметр SSID Broadcast (Транслирование SSID)

Запустив утилиту конфигурирования точки доступа D-Link DWL-2100AP, выбираем вкладку **Wireless** (Беспроводная сеть) (рис. 22.1). На ней находится раскрывающийся список **SSID Broadcast** (Транслирование SSID), из которого можно выбрать значения **Enable** (Разрешить) и **Disable** (Запретить). Соответственно, чтобы запретить транслирование идентификатора сети, необходимо установить значение **Disable** (Запретить).

22.2. Фильтрация MAC-адресов

Практически любая точка доступа позволяет создавать исключения, содержащие списки MAC-адресов беспроводных устройств, которым разрешено подключаться к ней.

Поскольку MAC-адрес — уникальный идентификатор сетевого устройства, то можно легко создать список таких MAC-адресов, которые однозначно идентифицируют подключаемое оборудование. Это обеспечивает дополнительный уровень защиты сети от атак. Но опять же такая защита может остановить только неопытных вредителей, не имеющих на вооружении нужных программных средств. С помощью специальных утилит можно достаточно легко подменить свой MAC-адрес на один из перехваченных, проникнуть в точку доступа и непосредственно в сеть.

Чтобы создать такой список адресов, запустите утилиту конфигурирования точки доступа. Затем перейдите на вкладку **Filters** (Фильтры). Далее в области **IEEE802.11f Access Setting** (Настройка доступа для устройств IEEE802.11g) необходимо установить флажок **Access Control** (Контроль доступа), как показано на рис. 22.2. Из раскрывающегося списка рядом выберите значение **Accept** (Принимать), это говорит точке доступа, что устройства с указанными MAC-адресами могут к ней подключаться.

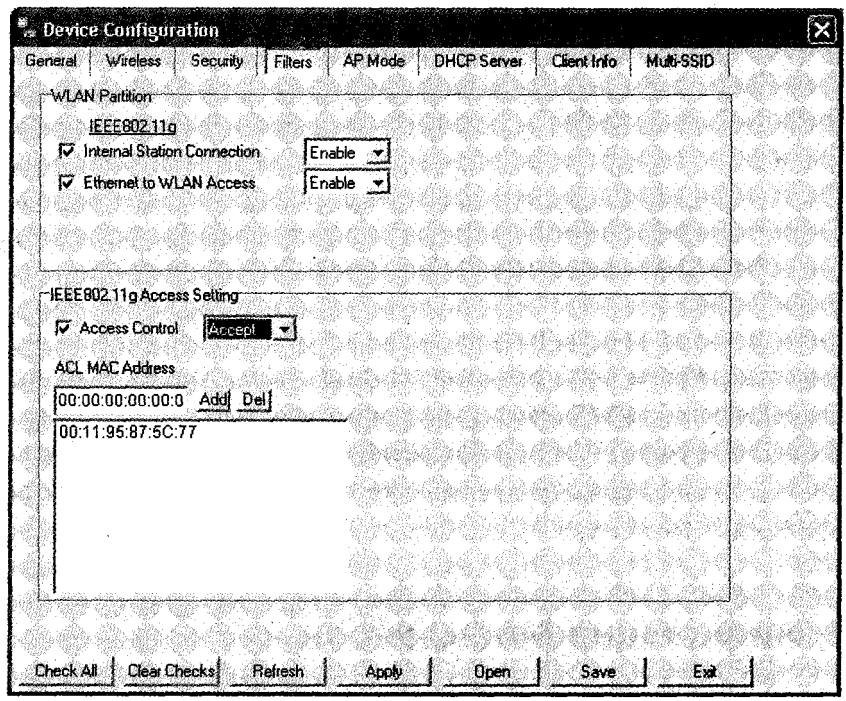


Рис. 22.2. Создаем список MAC-адресов

Чтобы ввести MAC-адрес, перейдите в поле ввода **ACL MAC Address**, введите адрес, придерживаясь указанного шаблона, и нажмите кнопку **Add**. Вводите данные очень внимательно, ошибка может привести к тому, что законный компьютер не сможет подключиться к точке доступа.

22.3. Настройка шифрования

Шифрование — один из главных способов обеспечения сохранности данных при передаче их через радиоэфир.

Современное беспроводное оборудование позволяет использовать для шифрования протоколы WEP, WPA и WPA2. Что касается первого из них, то его поддерживает все существующее оборудование, каким бы древним оно ни было. Иногда именно этот факт, то есть устаревшее оборудование, становится причиной использования данного протокола, который можно охарактеризовать как самый простой и неэффективный способ шифрования данных. Поскольку для этого используется статичный ключ, для множества специализированных программ не составляет особого труда проанализировать передаваемые данные и определить его. Конечно, ключ может быть разной длины, вплоть до 256 бит, однако это влияет лишь на время взлома.

Что касается протоколов WPA или WPA2 (более новая спецификация), то этот способ шифрования на сегодняшний день наиболее предпочтителен, поскольку позволяет оперировать динамичными ключами, которые могут меняться каждые 10 тысяч пакетов, что фактически исключает даже возможность взлома.

Как бы там ни было, протокол шифрования обязательно должен быть задействован при работе точки доступа, независимо от того, в каком режиме она функционирует.

Для настройки протокола безопасности воспользуемся утилитой конфигурирования, которая идет в комплекте с точкой доступа. После ее запуска перейдите на вкладку **Security** (Безопасность) (рис. 22.3).

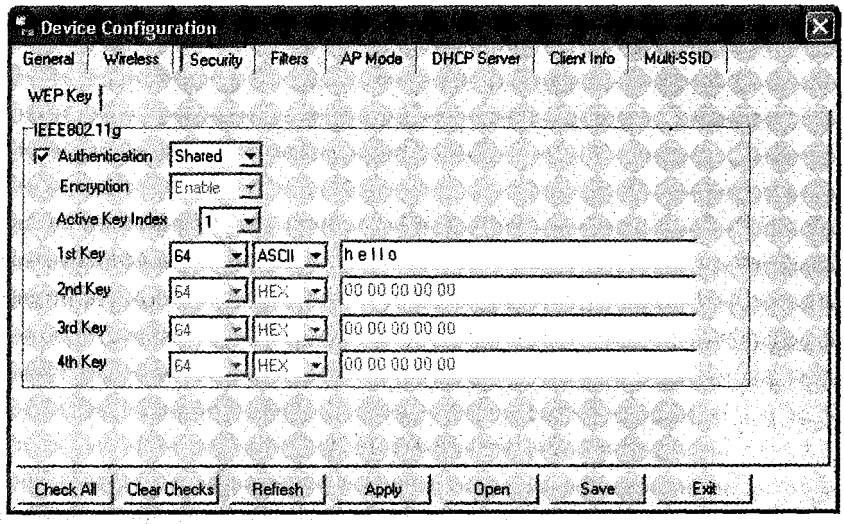


Рис. 22.3. Настраиваем протокол безопасности WEP

Здесь можно указать необходимый протокол шифрования и настроить параметры шифрования и подключения к точке доступа.

Если вы планируете использовать протокол WEP, что может быть обусловлено использованием устаревших беспроводных адаптеров, неспособных работать с более «продвинутым» протоколом, то установите флажок **Authentication** (Аутентификация) и выберите из раскрывающегося списка одно из значений: **Open** (Открытый), **Shared** (Разделенный) или **Both** (Оба режима). Кроме этого, установите флажок **Encryption** (Шифрование) и выберите из раскрывающегося списка значение **Enable** (Разрешить). Именно эти параметры отвечают за настройку протокола WEP.

После выбора одного из упомянутых значений необходимо настроить ключ шифрования, указав его длину, тип и саму символьную строку ключа. В своей работе точка доступа может использовать четыре разных ключа шифрования. При этом одновременно может применяться только один ключ (текущий).

Чтобы выбрать нужный ключ, достаточно в поле **Active Key Index** (Индекс активного ключа) установить номер ключа и настроить его, если это не было сделано раньше. При вводе символьной строки ключа, если его тип установлен в ASCII, старайтесь подбирать редко используемые словосочетания. При этом не забывайте, что ключ имеет фиксированное количество символов, например 5 или 13, что зависит от выбранной длины ключа.

Если оборудование, используемое для работы в сети, современное и поддерживает последние протоколы шифрования, обязательно воспользуйтесь этим и настройте параметры протокола WPA. Для этого установите флажок **Authentication** (Аутентификация) и выберите из раскрывающегося списка параметр **WPA-EAP** или **WPA-PSK**. В результате появится дополнительная вкладка **IEEE802.11g WPA** с некоторыми настройками протокола.

Если в вашей беспроводной сети установлен сервер аутентификации RADIUS, то следует выбрать значение **WPA-EAP**, поскольку лучшей защиты сети пока ничто обеспечить не может. Далее не забудьте указать IP-адрес и порт RADIUS-сервера. Кроме всего прочего, вам нужно определиться с типом шифра — TKIP (Temporal Key Integrity Protocol) или AES (Encryption Standard).

Первый обеспечивает динамическую генерацию ключа и проверку целостности пакетов с возможностью их шифрования с помощью разных ключей, что на

порядок выше возможностей протокола WEP. Второй же является представителем последнего достижения шифрования и обладает самым мощным алгоритмом, поддерживающим ключ длиной 256 бит[1].

Если у вас вызывает сомнения, какой из типов шифра выбрать, то предоставьте это самой точке доступа и установите в поле **Cipher Type** (Тип шифра) значение **Auto** (Автоматический выбор).

Если в вашей беспроводной сети не планируется применение RADIUS-сервера, но вам все-таки хочется воспользоваться возможностями протокола WPA, тогда в качестве параметра **Authentication** (Аутентификация) выбирайте значение **WPA-PSK**. При этом вам также необходимо будет определиться с типом шифра и указать фразу шифрования.

22.4. Снижение мощности передатчика

Как известно, для передачи данных в радиоэфир каждое беспроводное устройство снабжено приемником и передатчиком радиоволн. От его мощности зависит радиус действия беспроводной сети, а от чувствительности — качество приема сигнала. Радиоволны — инстанция неконтролируемая, и никогда нельзя предугадать, кто может их принимать, поэтому неплохим вариантом защиты сети является подбор такой мощности передатчика, которой вполне достаточно для покрытия всех устройств сети. Этим вы отсекаете всех недоброжелателей, которые могут пристроиться к вашей сети, например, из соседнего дома или в машине на стоянке рядом с офисом.

Другой плюс такого предприятия — экономия энергии, что критично для переносных компьютеров и устройств.

Для того чтобы выбрать уровень мощности сигнала, запустите утилиту конфигурирования точки доступа и перейдите на вкладку **Wireless** (Беспроводная сеть). На ней вы увидите параметр **Tx Power** (Мощность сигнала), который может принимать несколько значений: **Full** (Полная мощность), **Half** (Половина мощности), **Quarter** (Четверть мощности), **Eighth** (Восьмая часть мощности) и **Min** (Минимальная мощность) (рис. 22.4).

---

[1] Этот тип шифрования относится к спецификации протокола WPA2.

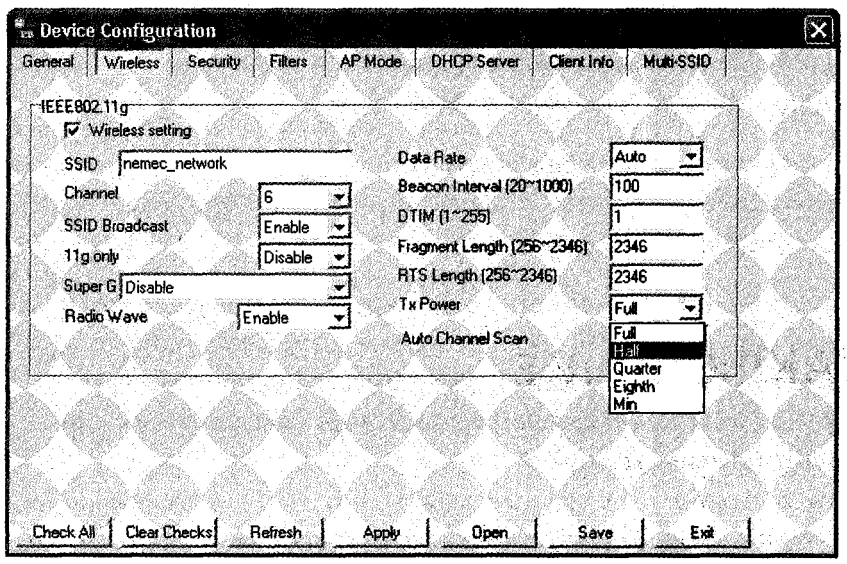


Рис. 22.4. Регулируем мощность передатчика

Не нужно сразу устанавливать слишком низкую мощность, поскольку этим можно «обрубить» связь с некоторыми удаленными компьютерами. Уменьшайте мощность постепенно, но не устанавливайте ту, на которой наблюдается пороговая работа устройства, поскольку в определенных условиях сигнал может еще более ослабнуть, что опять же приведет к отключению удаленных компьютеров.

Заключение

Доказать очевидное — вечная задача всех учителей и любой технической литературы. Подобная задача была возложена и на эту книгу. Справилась ли она с ней — судить вам, но для достижения этой цели были приложены все силы. Как бы там ни было, надеюсь, что книга не только принесла вам теоретические знания, но и побудила к определенным практическим действиям. Удачи вам в ваших начинаниях и не бойтесь делать практические шаги! Ведь нет ничего более ценного, чем опыт!

Приложение

Содержимое компакт-диска, который прилагается к книге

На прилагаемом к книге компакт-диске вы найдете шестую часть книги, в которую вошло краткое описание программ:

- для контроля сетевого трафика (DU Meter, TMeter, NetLimiter, NetStat Live, Bandwidth Monitor Pro, CommView, NetPeeker);
- антивирусной защиты (Symantec AntiVirus, Dr.Web, Panda Antivirus Platinum, «Антивирус Касперского», NOD32);
- работы в Интернете:
  - браузеров (Microsoft Internet Explorer, Opera, MyIE2, Mozilla Firefox);
  - почтовых клиентов (The Bat!, Outlook Express, Mozilla Thunderbird);
  - программ для борьбы со спамом (Anti Spammer, SpamPal, Agava Spamprotexx, Anti-Spam Filter);
  - менеджеров закачки файлов (ReGet Deluxe, FlashGet, Download Master, Teleport Pro);
  - интернет-пейджеров (ICQ, QIP, Trillian);
  - программ борьбы со SpyWare (Ad-Aware SE, Arovax Shield).

На компакт-диске вы также найдете многие из описанных программ, а главное — 22 видеоурока, в которых демонстрируется большинство из рассмотренных в книге действий. Видеоролики распределены по группам в соответствии с номером главы, в которой они описываются. Перед просмотром видеоурока рекомендуется изучить материал посвященного ему раздела книги, чтобы закрепить полученные знания и лучше понять каждый шаг к конечному результату.

Глава 7.

- **Урок 7.1. Обжим коаксиального кабеля.** Из данного видеоурока вы узнаете, как происходит подготовка кабеля и обжим коннекторов.
- **Урок 7.2. Подключение коаксиального кабеля к компьютеру.** В этом видеоуроке показано, как подключить готовый кабель к компьютеру.

Глава 8.

- **Урок 8.1. Обжим кабеля на основе витой пары.** В данном видеоуроке продемонстрировано, как обжимать кабель на основе витой пары.
- **Урок 8.2. Подключение кабеля на основе витой пары к компьютеру.** В этом видеоуроке показано, как подключить готовый кабель к компьютеру.

Глава 16.

- **Урок 16.1. Настройка DHCP-сервера.** Из данного видеоурока вы узнаете, как настроить DHCP-сервер в Windows 2003 Server.
- **Урок 16.2. Настройка Active Directory.** Данный видеоурок демонстрирует практический пример использования системной компоненты Active Directory в Windows 2003 Server. Вы научитесь создавать группы, подразделения и учетные записи пользователей.
- **Урок 16.3. Настройка общего доступа в Windows 2003 Server.** В этом видеоуроке продемонстрирована настройка общего доступа к файловым ресурсам и принтеру в Windows 2003 Server.

Глава 17.

- **Урок 17.1. Подключение кабеля на основе витой пары к коммутатору.** Из данного видеоурока вы узнаете, как подключить к коммутатору кабели, подготовленные и уже подсоединенные к сетевым компьютерам.
- **Урок 17.2. Установка сетевой карты в компьютер.** В этом видеоуроке показана установка сетевой карты в корпус компьютера.

Глава 19.

- **Урок 19.1. Подключение к домену в Microsoft Windows XP.** Данный видеоурок демонстрирует подключение к домену сети в Microsoft Windows XP.
- **Урок 19.2. Настройка общего доступа к файловым ресурсам в Microsoft Windows XP.** В этом видеоуроке показано, как настроить общий доступ к файловым ресурсам в Microsoft Windows XP.
- **Урок 19.3. Настройка общего доступа к принтеру в Microsoft Windows XP.** Из данного видеоурока вы узнаете, как настроить общий доступ к принтеру в Microsoft Windows XP.
- **Урок 19.4. Подключение к общим ресурсам в Microsoft Windows XP.** В этом видеоуроке показано, как подключиться к файловому ресурсу и общему принтеру в Microsoft Windows XP.

Глава 20.

- **Урок 20.1. Подключение к сети в Microsoft Windows Vista.** Данный видеоурок демонстрирует подключение к сети в Microsoft Windows Vista.

- **Урок 20.2. Настройка общего доступа к файловым ресурсам в Microsoft Windows Vista.** Из этого видеоурока вы узнаете, как настроить общий доступ к файловым ресурсам в Microsoft Windows Vista.
- **Урок 20.3. Настройка общего доступа к принтеру в Microsoft Windows Vista.** Из данного видеоурока вы узнаете, как настроить общий доступ к принтеру в Microsoft Windows Vista.
- **Урок 20.4. Подключение к общим ресурсам в Microsoft Windows Vista.** Этот видеоурок демонстрирует подключение к файловому ресурсу и общему принтеру в Microsoft Windows Vista.

Глава 24 (находится на прилагаемом компакт-диске).

- **Урок 24.1. Symantec AntiVirus Corporate Edition.** Данный видеоурок познакомит вас с возможностями антивирусного пакета Symantec AntiVirus Corporate Edition, который позволяет осуществлять постоянную защиту системы с возможностью ее ручной проверки и настройки планового сканирования.
- **Урок 24.2. Dr.Web.** Этот видеоурок демонстрирует работу антивирусного пакета Dr.Web (сканера, с помощью которого можно вручную проверять файловую систему на наличие вредоносных вирусов; модуля SpiDer Mail, следящего за входящей и исходящей корреспонденцией; модуля SpiDer Guard, постоянно защищающего операционную систему от вирусов, троянов, программ-шпионов и др.).
- **Урок 24.3. Panda Antivirus Platinum.** Данный видеоурок демонстрирует работу антивирусной программы Panda Antivirus Platinum, вы познакомитесь с ее основными настройками для защиты компьютера.
- **Урок 24.4. NOD32.** Этот видеоурок демонстрирует работу программы NOD32, которая защищает компьютер от вирусных атак.

Глава 25 (находится на прилагаемом компакт-диске).

- **Урок 25.1. Ad-Aware SE.** Из данного видеоурока вы узнаете о принципах работы программы Ad-Aware SE, которая «вылавливает» вредоносные объекты, типа шпионских программ и троянов.

Ватаманюк Александр Иванович

Видеосамоучитель. Создание и обслуживание локальных сетей (+CD)

Заведующий редакцией	*Д. Гурский*
Ведущий редактор	*Е. Крикунова*
Литературный редактор	*С. Дрозд*
Художник	*Б. Клюйко*
Корректоры	*Т. Курьянович, Е. Павлович*
Верстка	*О. Махлина*

Подписано в печать 11.09.07. Формат 70×100/16. Усл. п. л. 24,51.
Тираж 3000. Заказ 5194

ООО «Питер Пресс», 198206, Санкт-Петербург, Петергофское шоссе, 73, лит. А29.

Налоговая льгота — общероссийский классификатор продукции ОК 005-93, том 2; 95 3005 — литература учебная.

Отпечатано по технологии CtP
в ОАО «Печатный двор» им. А. М. Горького.
197110, Санкт-Петербург, Чкаловский пр., 15.