Ю.А. Родичев

КОМПЬЮТЕРНЫЕ СЕТИ: АРХИТЕКТУРА, ТЕХНОЛОГИИ, ЗАЩИТА

Учебное пособие для вузов

Рекомендовано Учебно-методическим объединением по образованию в области информационной безопасности в качестве учебного пособия для студентов высших учебных заведений, обучающихся по специальностям 090103 – «Организация и технология защиты информации» и 090105 – «Комплексное обеспечение информационной безопасности автоматизированных систем».

Издательство «Универс-групп»
Самара 2006

УДК 681.324
ББК 32.988.02я7
Р 60

Рецензенты:

Симановский Е.А., кандидат технических наук, доцент кафедры компьютерных систем Самарского государственного аэрокосмического университета

Морозов В.К., кандидат технических наук, доцент кафедры информационных технологий Самарского технического университета

Черемушкин А.В., кандидат физико-математических наук, доцент

Родичев, Ю.А.

Р 60 Компьютерные сети: архитектура, технологии, защита : учеб. пособие для вузов. – Самара : изд-во «Универс-групп», 2006. – 468 с.

ISBN 5–467–00067–5

В книге изложены основные принципы построения компьютерных сетей, описаны распространенные технологии локальных и глобальных сетей. Рассмотрены вопросы информатизации мирового сообщества и роли компьютерных сетей в этом процессе, фундаментальные математические основы (теория графов), необходимые для построения сетей.

Отдельная глава посвящена вопросам обеспечения безопасности корпоративных сетей и информационных систем, описана специфика защиты IP-сетей, рассмотрены способы защиты.

Рекомендовано Учебно-методическим объединением по образованию в области информационной безопасности в качестве учебного пособия для студентов высших учебных заведений, обучающихся по специальностям 090103 – «Организация и технология защиты информации» и 090105 – «Комплексное обеспечение информационной безопасности автоматизированных систем».

УДК 681.324
ББК 32.988.02я7

ISBN 5–467–00067–5

© Родичев Ю.А.
© «Универс-груп»

Содержание

Образование есть то, что остается после того, когда забывается все, чему нас учили.
Альберт Энштейн

Предисловие

Мировое сообщество в своем развитии вступило в новую фазу своего развития – стадию информационного общества. Характерным признаком такого общества является то, что информационные технологии и телекоммуникации становятся базовыми в экономике и уровень их внедрения в значительной степени определяет уровень развития страны в целом. Информация, а также средства ее хранения, передачи и доступа к ней являются важнейшими стратегическими ресурсами. Если несколько лет назадXVII сам термин «информационное общество» фигурировал только в кругах профессионалов, то теперь им оперируют и политики, и студенты, и даже школьники.

Необходимо отметить, что в России этот термин не постигла участь зародившегося много лет назад нового научного направления «кибернетика». Более того, Россия активно включилась в построение информационного общества. Принят ряд законов и нормативных актов, а также Федеральных целевых программ, оперирующих этим понятием и ставящих конкретные задачи на пути построения информационного общества. Более того, Россия стала участником ряда международных соглашений в области информатизации. Среди них следует отметить «Окинавскую хартию глобального информационного общества», принятую в 2000 году странами «большой восьмерки» и подписанную президентом России.

Ключевыми звеньями в построении информационного общества являются информация, компьютеры и телекоммуникации, обеспечивающие процессы хранения информации и доступа к ней в соответствии с установленными нормативно-правовыми актами. Информатизация общества становится стратегическим направлением, предопределяющим экономические и политические приоритеты в мировом сообществе. Человечество вступило в важнейший и неизбежный период своего развития – эру информатизации. Информационные сети, компьютеры и электронные информационные ресурсы составляют основу мировой инфраструктуры, позволяющей создавать единое информационное пространство и реализовать право каждого члена общества на информацию.

Развитие человечества знаменуется системой эпохальных открытий и перемен, преобладанием господствующих технологий, коренным об-

разом изменяющих характер жизни общества. Например, XVIII-е столетие было веком индустриальной революции, а в XIX-ом веке наступила эпоха паровых двигателей. В XX-ом веке главной технологией можно было считать сбор, обработку и распространение информации с помощью телефонных сетей, радио и телевидения, а также средствами компьютерной обработки. Согласно прогнозам XXI век станет веком глобальной информатизации и компьютеризации всего мира. В Окинавской хартии глобального информационного общества, в частности, говорится: «Информационно-коммуникационные технологии являются одной из самых мощных сил в формировании общества XXI века. Их революционное воздействие затрагивает образ жизни людей, их образование и работу. Они становятся жизненно важным двигателем роста мировой экономики».

Для перехода к информационному обществу и реализации его преимуществ Окинавская хартия определила, в частности, один из ключевых принципов, касающихся образовательных учреждений: «Развитие человеческих ресурсов, способных отвечать требованиям информационной эры, через образование, непрерывное обучение и удовлетворение растущего спроса на специалистов в области информационно-коммуникационных технологий».

Настоящее учебное пособие посвящено изложению основ теории построения информационных сетей. В нем описаны основные принципы передачи данных по физическим каналам, а также технологии построения локальных и глобальных сетей. В связи с возрастающей в последние годы проблемой защиты информации, в пособии описаны основные принципы обеспечения безопасности при построении компьютерных сетей и информационных систем.

Учебное пособие написано на основе накопленного автором многолетнего опыта практической работы в области разработки и внедрения информационно-коммуникационных технологий, проведенных научных исследований, а также чтения лекций в Самарском государственном университете. Оно рассчитано на студентов вузов, специализирующихся в области информационно-коммуникационных технологий, защиты информации и компьютерной безопасности.

Автор выражает искреннее признание рецензентам и специалистам Самарского государственного университета в области информационных технологий и компьютерных сетей за ценные советы и замечания по поводу содержания материала и методики его изложения.

ГЛАВА 1

РОЛЬ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В СОВРЕМЕННОМ ОБЩЕСТВЕ

Введение

Современная научно-техническая революция характеризуется гигантским возрастанием социального и экономического значения информационной деятельности как средства обеспечения научной организации, контроля, управления и осуществления общественного производства. Сформировалась и бурно развивается особая, находящаяся на самом острие научно-технического прогресса (НТП) отрасль народного хозяйства – индустрия информатики, организация которой обусловливает все в большей степени эффективное функционирование всех прочих отраслей народного хозяйства.

По данным ЮНЕСКО в настоящее время уже более половины занятого населения развитых стран прямо или косвенно принимают участие в процессе производства и распространения информации. Так, по статистическим данным процесс перераспределения трудовых ресурсов из сферы материального производства и обслуживания в информационную сферу хозяйства США привел к тому, что уже сейчас в информационной сфере работает более 60 % занятого населения страны. Это свидетельствует о начале перехода развитых стран на качественно новый этап их технического развития, который часто называют «веком информации». Действительно, материальные затраты многих стран на

хранение, передачу и обработку информации превышают аналогичные расходы на энергетику.

Академик Б.Н. Наумов еще в 80-х годах писал, что «индустрия обработки информации играет в настоящее время для промышленно развитых стран ту же роль, которую на этапе индустриализации играла тяжелая промышленность». «В конце этого (XX!) столетия информационные ресурсы станут основным национальным богатством (промышленно развитых стран), а эффективность их промышленной эксплуатации во все большей степени будет определять экономическую мощь страны в целом». Причем ведущую роль будут играть «активные» информационные ресурсы, то есть та часть ресурсов, которую составляет информация, доступная для автоматизированного поиска, хранения и обработки. В США, например, компьютерная информатика, занимавшая по объему капиталовложений совсем недавно третье место среди отраслей хозяйства (после автомобильной промышленности и нефтепереработки), сейчас вышла на первое место.

1.1. Что такое «информационное общество»

Непрерывно увеличивающийся объем информации во всех отраслях человеческой деятельности и все возрастающая потребность в ее оперативном и полном получении обусловили активизацию работ в области создания и внедрения компьютерных информационных технологий. Развитие систем телекоммуникаций и использование Internet/Intranet технологий позволили вывести информатизацию на новый качественный уровень. Современные автоматизированные информационные системы (АИС), опираясь на последние достижения в области аппаратно-программных средств и систем телекоммуникаций, дают возможность хранить в базе данных большие объемы информации, поддерживать распределенную обработку данных, обеспечивать доступ к ресурсам системы, как по локальной вычислительной сети (ЛВС), так и через Internet.

Значительный рост вычислительной мощности современных ПЭВМ и увеличение пропускной способности локальных вычислительных сетей обусловили в области информационных техно-

логий тенденцию к переходу от классической централизованной модели обработки данных, основанной на применении больших ЭВМ, к модели, подразумевающей распределенную обработку централизованно хранящейся информации. Такой подход дает возможность использования в глобальных информационных процессах вычислительных ресурсов ПЭВМ путем частичного переноса алгоритмов обработки данных с центральных ЭВМ (серверов) на компьютеры пользователей (рабочие станции).

Применение новых информационных технологий приносит целый спектр новых, недоступных ранее возможностей, устраняя рутинные операции, обеспечивая своевременный и быстрый доступ пользователей к нужной информации и в целом резко повышая эффективность всей работы. Реализация быстрого доступа к информации создает условия для выполнения основного принципа открытого общества – принципа всеобщей доступности информации.

По определению ЮНЕСКО, **информатизация** – *это «развитие и широкомасштабное применение методов и средств сбора, преобразования, хранения и распространения информации, обеспечивающих систематизацию имеющихся и формирование новых знаний и их использование обществом в целях его текущего управления и дальнейшего совершенствования и развития».* Информатизация общества (ИО) представляет собой целенаправленный процесс изменения социальной информационной среды. Цель ИО состоит в повышении эффективности эксплуатации информационных ресурсов общества путем системной компьютеризации всех этапов жизненного цикла информации – ее создания, накопления, хранения, обработки, использования.

Развитие процессов информатизации и информационной инфраструктуры, повышение доли информационной компоненты в жизни общества и превращение информационного продукта в стратегический ресурс приводят к глубинным социальным изменениям и являются необходимыми условиями трансформации общества из индустриального в гражданское и дальнейшего перехода к его высшей стадии – информационному обществу. Характерным признаком такого общества является то, что информационные технологии и телекоммуникации становятся базовыми в экономике и уровень их внедрения в значительной степени определяет уровень

развития страны в целом. Согласно прогнозам, XXI век станет веком глобальной информатизации и компьютеризации всего мира. В решении задач информатизации общества и перехода от индустриального общества к информационному особо важная роль принадлежит телекоммуникационным вычислительным сетям (ТВС), в которых сосредоточены новейшие средства вычислительной техники и средства связи, а также самые прогрессивные и эффективные технологии, в том числе информационные технологии. Трудно переоценить роль ТВС в любой сфере человеческой деятельности: социально-экономической, научно-технической, производственной, организационно-экономического управления, обучения и подготовки кадров, правовой. Можно утверждать в связи с этим, что ТВС составляют основу материально-технической базы информатизации общества.

Информатизацию можно трактовать как создание и совершенствование промышленно развитой системы (отрасли) производства и распространения информации, прежде всего средств вычислительной техники, связи и информационных технологий, которые получили название средств информатизации. Производство основных средств информатизации связывают с понятием новой отрасли хозяйства – индустрии информатики. Уже в середине 80-х годов эта отрасль вышла на ведущее место в мире как по масштабам охвата сфер человеческой деятельности, так и по темпам роста производства и объемов сбыта товарной продукции. В решении проблем информатизации чрезвычайно важная роль отводится информационной технологии (ИТ), т.е. информационному обеспечению любого вида человеческой деятельности. **Информационная технология** включает технологию получения, передачи, обработки, хранения информации и ее использования для обеспечения человеческой деятельности. Уровень развития ИТ – один из критериев не только экономического, но и политического могущества государства.

В июле 2000 года странами «Большой восьмерки» была принята Окинавская хартия глобального информационного общества, в которой, в частности, говорится: «Информационно-коммуникационные технологии являются одной из самых мощных сил в формировании общества XXI века. Их революционное воздействие затрагивает образ жизни людей, их образование и

работу, а также взаимодействие правительства с гражданским обществом. ИТ быстро становятся жизненно важным двигателем роста мировой экономики». Развитие информационной индустрии невозможно без активной роли государства в формировании «режима наибольшего благоприятствования». В развитых странах в структуре внутреннего валового продукта на развитие информационных технологий направляется около 20% средств. В России эта доля, к сожалению, составляет всего 1%. Крайне слаба оснащенность домашней компьютерной техникой и средствами телекоммуникаций.

В Москве компьютеры имеют около 40 % семей, в малых городах менее 5 %, а в сельской местности и того меньше, не говоря о том, что подключение к Интернет из дома на селе считается экзотикой.

Сегодня бизнес, связанный с информационными технологиями, является одним из самых динамичных и высокодоходных секторов мировой экономики. Позиции России здесь все еще очень скромные: менее одного процента мирового рынка. К сожалению, развитие ИТ-индустрии в России не является национальной стратегической программой, как, например, в Индии и ряде других стран.

Небольшая предыстория. Когда в 1985 г. началась перестройка, многим казалось, что через 5 – 10 лет страна выйдет на новый, широкий путь развития демократии. Однако, не блестящие результаты экономических экспериментов в эти годы не только дискредитировали в глазах общества понятие «демократии», но и привели к усилению в стране настроений в пользу «сильной руки», т.е., по сути, авторитарного режима. Почему? Утверждают, что главная причина – это слабость российского гражданского общества. А есть ли у нас это общество вообще?

Гражданское общество – это понятие сложное, неоднозначное. Если *информационное общество* – это понятие, обсуждаемое в основном в среде профессионалов, которые имеют опыт работы с информационными ресурсами и пытаются создать некую обобщающую платформу, то понятие «гражданское общество», по-видимому, кажется ясным всем. В Юридической энциклопедии дано определение гражданского общества: **Гражданское общество** – *это общество с развитыми экономическими, культурны-*

ми, правовыми и политическими отношениями между его членами, не зависимое от государства, но взаимодействующее с ним; общество граждан высокого социального, экономического, политического, культурного и морального статусов, создающих совместно с государством развитые правовые отношения (Юридическая энциклопедия / Под ред. Ю.Н. Тихомирова. 1999).

Если данное определение взять за основу, то для гражданского общества необходимы следующие компоненты: признание и равная защита всех форм собственности, приоритет фундаментальных прав и свобод человека и гражданина, разделение властей, идеологическое, политическое многообразие и многопартийность, развитие всех форм самоуправления, в особенности территориального, автономия университетов и профессиональных сообществ, свобода вероисповедания.

Ответ на вопрос, есть такое общество у нас или нет, очевиден. Мы находимся лишь на начальной стадии создания гражданского общества. Поэтому можно постулировать следующее: в отличие от развитых западных стран, которые прошли естественный путь, т.е. создали сначала гражданское общество, а затем обеспечили условия для перехода к информационному, мы вынуждены делать эти вещи параллельно. Для утешения можно сказать, что мы в этом не одиноки, и не только страны Восточной Европы и СНГ разделяют нашу участь.

Можно сколько угодно спорить о том, какого уровня «информационности» общества мы уже достигли и достигли ли вообще, живем ли мы в информационном обществе или еще нет и т.д. Очевидно одно – наше общество вступило на путь к информационному, и эта тенденция характерна для всех стран, входящих в третье тысячелетие. Информатизация общества становится стратегическим направлением, предопределяющим экономические и политические приоритеты в мировом сообществе. Человечество вступило в важнейший и неизбежный период своего развития – эру информатизации. Информация становится важнейшим стратегическим ресурсом общества, во многом определяющим его способность к дальнейшему развитию. Информатизация – это всеобщий неизбежный период развития человеческой цивилизации, период создания индустрии производства и обработки информации.

Конечно, уровень «информационности» общества во всех странах разный. Он выше там, где созданы основы гражданского общества, развита информационная и телекоммуникационная индустрия, компьютерные технологии стали такой же неотъемлемой частью жизни, как жилье, еда, транспорт. Мы не можем всем этим похвалиться, однако и наш уровень неуклонно повышается. Интернет прочно обосновался в стране и уже становится, как и во всем мире, единой коммуникационной и информационной средой. Огромное количество компьютеров ежедневно прибывает в Россию. Это уже неплохой показатель «информационности» нашего общества.

Термин *информационное общество* и масштабные проекты, нацеленные на его создание, впервые появились на Западе. Например, понятие *национальная глобальная информационная инфраструктура* ввели в США после известной конференции Национального научного фонда 1992 г. и знаменитого доклада Б. Клинтона – А. Гора «Технологии для экономического роста Америки: новые направления, которые предстоит создать» (1993); *информационное общество* – появилось в работах Экспертной группы Европейской комиссии по программам информационного общества под руководством Мартина Бангеманна, одного из наиболее уважаемых в Европе экспертов по информационному обществу; *информационные магистрали* и *супермагистрали* – в канадских, британских и американских публикациях.

Сегодня термин *информационное общество* прочно занял свое место, причем не только в лексиконе специалистов в области информации, но и в лексиконе политических деятелей, экономистов, ученых. В большинстве случаев это понятие ассоциируется с развитием информационных технологий и средств телекоммуникации, позволяющих на платформе гражданского общества (или, по крайней мере, на основе продекларированных его принципов) осуществить новый эволюционный скачок и достойно войти в следующий век уже в качестве информационного общества или его начального этапа.

Следует сказать, что информационное общество отличается прежде всего тем, что информационные технологии и услуги растут более быстрыми темпами и начинают доминировать в экономике. Они становятся базовыми, и уровень их развития в значи-

тельной степени определяет уровень развития страны в целом. Характерные черты и признаки информационного общества, которые были сформированы в США, странах Западной Европы, Канаде и ряде развитых стран Азии, должны, естественно, служить ориентиром и для отбора направлений и приоритетов при построении такого общества в России.

Это путь долгий, так как необходимо достичь той ступени постиндустриального развития, которая требуется для построения информационного общества. *На этом пути вхождения в информационное общество существуют ориентиры, которые можно сформулировать в виде следующих положений:*

– *формирование единого информационно-коммуникационного пространства* как части мировой информационной инфраструктуры;

– *развитие новых и высоких технологий*, базирующихся на массовом использовании перспективных информационных технологий;

– *создание и развитие рынка информации* и удовлетворение потребности общества в информационных продуктах и услугах;

– *повышение уровня образования*, научно-технического и культурного обмена за счет расширения регионального, национального и международного информационного взаимодействия;

– *создание системы обеспечения прав граждан* и социальных институтов на свободное получение, распространение и использование информации, а также ряд других положений.

В историческом аспекте можно привести краткую хронологию американского пути вхождения в информационное общество (все даты достаточно условны, но, тем не менее, многие из них являются определяющими):

1988 г. – Подкомитет по науке, технологиям и космосу Сената США провел слушания под председательством Альберта Гора по теме компьютерных сетей и будущей сети Национального научного фонда США, которая и была создана при непосредственном участии и патронаже А. Гора.

1991 г. – А. Гор выдвинул новую *сетевую инициативу,* предложил создать Национальную компьютерную сеть для науки и образования (National Research and Education Network – NREN).

NREN связала суперкомпьютерные центры страны, сделав эту мощь доступной для всех ученых и исследователей.

1992 г. – Национальный научный фонд (NSF) организовал конференцию, в рамках которой были опубликованы ключевые доклады по созданию Национальной информационной инфраструктуры и выработке государственной политики; здесь впервые было введено понятие *глобальной информационной инфраструктуры*.

1993 г. – Опубликован меморандум Б. Клинтона – А. Гора, что считается важным этапом в достижении определенного уровня *информационности* американского общества.

Следует подчеркнуть, что все названные документы принимались на самом высоком уровне, и в их формулировках фигурируют первые лица страны.

Далее **(1994 г.)** были предложения о создании высокоскоростных информационных магистралей и супермагистралей, появились мощные трансатлантические сети и проекты, которые связали к тому времени (1995 – 1997 гг.) программы информационного общества США с соответствующими программами европейских стран. Европейский Союз начал практическую деятельность в этом направлении уже в 1993 г.

В **июле 2000 года** странами «Большой восьмерки» была принята «Окинавская хартия глобального информационного общества».

Развитие человечества знаменуется системой эпохальных открытий и перемен, коренным образом изменяющих характер жизни общества. К таким событиям, безусловно, относится и повсеместное распространение информационных технологий (ИТ) и телекоммуникаций. Чтобы еще лучше понять наступающую эпоху информационного общества, следует немного углубиться и в более раннюю историю. Многие исследователи считают первым этапом, первой исторической вехой изобретение в XV веке печатного станка. Вторым этапом по праву считается появление телефона, ибо он позволил создать новую коммуникационную технологию. Далее, третий этап – радио, послужившее прообразом сегодняшних спутниковых коммуникаций. Четвертым этапом информационной эволюции можно считать появление персональных компьютеров, которые позволили человеку общаться без

посредников с информационным пространством. И, наконец, пятый этап – период компьютерных коммуникаций, развития средств доступа к информации, Интернета и мировой информационной инфраструктуры.

Появление всемирной коммуникационной оболочки – Internet внесло революционные перемены в аспекте свободы распространения информации. Internet стал открытым каналом, позволяющим каждому пользователю публиковать собственные взгляды и идеи. По сути сняты финансовые и региональные барьеры на пути глобального распространения информации, обеспечен доступ к процедурам ее извлечения и модификации. С другой стороны, на передний план выдвигается чрезвычайно важная и актуальная проблема борьбы с правонарушениями в сфере информационных технологий и электронным терроризмом в телекоммуникационных сетях.

1.2. Условия построения информационного общества

Основная проблема информатизации заключается не только и не столько в том, чтобы разработать и внедрить средства информатизации, а в том, чтобы обеспечить эффективность их применения в различных областях производства, науки и социально-бытовой сферы. Эффективность использования средств информатизации зависит от таких факторов, как уровень совершенства действующих экономических отношений, подготовленность общества и отдельных его членов к восприятию информационных технологий, финансовые возможности, уровень материально-технической базы, состояние технологии производства. В связи с этим информатизация конкретных объектов предполагает наличие подготовительного этапа, на котором перечисленные факторы приводятся в адекватное соответствие с ее требованиями.

Наше государство сделало достаточно большой шаг на пути построения гражданского общества. Для перехода к следующей стадии развития и построению информационного общества необходимо решить еще ряд сложных задач. Эти задачи в научной литературе трактуются неоднозначно. Например, Я.Л Шрайберг.

(Основные положения и принципы разработки автоматизированных библиотечно-информационных систем и сетей. М.: «Либерея», 2001 – 104 с.) формулирует задачи следующим образом:

– развитие и совершенствование информационной и телекоммуникационной инфраструктуры;

– содействие приходу частных инвестиций в информационные и телекоммуникационные технологии (государственные инвестиции пусть слабо, но идут, а вот частные – это новый шаг для страны, и по этому пути проходили все развитые страны);

– стимулирование использования информационных технологий в образовании, научных исследованиях и культуре;

– создание и развитие информационных ресурсов и электронных библиотек;

– обеспечение информационной безопасности и защита информации;

– расширение международного сотрудничества и коммерческой взаимовыгодной деятельности в области информационных и телекоммуникационных технологий.

Очевидно, что для перехода к информационному обществу необходима в первую очередь высокая информационная культура его членов, а также кадры профессионалов в области разработки и внедрения информационных технологий. Поэтому в плане подготовки членов информационного общества ведущая роль принадлежит образовательным учреждениям. Во многих концепциях и программах в сфере образования ставятся задачи по подготовке кадров и информатизации сферы образования, состоящие из следующих основных компонент:

1. Оснащение аппаратно-программными средствами.
2. Телекоммуникационная инфраструктура.
3. Информационные ресурсы.
4. Нормативно-правовая база.
5. Организационная структура.
6. Кадры.

В принципе указанные задачи определены верно. Однако для решения каждой из них необходимы квалифицированные кадры. Для решения первых двух задач в мире существует целый спектр технических средств и методологий. Выбор оптимальных вариантов должны определить специалисты. В свое время, по моему

убеждению, было принято ошибочное решение о сворачивании производства отечественных ЭВМ серии «Минск», «Мир», «БЭСМ» в пользу моделей ЕС и СМ, основанных на идеологии IBM и PDP. В результате отечественная компьютерная промышленность была уничтожена, а теоретические разработки и идеи наших ученых оказались реализованными в других государствах, продукцию которых мы вынуждены закупать.

Ключевыми составляющими информационного общества являются информация и знания. Обе они зависят от интеллектуального потенциала человека, их создающего и развивающего. Именно «интеллектуалоемкость» ИТ позволяет многим развивающимся странам поставлять на мировой рынок информационные услуги, продукты и технологии. Ярким примером тому может служить Индия. Для перехода к информационному обществу нужны в первую очередь специалисты в области информационных технологий, которые будут не только осуществлять процесс оснащения компьютерной техникой и системами телекоммуникаций, но и определять идеологию разработки новых отечественных аппаратно-программных средств и технологий.

Для перехода к информационному обществу и реализации его преимуществ в «Окинавской хартии» страны «Большой восьмерки» определили, в частности, один из ключевых принципов, касающийся учреждений подготовки и развития интеллекта: «Развитие человеческих ресурсов, способных отвечать требованиям информационной эры, через образование, непрерывное обучение и удовлетворение растущего спроса на специалистов в области ИТ. Концентрация внимания на общем образовании, а также расширении возможностей непрерывного обучения с упором на развитие навыков в сфере ИТ. Поощрение более эффективного и широкого использования ИТ в образовании…». Поэтому на первый план выдвигается задача подготовки кадров в области информационных технологий, а для этого необходимо опережающее оснащение средствами информатизации учреждений сферы подготовки и развития интеллекта.

Многие крупные фирмы, занимающиеся разработкой информационных технологий (например, Microsoft, IBM, и другие), передают свои разработки в образовательные учреждения по низким ценам, либо вообще бесплатно при их использовании для це-

лей образования. Информатизация образования во многих странах является приоритетным направлением развития. К сожалению, в законах «Об образовании», «Об информации, информатизации и защите информации», «О высшем и послевузовском профессиональном образовании» нет явных положений о первоочередном внедрении информационных технологий в образовательных учреждениях. Выделяемые на эти цели бюджетные средства явно недостаточны.

Как ни странным это может показаться, но качественного массового образования в области информационных технологий в России по большому счету нет. Для масштабного внедрения информационных технологий, а тем более для разработки отечественных аппаратно-программных средств и технологий необходимы не сотни, а десятки тысяч квалифицированных программистов. Однако, при существующем финансировании вузов и как следствие, слабой оснащенности средствами информатизации, говорить о массовой и качественной подготовке ИТ–специалистов не приходится. Количество Российских вузов, способных готовить специалистов в соответствии с мировым уровнем в области информационных технологий, можно пересчитать по пальцам.

На совещании по вопросам развития информационных технологий, состоявшемся 11 января 2005 года в городе Новосибирске, президент России В.В. Путин, в частности, отметил «Формирование современной инфраструктуры информационного сектора экономики может стать крупным национальным проектом… Формирование инфраструктуры информационного бизнеса должно идти в тесной увязке с модернизацией профессионального образования».

Наблюдающийся в последние годы процесс бурного развития глобального информационного обмена поставил ряд серьезных правовых вопросов. Мировое сообщество и, в частности, Россия явно отстает от процесса разработки соответствующих правовых норм, регулирующих отношения в сфере информационных технологий. В принятой федеральной целевой программе «Электронная Россия» среди факторов, сдерживающих широкое внедрение и эффективное использование ИТ в экономике России,

названа несовершенная нормативно-правовая база, разрабатывавшаяся без учета возможностей современных технологий.

На совещании в Новосибирске 11.01.2005 г. был рассмотрен вопрос о пилотном проекте создания четырех технопарков в области информационных технологий: в Сатисе (Нижегородская область, около г. Саров), Дубне, Санкт-Перербурге и под Новосибирском. Выступая на совещании, президент В.В. Путин отметил: «Деятельность создаваемых технопарков и других элементов инновационной инфраструктуры должна опираться на адекватное законодательство».

Учитывая вышесказанное, задачи по построению информационного общества можно сформулировать следующим образом:

1. Подготовка высококвалифицированных кадров в области разработки и внедрения информационных технологий, повышение уровня образования граждан в области использования информационных технологий в профессиональной деятельности, для чего необходимо оснащение компьютерной техникой в первую очередь учреждений сферы подготовки и развития интеллекта.

2. Развитие телекоммуникационной инфраструктуры и формирование единого информационного пространства, интегрированного с мировой информационной инфраструктурой.

3. Создание и защита отечественных электронных информационных ресурсов, доступных всем членам общества и удовлетворяющих его потребности в различных сферах деятельности.

4. Создание нормативно-правовой базы в области информационных технологий, в том числе информационной безопасности и защите авторских прав на электронные информационные ресурсы.

1.3. Роль образовательных учреждений в построении информационного общества

В решении указанных выше задач по построению информационного общества важнейшая роль принадлежит учреждениям сферы подготовки и развития интеллекта (образовательным учреждениям). На систему образования возлагается задача подготовки высококвалифицированных специалистов, способных использовать информационные технологии в профессиональной

деятельности. С другой стороны сами образовательные учреждения должны обладать высокой степенью использования информационно-коммуникационных технологий. Информатизация сферы образования должна способствовать решению двух основных задач: расширение доступности образования и существенное улучшение его качества. В связи с этим встает вопрос о критериях оценки качества подготовки специалистов образовательными учреждениями. Например, в высшем образовании в настоящее время основными критериями оценки студентов являются успеваемость и посещаемость. Практически нет критериев, использующих понятия эффективности и степени отдачи от вложенных в подготовку специалиста средств. В результате такой системы подготовки многие выпускники остаются без работы по специальности.

Более эффективной является модель системы подготовки специалистов, состоящая из триады: «заказчик», «интеллект», «отдача» (рис.1.1). Заказчик финансирует подготовку специалиста (интеллекта) в соответствии со своими потребностями и уровнем развития науки и техники. Полученные специалисты не только выполняют конкретную работу для заказчика на основе полученных знаний, но и создают новые идеи в сфере производства, науки и технологий. В результате рождаются новые идеи, научные направления и отрасли, для реализации которых появляются заказчики и необходимость в подготовке кадров по новым специальностям. Подтверждением жизнеспособности такой модели может стать, например, начало подготовки кадров для индустрии информатизации по специальностям в области компьютерной безопасности и защиты информации.

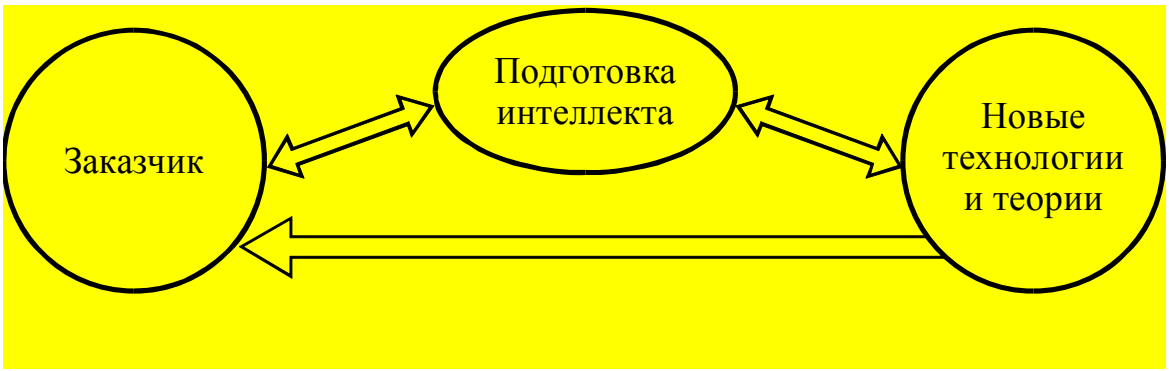


Рис 1.1. Модель подготовки специалистов

В последние годы в сфере образования наблюдается рост числа коммерческих образовательных учреждений разного уровня. Качество подготовки специалистов в них во многом определяется степенью использования учреждением информационных технологий. В настоящее время уровень информатизации образовательных учреждений определяется в основном простым статистическим учетом количества компьютеров. Существует простой показатель уровня – количество студентов на один компьютер. Однако одинаковые по мощности компьютеры в локальном варианте и в составе корпоративной сети с возможностью доступа к мировым информационным ресурсам имеют совершенно разный качественный уровень. Поэтому наличие корпоративной сети и количество включенных в нее компьютеров является более точным показателем уровня информатизации.

Особенностью сферы подготовки интеллекта является обязательное наличие учебно-научной библиотеки. От эффективности ее работы во многом зависит качество подготовки специалистов. Совершенно разный уровень качества библиотеки определяется организацией доступа к библиотечным ресурсам. Несоизмеримо быстрее осуществить библиографический поиск по электронному каталогу, чем по бумажным картотекам. Наличие автоматизированной библиотечной информационной системы с доступом к электронным каталогам и полнотекстовой информации также является важным показателем уровня информатизации.

Важным показателем также является степень использования компьютеров в преподавании дисциплин учебного плана. В данном случае использование компьютеров предполагает наличие обучающих курсов по изучаемым дисциплинам, электронных учебников и других электронных ресурсов учебного назначения.

В связи с этим простой показатель количества компьютеров не отражает уровень информатизации образовательных учреждений, а также не характеризует эффективность использования информационных технологий. Для оценки уровня информатизации предлагается ввести термин «информационный интеллект учреждения».

Определение 1

Информационный интеллект учреждения – совокупность компьютеров, средств телекоммуникаций и доступных рациональных информационных материалов на электронных носителях.

Фактически информационный интеллект образовательного учреждения (I) функционально зависит от степени оснащения компьютерной техникой (К), средствами телекоммуникаций (Т) и доступными электронными информационными ресурсами (М)

$$I=F(K, T, M).$$

Уровень информационного интеллекта учреждения может быть рассчитан по формуле:

$$У=Ко\times(Кт+Кб+Ку),$$

где Ко – коэффициент оснащенности компьютерами, Кт – коэффициент использования телекоммуникаций, Кб – коэффициент автоматизации доступа к библиотечно-информационным ресурсам, Ку – коэффициент информатизации учебного процесса, который отражает использование мультимедийных обучающих систем, электронных курсов лекций и других электронных учебно-методических материалов.

В свою очередь указанные коэффициенты определяются следующими отношениями:

$$Ко=Nк/Nу,$$

$$Кт=Nс/Nк,$$

$$Кб=Бэ/Бо,$$

$$Ку=Ук/Уо,$$

где Nк – количество компьютеров, Nу – количество обучаемых, Nс – количество компьютеров, объединенных в корпоративную сеть, Бо – общий фонд библиотеки, Бэ – фонд в электронном каталоге, Уо – общее количество учебных дисциплин, Ук – количество учебных дисциплин, в преподавании которых используются информационные технологии.

В определении информационного интеллекта специально использовано понятие «рациональных информационных материа-

лов». Имея развитые средства телекоммуникаций с доступом к мировым информационным ресурсам, встает вопрос о полезности получаемой информации для развития интеллекта. В течение нескольких лет в России наблюдалась эйфория в связи с открытием доступа в Интернет. Все стремились получить доступ в мировую сеть, считая, что этим решат большинство проблем по информатизации. Однако мало кто отдавал себе полный отчет в том, сколько нужно этого «Интернета», за какие деньги и что он даст полезного для развития интеллекта.

При поддержке фонда Сороса в ряде университетов России были открыты центры Интернет с классами открытого доступа. Автором был проведен анализ наиболее часто посещаемых студентами сайтов в нескольких таких центрах. Оказалось, что около 80% обращений составили сайты развлекательного характера и только около 10% составили сайты с познавательной информацией, способствующей развитию интеллектуальных способностей и связанных с обучением по специальности. Таким образом, только десятая часть вложенных в центры Интернет средств (без учета стоимости аренды площадей и эксплуатационных расходов) пошла на решение основной задачи по подготовке кадров, формированию и развитию интеллекта. Более того, в «мировой паутине» (Интернет) содержится большое количество не только бесполезной, но и вредной информации (особенно для молодежи), например порнографического содержания, разжигающей национальную и религиозную вражду, террористической направленности и т. п. К вредной информации могут быть отнесены и некоторые типы компьютерных игр.

Следовательно, качественным является не показатель наличия выхода в Интернет, а показатель о характере получаемой информации, ее практическом влиянии на процесс подготовки высококвалифицированных специалистов и развития интеллекта. В связи с этим необходимо ввести термин «**информационная экология**». Уровень состояния информационной экологии может определяться по формуле

$$Э=Ор/Оо,$$

где Оо – общее количество полученной из сети информации, Ор – количество полученной рациональной информации.

В связи с этим всякая информационная система должна содержать технические, программные и нормативные средства, позволяющие контролировать и поддерживать соответствующий уровень информационной экологии. Эта задача далеко не простая и требует проведения технических и научных исследований, на основании которых могут быть приняты соответствующие нормативные акты. Кроме того, наряду с информационной составляющей информационная экология должна отражать и уровень вредного воздействия технических средств на организм человека. Поэтому можно дать следующее определение науки «информационная экология»:

Определение 2

Информационная экология – область науки об отношениях человека и информационных технологий, включая факторы вредного воздействия на человека технических средств и электронных информационных материалов.

1.4. Основные положения «Окинавской хартии глобального информационного общества»

Хартия принята странами «Большой восьмерки» 22 июля 2000 года на острове Окинава (Япония). От имени России ее подписал президент РФ. Она нацелена на решение проблем глобального информационного общества. Этот документ имеет для России большое значение и оказывает влияние на развитие законодательства в информационной сфере. В российском праве принципы Окинавской хартии прослеживаются в Программе социально-экономического развития и в ФЦП «Электронная Россия». Хартия декларирует два основных базовых принципа: максимально полная реализация преимуществ ИТ («открытие цифровых возможностей») и преодоление неравного доступа к ИТ («преодоление цифрового разрыва»). Окинавской хартии предшествовала Правительственная декларация экономического и социального совета ООН о роли ИТ в контексте глобальной экономики, основанной на знани-

ях, в которой подчеркивается необходимость принятия согласованных усилий на международном уровне. Ниже приводится текст хартии (взят из книги: Шамраев А.В. Правовое регулирование информационных технологий (анализ проблем и основные документы) – М.: «Статут», 2003. – 1013 с. www. b2b-lex. ru).

Окинавская Хартия глобального информационного общества от 22 июля 2000 г.

1. Информационно-коммуникационные технологии (ИТ) являются одной из самых мощных сил в формировании общества двадцать первого века. Их революционное воздействие затрагивает образ жизни людей, их образование и работу, а также взаимодействие правительства с гражданским обществом. ИТ быстро становятся жизненно важным двигателем роста мировой экономики. Они также обеспечивают многим частным лицам, фирмам и сообществам, занимающимся предпринимательской деятельностью, во всех частях земного шара возможность решать экономические и социальные проблемы с большей эффективностью и воображением. Огромные возможности открываются перед всеми нами и разделяются всеми нами.
2. Сущностью стимулируемой ИТ экономической и социальной трансформации является ее способность содействовать людям и обществам использовать знания и идеи. Наше видение информационного общества является тем, которое лучше позволяет людям использовать свой потенциал и реализовывать свои устремления. Для этого мы должны обеспечить, чтобы ИТ служили достижению взаимодополняющих целей создания устойчивого экономического роста, повышения общественного благосостояния, содействия социальному согласию и работали в целях полной реализации своего потенциала в укреплении демократии, увеличении прозрачности и подотчетности в управлении, поощрении прав человека, усилении культурного разнообразия и содействии международному миру и стабильности. Достижение этих целей и решение возникающих проблем потребует эффективных национальных и международных стратегий.

3. При достижении этих целей мы вновь повторяем свою приверженность принципу вовлечения: каждому повсеместно должна быть обеспечена возможность пользоваться преимуществами глобального информационного общества и никто не должен из этого исключаться. Устойчивость такого общества зависит от демократических ценностей, содействующих человеческому развитию, таких как свободное движение информации и знаний, взаимная терпимость и уважение человеческого разнообразия.
4. Мы будем осуществлять руководство в продвижении усилий правительств по содействию надлежащей политике и регулятивному окружению в целях стимулирования конкуренции и инноваций, обеспечения экономической и финансовой стабильности, развития сотрудничества участников [экономического процесса] в оптимизации глобальных сетей, борьбе со злоупотреблениями, подрывающими целостность сетей, преодолению цифрового разрыва, инвестированию в людей и поощрению глобального доступа и участия.
5. Прежде всего, настоящая Хартия является призывом ко всем, как в государственном, так и в частном секторе, преодолеть международный разрыв в области информации и знаний. Солидная основа для политики и действий в сфере ИТ может изменить методы нашего взаимодействия по продвижению социальных и экономических возможностей в мировом масштабе. Эффективное партнерство участников [экономического процесса], включая сотрудничество в выработке совместной политики, также является ключевым для прочного развития по-настоящему глобального информационного общества.

Открытие цифровых возможностей

6. Потенциальные преимущества ИТ, стимулирующие конкуренцию, способствующие увеличению производительности, создающие и поддерживающие экономический рост и занятость, имеют значительные перспективы. Наша задача заключается не только в стимулировании и содействии переходу к информационному обществу, но также и в реализации его полных экономических, социальных и культурных преимуществ. Для достижения этого важно основываться на следующих ключевых принципах:

– экономические и структурные реформы для создания атмосферы открытости, эффективности, конкуренции и инноваций, поддерживаемые политикой, нацеленной на адаптирующиеся рынки рабочей силы, развитие человеческих ресурсов и социальное согласие;

– рациональное макроэкономическое управление для содействия деловым кругам и потребителям более уверенно планировать будущее и использовать преимущества новых информационных технологий;

– разработка информационных сетей, предлагающих быстрый, надежный безопасный и экономичный доступ к сетевым технологиям, услугам и компьютерным [программным] приложениям через конкурентные рыночные условия и соответствующие инновации;

– развитие человеческих ресурсов, способных отвечать требованиям информационной эры, через образование, непрерывное обучение и удовлетворение растущего спроса на специалистов в области ИТ во многих секторах наших экономик;

– активное использование ИТ в государственном секторе и содействие предоставлению в онлайновом режиме услуг, необходимых для обеспечения повышенной доступности правительства для всех граждан.

7. Частный сектор играет ведущую роль в разработке информационных и коммуникационных сетей в информационном обществе. Однако, разработка предсказуемой, транспарентной и недискриминационной политики и регулятивного окружения, необходимого для информационного общества, зависит от правительств. Важно исключить излишнее регулятивное вмешательство, которое могло бы препятствовать продуктивным инициативам частного сектора по созданию благоприятного для ИТ окружения. Мы должны обеспечить, чтобы правила и практика, имеющие отношение к ИТ, отвечали революционным изменениям в экономических деловых связях, учитывая принципы эффективного партнерства между государственным и частным сектором, транспарентности и технологической нейтральности. Такие правила должны быть предсказуемыми и способствовать доверию деловых кругов и потребителей. Чтобы максимизировать социальные и экономические выгоды информационного

общества, мы соглашаемся со следующими ключевыми принципами и подходами и рекомендуем их другим:

– продолжать содействовать конкуренции и открывать рынки для поставки продуктов и услуг информационных технологий и телекоммуникаций, включая недискриминационное и основанное на затратах подключение к базовым телекоммуникациям;

– защита прав интеллектуальной собственности на технологии, связанные с ИТ, является жизненно важной для продвижения инноваций, связанных с ИТ, конкуренции и распространения новых технологий; мы приветствуем уже ведущуюся совместную работу органов в сфере интеллектуальной собственности и в дальнейшем будем поощрять наших экспертов обсуждать будущие направления работ в этой сфере;

– повторное обязательство правительств использовать программное обеспечение с полным соблюдением принципов защиты прав интеллектуальной собственности также является важным;

– ряд услуг, включая телекоммуникации, перевозки, доставку отправлений, является крайне важным для информационного общества и экономики, повышение их эффективности позволит максимизировать выгоды; таможенные и иные торговые процедуры также важны для развития благоприятного для ИТ окружения;

– содействовать трансграничной электронной коммерции путем дальнейшей либерализации и совершенствования сетей и связанных услуг и процедур в контексте строгих рамок Всемирной торговой организации (ВТО), продолжать работу в области электронной коммерции в ВТО и на других международных форумах, а также применение существующих торговых правил ВТО к электронной коммерции;

– совместные подходы к налогообложению электронной коммерции, основанные на конвенционных принципах, включая нейтральность, справедливость, простоту и прочие ключевые элементы, согласованные в процессе работы Организации экономического сотрудничества и развития (ОЭСР);

– продолжать практику невзимания таможенных пошлин с электронных передач данных до пересмотра этого вопроса на уровне правительств на следующей конференции ВТО;

– продвижение рыночных стандартов, включая, например, технические стандарты операционного взаимодействия;

– повышать доверие потребителей к электронным торговым площадкам в соответствии с основными принципами ОЭСР и предоставлять потребителям в онлайновом мире такую же защиту, что и в офлайновом, в том числе через эффективные инициативы саморегулирования, как онлайновые кодексы поведения, знаки доверия и другие программы надежности, а также изучать варианты устранения сложностей, испытываемых потребителями при трансграничных спорах, включая использование альтернативных механизмов разрешения споров;

– развитие эффективного и значимого механизма защиты частной жизни потребителей, а также защиты частной жизни при обработке персональных данных, обеспечивая при этом свободный поток информации, а также;

– дальнейшее развитие и эффективное функционирование электронной аутентификации, электронной подписи, криптографии и других средств обеспечения безопасности и определенности сделок.

8. Международные усилия по развитию глобального информационного общества должны сопровождаться согласованными действиями по созданию свободного от преступности и безопасного киберпространства. Мы должны обеспечивать, чтобы эффективные меры, изложенные в Общих принципах ОЭСР по безопасности информационных систем, претворялись в жизнь в целях борьбы с киберпреступностью. Будет расширено сотрудничество стран «Большой восьмерки» в рамках Лионской группы по транснациональной организованной преступности. Мы будем и далее содействовать диалогу с индустрией, основываясь на успехе недавней Парижской конференции «Большой восьмерки» «Диалог правительства и индустрии о безопасности и доверии в киберпространстве». Насущные проблемы безопасности, такие, как хакерство и компьютерные вирусы, также требуют эффективной политической реакции. Мы будем продолжать привлечение представителей индустрии и других участников

экономического процесса к защите жизненно важных информационных инфраструктур.

Преодоление цифрового разрыва

9. Преодоление цифрового разрыва внутри государств и между ними занимает важное место в наших соответствующих национальных повестках дня. Каждый должен иметь возможность доступа к информационным и коммуникационным сетям. Мы вновь подтверждаем нашу приверженность уже предпринимаемым усилиям в целях сформулировать и реализовать последовательную стратегию решения данного вопроса. Мы также приветствуем растущее признание со стороны индустрии и гражданского общества необходимости преодоления этого разрыва. Мобилизация наших знаний и ресурсов является необходимым элементом нашей реакции на данный вызов. Мы будем продолжать стремиться к эффективному партнерству между правительствами и гражданскими обществами, чутко реагирующими на высокие темпы технологического и рыночного развития.
10. Ключевой составляющей нашей стратегии должно стать непрерывное движение в направлении универсального и экономичного доступа. Мы продолжим:
    – содействовать рыночным условиям, способствующим предоставлению экономичных коммуникационных услуг;
    – изыскивать другие дополнительные средства, включая доступ через имеющиеся публичные мощности;
    – отдавать приоритет улучшению сетевого доступа, в особенности в отсталых городских, сельских и отдаленных территориях;
    – уделять особое внимание потребностям и возможностям социально незащищенных, ограниченно трудоспособных и пожилых людей, а также активно осуществлять меры, способствующие доступу и использованию с их стороны;
    – поощрять дальнейшее развитие «дружественных» для пользователей, «безбарьерных» технологий, включая мобильный доступ к Интернету, а также более широкое использование бесплатного и общедоступного информационного наполнения таким образом, который уважает права интеллектуальной собственности.

11. Политика прогресса информационного общества должна сопровождаться развитием человеческих ресурсов, способных отвечать требованиям информационной эры. Мы обязуемся предоставлять всем нашим гражданам возможность приобретения грамотности и навыков в области ИТ через образование, непрерывное обучение и подготовку. Мы продолжим работу в направлении этой масштабной цели, предоставляя онлайновый доступ школам, классам и библиотекам, а также преподавателей, имеющих навыки работы в сфере ИТ и мультимедийных ресурсов. Кроме того, будут реализовываться меры, направленные на предложение поддержки и инициатив предприятиям малого, среднего бизнеса и самозанятым по выходу в онлайн и эффективному использованию Интернета. Мы также будем поощрять использование ИТ в целях предоставления инновационных возможностей непрерывного обучения, в частности, тем, кто иначе не имел бы доступа к образованию и подготовке.

Содействие глобальному участию

12. ИТ открывают огромные возможности для возникающих и развивающихся экономик. Страны, преуспевшие в использовании своего потенциала, могут надеяться на преодоление традиционных препятствий инфраструктурного развития, более эффективное решение своих насущных задач в области развития, таких, как сокращение бедности, здравоохранение, санитарные условия и образование, а также использование преимуществ быстрого роста глобальной электронной коммерции. Некоторые развивающиеся страны уже достигли значительного прогресса в этих областях.
13. Вместе с тем, не может недооцениваться проблема преодоления международного разрыва в области информации и знаний. Мы признаем приоритетность этого со стороны многих развивающихся стран. В действительности, все развивающиеся страны, которые не способны поддерживать возрастающий темп инноваций в области ИТ, могут быть лишены возможности в полной мере участвовать в информационном обществе и экономике. Это особенно справедливо там, где распространение ИТ сдерживается существующими недостатками в развитии базо-

вой экономической и социальной инфраструктуры, такой как электроэнергетика, телекоммуникации и образование.

14. Мы признаем, что при решении этой проблемы следует учитывать разнообразие условий и потребностей развивающихся стран. Здесь отсутствует универсальное решение. Для развивающихся стран крайне важно приходить к решению через принятие последовательных национальных стратегий для создания благоприятного для ИТ и конкуренции политического и регулятивного окружения, использования ИТ для достижения целей развития и социального согласия, развития человеческих ресурсов, обладающих навыками в области ИТ, а также поощрения инициатив сообществ и местного предпринимательства.

Дальнейший путь

15. Усилия по преодолению международного разрыва в наших обществах в решающей степени зависят от эффективного сотрудничества между всеми участниками [экономического процесса]. Двустороннее и многостороннее сотрудничество будет продолжать играть важную роль в создании рамочных условий для развития ИТ. Международные финансовые организации (МФО), включая многосторонние банки развития (МБР), в частности Всемирный банк, достаточно приспособлены для участия в этом посредством разработки и проведения программ содействия экономическому росту, борьбе с бедностью, а также расширению совместимости, доступа и обучения. Международный союз электросвязи (МСЭ), Конференция ООН по торговле и развитию (ЮНКТАД), Программа развития ООН (UNDP) и другие соответствующие международные форумы также должны играть важную роль. Частный сектор сохраняет свою центральную роль в продвижении ИТ в развивающихся странах и может существенно способствовать международным усилиям по преодолению цифрового разрыва. Неправительственные организации (НО) с их уникальными возможностями достижения широких результатов могут плодотворно способствовать развитию человеческих и общественных ресурсов. Кратко говоря, ИТ глобальны по своему измерению и требуют глобальной реакции.

16. Мы приветствуем уже предпринимаемые усилия по преодолению международного цифрового разрыва через двусторон-

нюю помощь в области развития и по линии международных организаций и частных групп. Мы также приветствуем вклад частного сектора в лице таких организаций, как Глобальная инициатива по преодолению цифрового разрыва Всемирного экономического форума (WEF), Глобальный бизнес-диалог по электронной коммерции (GBD) и Глобальный форум.

17. Как отмечается в Правительственной декларации о роли ИТ в контексте глобальной экономики, основанной на знаниях, Экономического и социального совета ООН (ECOSOC), существует необходимость расширения международного диалога и сотрудничества в целях повышения эффективности программ и проектов в области ИТ совместно с развивающимися странами и сведения воедино «наилучшей практики», а также мобилизации ресурсов, имеющихся у всех участников, чтобы способствовать ликвидации цифрового разрыва. «Большая восьмерка» будет стремиться содействовать упрочнению партнерства между развитыми и развивающимися странами, гражданским обществом, включая частные фирмы и НО, фонды и академические учреждения, а также международными организациями. Мы будем также работать над тем, чтобы развивающиеся страны в партнерстве с другими участниками [экономического процесса] могли получать финансовые, технические и политические ресурсы в целях создания лучшего окружения для ИТ и их использования.

18. Мы соглашаемся образовать Рабочую группу по цифровым возможностям (Группу DOT) в целях включения наших усилий в общий более широкий международный подход. С этой целью Группа DOT будет созвана в кратчайшие сроки для изучения наилучших возможностей присоединения к работе всех участников [экономического процесса]. Эта Рабочая группа высокого уровня в тесных консультациях с другими партнерами и с учетом потребности развивающихся стран будет:

– активно содействовать дискуссиям с развивающимися странами, международными организациями и другими участниками [экономического процесса] для продвижения международного сотрудничества в целях формирования политической, регулятивной и сетевой готовности, улучшения совместимости, расширения доступа и снижения затрат, формирования чело-

веческого потенциала, а также поощрения участия в сетях глобальной электронной коммерции;

– поощрять собственные усилия «Большой восьмерки» в целях сотрудничества по связанным с ИТ пилотным программам и проектам;

– содействовать более тесному политическому диалогу между партнерами и работать над повышением глобальной общественной информированности о вызовах и возможностях;

– изучать вклад частного сектора и других заинтересованных групп, таких, как Глобальная инициатива по преодолению цифрового разрыва;

– сообщать о своей деятельности и выводах нашим личным представителям до следующей встречи в Генуе.

19. Для выполнения этих задач Группа DOT будет изыскивать пути к принятию конкретных шагов в указанных ниже приоритетных направлениях:

Формирование политической, регулятивной и сетевой готовности:

– консультирование поддерживающей политики и строительство местного потенциала в целях содействия конкурентной, гибкой и социально содержательной политике и регулятивному окружению;

– содействие обмену опытом между развивающимися странами и другими партнерами;

– поощрение более эффективного и широкого использования ИТ в рамках усилий в сфере развития, охватывающих такие широкие области, как сокращение бедности, образование, государственное здравоохранение и культура;

– совершенствование системы управления, включая изучение новых методов разработки комплексной политики;

– поддержка усилий МБР и других международных организаций в целях объединения интеллектуальных и финансовых ресурсов в контексте программ сотрудничества, таких, как программа «Информационное развитие (InfoDev)».

Улучшение совместимости, расширение доступа и снижение затрат:

– мобилизация ресурсов в целях улучшения информационной и коммуникационной инфраструктуры с особым вниманием к

«партнерскому» подходу, вовлекающему правительства, международные организации, частный сектор и НО;

– работа над способами снижения затрат по совместимости для развивающихся стран;

– поддержка программ доступа сообществ;

– поощрение исследований и разработок технологий и [компьютерных программных] приложений, учитывающих специфические потребности развивающихся стран;

– улучшение операционной совместимости сетей, услуг и [компьютерных программных] приложений;

– поощрение производства локализованного и содержательного информационного наполнения, включая его развитие на различных языках.

Укрепление человеческого потенциала:

– концентрация внимания на общем образовании, а также расширении возможностей непрерывного обучения с упором на развитие навыков в сфере ИТ;

– содействие формированию круга подготовленных специалистов в сфере ИТ и других соответствующих областях политики, а также по вопросам регулирования;

– разработка инновационных подходов в целях расширения традиционной технической помощи, включая дистанционное обучение и подготовку на местном уровне;

– сетевое объединение государственных учреждений и сообществ, включая школы, научно-исследовательские центры и университеты.

Поощрение участия в сетях глобальной электронной коммерции:

– оценка и увеличение готовности и возможностей по использованию электронной коммерции через оказание консультаций при начале бизнеса в развивающихся странах, а также через мобилизацию ресурсов в целях содействия предпринимательским структурам в использовании ИТ для повышения эффективности их деятельности и расширения доступа к новым рынкам;

– обеспечение того, что «правила игры», как они складываются, соответствовали усилиям в сфере развития и формиро-

ванию способности развивающихся стран играть конструктивную роль в установлении этих правил.

1.5. Основные положения федеральной целевой программы «Электронная Россия (2002–2010 годы)»

1.5.1. Общая характеристика Программы

Федеральная целевая программа «Электронная Россия (2002–2010 годы)» утверждена постановлением Правительства Российской Федерации от 28 января 2002 года № 65. Основными целями Программы являются создание условий для развития демократии, повышение эффективности функционирования экономики, государственного управления и местного самоуправления за счет внедрения и массового распространения информационных и коммуникационных технологий (ИКТ), обеспечения прав на свободный поиск, получение, передачу, производство и распространение информации, расширения подготовки специалистов по ИКТ и квалифицированных пользователей. Программа призвана обеспечить формирование необходимой нормативной базы и развитие соответствующей инфраструктуры, заложить условия для подключения пользователей различного уровня к открытым информационным системам, а также обеспечить взаимодействие органов власти с гражданами и хозяйствующими субъектами на основе широкого внедрения ИКТ.

Нужно особо отметить, что реализация Программы заключается не только в развитии средств телекоммуникаций. Подчеркнем, что один из важнейших ее аспектов – это обеспечение условий для открытого взаимодействия между органами исполнительной власти и обществом. Здесь можно говорить о модернизации государственных структур с помощью внедрения информационных технологий и обеспечения информационной прозрачности и открытости. Таким образом, речь идет об усилиях по созданию нового гражданского общества, отлаживании механизмов эффективного взаимодействия граждан и власти. В этой связи

необходимо отметить и такой аспект, как возможность граждан воспользоваться достижениями новейших технологий и накопленными человечеством информационными ресурсами. Эту возможность должен иметь каждый человек независимо от места проживания, в большом ли городе он живет или в далеком глухом поселке.

При разработке проекта Программы учитывались приоритеты и цели социально-экономического развития Российской Федерации, прогнозы развития общегосударственных потребностей и финансовых ресурсов, результаты анализа экономического и социального состояния страны, внешнеполитические и внешнеэкономические условия, а также международные договоренности.

Цели и задачи Программы определены с учетом Стратегии социально-экономического развития России на период до 2010 года, основных положений Окинавской хартии глобального информационного общества, принятой на совещании Группы восьми 22 июля 2000 года на острове Окинава, Концепции формирования и развития единого информационного пространства России и соответствующих государственных информационных ресурсов, Доктрины информационной безопасности Российской Федерации. Аналогичные программы уже реализуются в США и европейских странах, что, например, позволяет гражданам этих государств добывать из Интернета информацию, связанную с деятельностью государственных органов власти, отправлять по электронной почте налоговые декларации, задавать вопросы и получать квалифицированные ответы от государственных специалистов.

Программа направлена на координацию действий государственных органов власти всех уровней в области развития и массового распространения ИКТ в экономике и государственном управлении, в том числе в рамках других федеральных, региональных и ведомственных программ, в частности, Федеральной целевой программы «Развитие единой информационно-образовательной среды (2001-2005 годы)». В этом аспекте Программа призвана не только дополнить другие программы в части развития инфраструктуры публичных сетей доступа и широкого внедрения ИКТ, но и выполняет ряд более общих, координирующих функций по отношению к другим программам. Так, в рамках Программы определены концептуальные направления

развития ИКТ в стране, включая основные принципы, общие стандарты и типовые решения по реализации различных проектов в области информатизации, финансируемых из федерального бюджета, критерии их эффективности, порядок мониторинга, отчетности и др.

Чтобы реально продвинуться по всем этим позициям, необходимо решить целый ряд вопросов, связанных прежде всего с развитием законодательной и нормативно-правовой базы, поскольку без построения правил, законов, соответствующих положений невозможно создать условия для опережающего развития информационных технологий. В этом плане Программа взаимоувязана с Концепцией развития рынка телекоммуникаций, принятой Правительством Российской Федерации в декабре 2000 года.

Задачи координации деятельности заказчиков и исполнителей программ, содержащих мероприятия по разработке и использованию информационно-коммуникационных технологий в Российской Федерации, решает Межведомственная комиссия, созданная постановлением Правительства Российской Федерации от 8 октября 2002 года № 743. Возглавляют эту комиссию два сопредседателя: Л.Д. Рейман – министр РФ по связи и информатизации и Г.О. Греф – министр экономического развития и торговли РФ. Коллегиальным органом управления реализацией программы является Дирекция Федеральной целевой программы «Электронная Россия (2002-2010 годы)». Главная задача Дирекции – планирование, управление и мониторинг за ходом реализации Программы. Дирекция формируется Минсвязи России, которое на заседании Правительства Российской Федерации 5 июля 2002 года определено государственным заказчиком – координатором Программы.

Все сказанное выше определяет исключительную важность программы «Электронная Россия (2002-2010 годы)» для страны в целом. Успешная реализация Программы обеспечит развитие рынка телекоммуникационных услуг, электроники, технического образования, ускорение документооборота в государственных организациях, сблизит отдаленные регионы страны и центр, а в конечном плане позволит увеличить темпы экономического роста. К сожалению, в настоящее время программа не финансируется должным образом.

1.5.2. Этапы реализации Программы

На первом этапе реализации Программы (2002 год) должны быть сформированы институциональные предпосылки к реализации мероприятий Программы. Это предполагает анализ действующей нормативно-правовой базы с целью выявления ключевых проблем и барьеров в области законодательства, препятствующих широкому внедрению ИКТ, проведение инвентаризации достигнутого уровня информатизации бюджетного и частного секторов экономики, анализ эффективности государственных расходов в сфере информатизации, полномасштабный аудит всех информационных активов и ресурсов федеральных органов государственной власти. В ходе первого этапа необходимо сформировать системы мониторинга:

– мировых тенденций развития ИКТ и уровня распространения информационных технологий в стране;

– эффективности бюджетных расходов в сфере информатизации;

– эффективности использования информационных технологий, информационных ресурсов в органах государственной власти и бюджетном секторе экономики, их технической и телекоммуникационной обеспеченности;

– эффективности действующей нормативно-правовой базы в области регулирования рынка ИКТ и вопросов социально-экономических приложений ИКТ.

Одной из целей первого этапа является формирование системы межведомственной координации деятельности органов государственной власти всех уровней в области развития и массового распространения ИКТ, разработка критериев эффективности государственных расходов этой области и создан механизм, обеспечивающий их достижение. В рамках данного этапа необходимо создать предпосылки для законодательного обеспечения прав граждан на доступ к открытой информации государственных органов власти на основе использования информационных технологий. Необходимо реализовать первые пилотные проекты по переходу к электронному документообороту в государственных и муниципальных органах власти, по развитию инфраструктуры доступа к телекоммуникационным сетям для органов государствен-

ной власти и местного самоуправления, бюджетных и некоммерческих организаций, а также проекты по модернизации системы профессионального образования в области создания и использования ИКТ.

Важной задачей на этом этапе является выработка позиции России по участию в работе различных международных организаций (ВТО, ОЭСР, АТЭС, ЮНКТАД, ЕС и т.д.). В рамках процесса по присоединению к ВТО необходимо провести всестороннюю проработку участия России в соглашениях по товарам информационных технологий, принять решения по обязательствам либерализации рынка телекоммуникаций и по содействию экспорта интеллектуальной продукции.

На втором этапе (2003-2004 годы) на основе проведенных исследований, разработанных концептуальных документов и сформированной законодательной базы необходимо реализовать организационные мероприятия по расширению и развитию проектов по интерактивному взаимодействию органов государственной власти с гражданами и хозяйствующими субъектами; отработать типовые проектные решения, апробировать различные информационные технологии, оценить и открыто обсудить достигнутые результаты. Одновременно продолжится процесс развития и корректировки законодательной базы информационных технологий. Необходимо начать на регулярной основе деятельность по продвижению России в качестве поставщика услуг и решений в области информационных технологий на мировом рынке, создать современную материально-техническую базу для подготовки специалистов по информационным технологиям и их использованию в ведущих учебных заведениях страны, развернуть широкую подготовку таких специалистов.

На этом этапе должна в основном сформироваться единая телекоммуникационная инфраструктура для органов государственной власти и местного самоуправления, бюджетных и некоммерческих организаций, центров общественного доступа к информационным сетям, определиться основная конфигурация «электронного правительства».

На третьем этапе (2005-2010 годы) будут созданы предпосылки для массового распространения информационных технологий в экономике, а также для полной реализации прав граждан

на доступ к информации и экономическую деятельность на основе использования информационных технологий. По результатам предыдущих этапов будет обеспечено комплексное внедрение стандартизированных систем документооборота, повышающих эффективность коммуникации органов государственного управления как на внутри- и межведомственном уровнях, так и с хозяйствующими субъектами и гражданами. На этом этапе будет завершено формирование единой телекоммуникационной инфраструктуры для органов государственной власти и местного самоуправления, бюджетных и некоммерческих организаций, центров общественного доступа к информационным сетям.

В результате осуществления массовой переподготовки кадров по ИКТ, повышения качества высшего и среднего образования, модернизации системы государственного управления на базе внедрения ИКТ, формирования развитой телекоммуникационной инфраструктуры, организации эффективной системы правового регулирования будут созданы предпосылки для активной структурной перестройки экономики.

1.5.3. Основные направления мероприятий по реализации Программы

В Программе предусматривается реализация мероприятий по девяти основным направлениям.

Совершенствование законодательства и системы государственного регулирования в сфере ИКТ. Основными задачами, реализуемыми в рамках данного направления, являются создание правовой базы для решения проблем, связанных с производством и распространением документов в электронной цифровой форме, снижением административных барьеров и ограничений, препятствующих выходу организаций России на рынки ИКТ, обеспечение равных прав на получение информации из всех общедоступных информационных систем, усиление контроля целесообразности любого расширения перечня требований к хозяйствующим субъектам со стороны государственных и местных органов исполнительной власти, применение средств криптографии в сфере гражданско-правовых отношений.

Обеспечение открытости в деятельности органов государственной власти и общедоступности государственных информационных ресурсов, создание условий для эффективного взаимодействия между органами государственной власти и гражданами на основе использования ИКТ. Основными задачами этого направления являются расширение объема информации и перечня информационных услуг, предоставляемых гражданам и хозяйствующим субъектам органами государственной власти и органами местного самоуправления, формирование механизма общественного контроля их деятельности.

Совершенствование деятельности органов государственной власти и органов местного самоуправления на основе использования ИКТ. Основной задачей мероприятий данного направления является повышение эффективности работы органов государственной власти и органов местного самоуправления путем обеспечения совместимости стандартов хранения информации и документооборота, подключения к компьютерным сетям органов государственной власти и органов местного самоуправления, бюджетных учреждений, реализации отраслевых программ информатизации, создания межведомственных и местных информационных систем и баз данных. Использование ИКТ позволит обеспечить реализацию прав граждан России на свободное получение открытой информации из информационных систем, а также на использование других услуг, предоставляемых этими системами.

Совершенствование взаимодействия органов государственной власти и органов местного самоуправления с хозяйствующими субъектами и внедрение ИКТ в реальный сектор экономики. Мероприятия этого направления предусматривают перевод в электронную цифровую форму большей части документооборота, осуществляемого между хозяйствующими субъектами, органами государственной власти и органами местного самоуправления.

Развитие системы подготовки специалистов по ИКТ и квалифицированных пользователей. Мероприятия этого направления нацелены на совершенствование системы подготовки специалистов для работы с современными ИКТ, ее структурное изменение, обеспечение современного материально-технического

оснащения учебного процесса. Мероприятия разработаны с учетом Федеральной целевой программы «Развитие единой образовательной информационной среды (2001-2006 годы)».

Содействие развитию независимых средств массовой информации посредством внедрения ИКТ. Использование ИКТ в средствах массовой информации будет осуществляться на основе конкурса проектов. При принятии решений о выделении средств из федерального бюджета для реализации подобных проектов будут учитываться профессиональный уровень творческих коллективов, наличие обоснованного проекта использования ИКТ и участие редакции в финансировании проекта. Конкурсы предполагается проводить на федеральном и региональном уровнях. При этом будет обеспечено тесное взаимодействие со сложившимися в данной сфере профессиональными объединениями.

Развитие телекоммуникационной инфраструктуры и создание пунктов подключения к открытым информационным системам. Реализация мероприятий этого направления будет обеспечиваться преимущественно путем снижения административных барьеров и снятия ограничений для предпринимательской деятельности, повышения конкуренции и создания благоприятных условий для притока иностранных инвестиций в сферу ИКТ. Планируется также развитие пунктов подключения к общедоступным информационным системам органов государственной власти, бюджетных и некоммерческих организаций за счет средств федерального бюджета.

Разработка и создание системы электронной торговли. Мероприятия этого направления предусматривают создание системы электронной торговли, в том числе для осуществления закупок продукции для федеральных государственных нужд. Такая система существенно повысит эффективность использования средств федерального бюджета и бюджетов субъектов Российской Федерации при осуществлении государственных закупок, а также создаст предпосылки для широкого использования ИКТ в процессе взаимодействия органов государственной власти и хозяйствующих субъектов.

Формирование общественной поддержки выполнения мероприятий Программы. В рамках данного направления планируется проведение научно-практических конференций по про-

блемам развития ИКТ и их использованию в экономике России, организация обсуждения через сеть Интернет стандартов, необходимых для распространения ИКТ, обеспечение широкого информационного сопровождения Программы для привлечения к ней общественного внимания и другие мероприятия.

1.5.4. Ожидаемые результаты реализации Программы

Реализация мероприятий Программы окажет комплексное воздействие на все сферы экономики и общественной жизни. Эффективность программных мероприятий в части совершенствования законодательной базы будет выражаться в росте числа организаций сектора и развитии конкуренции на всех сегментах рынка ИКТ, что приведет к снижению стоимости предоставления услуг доступа к Интернету (в реальном выражении). Обеспечение стимулов к легализации бизнеса в сфере ИКТ позволит заметно сократить долю нелегального рынка программного обеспечения, повысить эффективность разработок в секторе ИКТ и увеличить налоговые поступления в бюджет.

Создание предпосылок для роста как спроса, так и предложения на рынке ИКТ (в том числе государственного спроса в рамках создания «электронного правительства») обеспечит темпы роста отечественного производства для внутреннего потребления и экспорта не менее 15-25% в среднем в год в период до 2005 года. В частности, предполагается рост объемов рынка информационных услуг и программного обеспечения в 2-3 раза к 2005 году и в 5-6 раз к 2010 году.

Доля сектора ИКТ в экономике увеличится в несколько раз и составит к 2010 году не менее 2%. Реализация мероприятий Программы в области подготовки кадров и создание благоприятных законодательных условий внешнеэкономической деятельности компаний сектора ИКТ позволит многократно увеличить объем экспорта из России информационных продуктов и услуг. К 2010 году экспорт этого сегмента сферы ИКТ составит от 1 до 2 млрд. долларов в зависимости от конъюнктуры мирового рынка.

Реализация мероприятий по развитию и распространению ИКТ во всех сферах деятельности обеспечит опережающий рост числа пользователей информационных сетей и объемов передаваемой информации по сравнению с ростом парка компьютеров. Прогнозируется, что количество пользователей Интернета вырастет к 2005 году по сравнению с 2000 годом более чем в 8 раз. К 2010 году около двух третей компьютеров будут иметь доступ к глобальным информационным сетям. Важным условием распространения Интернета является стоимость подключения и пользования. В свою очередь, расширение числа пользователей и объемов передаваемой информации выступает основным фактором снижения издержек провайдеров. Ожидается, что расширение объемов рынка позволит существенно снизить цены за пользование этими услугами к 2005 году на 40% и примерно вдвое к 2010 году. Вместе с тем такое снижение нельзя рассматривать как автоматическое. Эти оценки основаны на предположении о реализации тех пунктов программы, которые направлены на совершенствование регулирования и саморегулирования сектора, проведение эффективной антимонопольной политики.

Быстрое развитие сектора ИКТ, расширение применения современных информационных технологий в других отраслях экономики будет способствовать формированию более прогрессивной структуры экономики, послужит импульсом к развитию отечественных высокотехнологичных производств, создаст принципиально новые возможности для наращивания производства и экспорта отечественной продукции высокой степени переработки. На базе развития «новой экономики», основанной на информационных технологиях, станет возможным изменение тенденций нарастания доли сырьевого сектора в экономике России и, в частности, в экспорте.

Меры Программы по развитию информатизации всех уровней государственного управления обеспечат кардинальное ускорение процессов информационного обмена как внутри общества и бизнеса, так и между гражданами и государством. Следствием этого станет повышение эффективности государственного управления, создание принципиально новых возможностей для мониторинга процессов в экономике и обществе и принятия своевременных решений по регулированию этих про-

цессов. Косвенным индикатором будет служить рост доли населения и организаций, использующих ИКТ во взаимоотношениях с органами управления для получения и передачи информации.

Программа позволит за счет наращивания информационных ресурсов и распространения ИКТ на новые сферы жизнедеятельности создать дополнительные стимулы к применению ИКТ как бизнесом, так и населением. Парк персональных компьютеров, используемых бизнесом, увеличится в 6 раз (используемых населением – в 4 раза) и существенно обновится. Прогнозируется, что примерно каждый второй компьютер будет иметь выход в Интернет.

Внедрение современных информационных технологий в организацию работ министерств и ведомств, а также региональных органов управления позволит сократить издержки на управление, в том числе и за счет высвобождения части технического персонала этих служб. Целевым индикатором информатизации работы органов управления может выступать доля безбумажного документооборота внутри ведомств и между ними. Предполагается довести долю безбумажного документооборота в среднем до 65% внутри ведомств и до 40% в межведомственном обороте.

Интеграция государственных информационных ресурсов в единую систему (в частности, МНС, ГТК и других ведомств) позволит радикально сократить возможности для хозяйственных махинаций, нарушения законов, уклонения от налогов и т. п. Эффект от этой части Программы будет выражаться в повышении собираемости налогов и сокращении потерь от экономических преступлений. Создание единой системы сбора, передачи и обработки информации позволит существенно повысить возможности скоординированных действий силовых структур и будет способствовать повышению безопасности и обороноспособности страны.

Для формирования равных условий комплексного и системного информационного обеспечения процессов развития и внедрения электронной торговли во всех субъектах Российской Федерации Программой предусматриваются мероприятия по созданию базовой основы интегрированной информационной инфраструктуры электронной торговли, а также регионального пилотного

проекта ее полнофункционального сегмента для последующего тиражирования проверенных практикой решений в других регионах страны.

Реализация Программы создаст необходимые и достаточные условия для ускоренной интеграции России в мировую систему коммуникаций и стандартов, будет способствовать расширению присутствия России в глобальной информационной сети, а также спектра направлений и масштабов участия России в международном разделении труда. Индикатором эффективности Программы по этому направлению будут выступать объемы российских информационных ресурсов в сети Интернет, их доля в общих мировых ресурсах, а также объемы внешнеэкономической деятельности в сфере ИКТ. Особенности географического положения России, структуры размещения производства и распределения населения, отставание развития транспортной инфраструктуры определяют особую важность информационных технологий и систем удаленного доступа к информации для обеспечения населения и бизнеса необходимыми консультационными услугами.

Развитие ИКТ потенциально позволит всем гражданам дистанционно получать медицинские, юридические и иные виды консультационных услуг, существенно повысит возможности дистанционного обучения и повышения квалификации. Это явится важным шагом по пути развития демократии и реальному обеспечению равных прав всех граждан в области информации. Индикатором выступают число пользователей Интернета и объемы услуг, предоставляемых с помощью систем удаленного доступа.

На базе развития современных методов информационного обмена между государством и обществом будут созданы принципиально новые возможности для обеспечения информационной открытости и гласности принятия решений, для повышения уровня доверия и взаимодействия между обществом и государством. У граждан России появятся условия для сокращения затрат времени на реализацию своих конституционных прав и обязанностей.

Предполагаемые Программой темпы распространения ИКТ в экономике и обществе резко увеличат потребность в специалистах сектора ИКТ. К 2005 году ежегодная потребность

в специалистах с высшим и средним специальным образованием составит до 100 тыс. в год, а к концу срока действия Программы – более 130 тыс. ежегодно. Мероприятиями Программы предусмотрено обеспечить ежегодные объемы подготовки кадров в области информационных технологий к 2005 году не менее 25 тыс. специалистов с высшим образованием и не менее 60 тыс. со средним специальным и начальным профессиональным образованием. Дальнейшее развитие кадрового потенциала будет определяться потребностями рынка рабочей силы этой квалификации. В рамках реализации данной Программы и программы развития образования будет достигнут уровень компьютеризации (включая доступ к Интернету) в 100% для высших учебных заведений к 2005 году и 100% средних учебных заведений к 2010 году.

Создание условий для ускорения процессов внедрения современных информационных технологий во все сферы общественной жизни и бизнеса позволит России сократить отставание от развитых стран мира, избежать информационной и экономической изоляции от мировой экономики и мирового сообщества, обеспечить динамизм процессов международной интеграции. Решение задач, определенных в Программе, позволит российской отрасли связи и информатизации обеспечить жителей всех регионов России широкополосными стационарными и беспроводными линиями связи. Пользователи персональных компьютеров и мобильных коммуникаторов смогут выходить в Интернет практически из любой точки страны. В результате образование и квалифицированная медицинская помощь станут доступны населению по всей территории России, жители страны будут иметь возможность приобрести либо реализовать товары по приемлемым ценам, найти или предложить на рынке труда свои услуги в любой точке земного шара. Таким образом, реализация Программы позволит обеспечить эффективность государственного управления на всей территории России, повысит конкурентоспособность экономики страны за счет снижения издержек и повышения качества продукции и услуг, обеспечит рост качества жизни населения.

1.6. Основные положения федеральной целевой программы «Развитие единой образовательной информационной среды (2001-2005 годы)»

Программа «Развитие единой образовательной информационной среды (2001-2005 годы)» утверждена постановлением Правительства Российской Федерации от 28 августа 2001 г. N 630.

Государственным заказчиком Программы является Министерство образования Российской Федерации. Основные разработчики Программы – Министерство образования Российской Федерации, Министерство Российской Федерации по связи и информатизации, Министерство экономического развития и торговли Российской Федерации, Министерство финансов Российской Федерации, Министерство промышленности, науки и технологий Российской Федерации, Министерство юстиции Российской Федерации.

Цели Программы – создание и развитие в Российской Федерации единой образовательной информационной среды, обеспечивающей:

– единство образовательного пространства на всей территории страны;

– повышение качества образования во всех регионах России;

– сохранение, развитие и эффективное использование научно-педагогического потенциала страны;

– создание условий для поэтапного перехода к новому уровню образования на основе информационных технологий;

– создание условий для предоставления российских образовательных услуг русскоязычному населению за рубежом.

Задачи Программы:

– формирование информационно-технологической инфраструктуры системы образования, включая:

– создание федеральной системы информационного и научно-методического обеспечения развития образования;

– предоставление образовательным учреждениям средств вычислительной техники, средств доступа к глобальным информа-

ционным ресурсам, общесистемных и прикладных программных средств, технического обслуживания;

– применение новых информационных и телекоммуникационных технологий в учебном процессе, включая:

– создание и использование в учебном процессе современных электронных учебных материалов наряду с традиционными учебными материалами;

– разработку электронных средств информационно-технологической поддержки и развития учебного процесса;

– подготовку педагогических, административных и инженерно-технических кадров образовательных учреждений, способных эффективно использовать в учебном процессе новейшие информационные технологии.

Этапы реализации Программы:

Первый этап – 2001 год. Поставка аппаратно-программного обеспечения в сельские школы, отбор прикладного программного обеспечения для использования в сельских школах в переходный период, организация подготовки учителей сельских школ к работе с информационными технологиями в образовании.

Второй этап – 2002-2003 годы. Разработка стратегии и методологии реализации Программы, организация федеральной системы информационного и научно-методического обеспечения развития образования, обеспечение учебных заведений средствами информатизации и доступа к информационно-образовательным ресурсам, разработка современных электронных учебных материалов и их экспериментальное апробирование, разработка программ, учебных планов и материалов, проведение курсов повышения квалификации и профессиональной переподготовки педагогических, административных и инженерно-технических кадров.

Третий этап – 2004-2005 годы. Завершение поставок средств информатизации в учебные заведения, организация системы технического обслуживания, разработка и тиражирование электронных учебных материалов, повышение квалификации и профессиональная переподготовка педагогических, административных и инженерно-технических кадров, создание системы открытого образования на основе дистанционных технологий обучения.

Основные направления:

1) развитие информационных технологий сферы образования:

– создание основ единой системы информационного и научно-методического обеспечения образования;

– формирование перечня электронных учебных материалов и информационно-технологических средств, необходимых для обеспечения учебного процесса различных уровней образования;

– разработка и тиражирование электронных средств поддержки и развития учебного процесса;

– организация электронных библиотек учебных материалов и обеспечение доступа к ним;

– организация системы открытого образования, включая интерактивные дистанционные технологии обучения учащихся учебных заведений различного уровня;

– формирование концепции информационной безопасности, организация и обеспечение соответствующих образовательных курсов;

– организация сети ресурсных центров;

– разработка нормативных документов по стандартизации в области образования, открытого образования, включая дистанционные технологии обучения, информационные технологии, информационную поддержку образования, телекоммуникационные сети, открытые системы, системы передачи, хранения и обработки данных.

2) повышение квалификации и профессиональная переподготовка педагогических, административных и инженерно-технических кадров:

– формирование программ и разработка методического обеспечения повышения квалификации и профессиональной переподготовки педагогических, административных и инженерно-технических кадров в области новых информационных технологий;

– повышение квалификации и профессиональная переподготовка педагогических, административных и инженерно-технических кадров.

3) оснащение образовательных учреждений средствами информатизации:

– организация конкурсов на лучший проект оснащения общеобразовательных учреждений средствами информатизации;

– оснащение образовательных учреждений средствами вычислительной техники, средствами телекоммуникаций;

– оснащение образовательных учреждений лицензионными и сертифицированными программными продуктами, предоставление услуг по их сопровождению;

– оснащение образовательных учреждений специализированной мебелью для учебных кабинетов и компьютерных классов.

4) организация системы технического обслуживания:

– разработка нормативно-технического и методического обеспечения, организационных форм и принципов управления техническим обслуживанием на отраслевом, региональном и местном уровнях;

– создание материально-технической базы и подготовка кадров для центров технического обслуживания.

Ожидаемые результаты:

1) создание основ единой образовательной информационной среды, обеспечивающей:

– доступ учащихся и преподавателей 50 процентов общеобразовательных и 70 процентов учебных заведений профессионального образования к высококачественным локальным и сетевым образовательным информационным ресурсам, в том числе к системе современных электронных учебных материалов по основным предметам общеобразовательной школы;

– возможность проведения тестирования и оценки качества образования с использованием специализированного программного обеспечения на всей территории Российской Федерации;

– методическую поддержку и возможность непрерывного повышения квалификации преподавателей образовательных учреждений всех уровней;

– подключение вузов к глобальным информационным ресурсам по высокоскоростным каналам;

– переход к системе открытого образования на основе интерактивных дистанционных технологий обучения;

– создание для граждан России с ограниченными возможностями условий, обеспечивающих получение полноценного обра-

зования, необходимой специальной (коррекционной) помощи, а также социальную адаптацию и реабилитацию с помощью образовательных средств;

– поэтапный переход к новой организации российского образования на основе информационных технологий.

2) доведение числа компьютеров в общеобразовательных учреждениях до соотношения – 1 компьютер на 80 учащихся;

3) достижение отвечающего современным требованиям уровня подготовки российских преподавателей в области информационных технологий;

4) повышение качества обучения в образовательных учреждениях, находящихся в удалении от методических центров (сельские школы, школы в закрытых военных городках и др.), путем организации доступа таких учреждений к существующим образовательным ресурсам, рационального использования педагогических кадров высшей квалификации, подготовки специалистов в области новых информационных технологий для этих учреждений;

5) создание сети ресурсных центров, обеспечивающих информационную и научно-методическую поддержку учебного процесса, обслуживание аппаратно-программных средств, оказание консультационных услуг;

6) развитие фундаментальных и прикладных исследований для реализации задачи, формулой которой является «образование через всю жизнь».

Полный текст программы помещен на сайте:

WWW. educom. ru/ru/projects/programs/development/

Контрольные вопросы к главе 1

1. Назовите основные черты информационного общества.
2. Каковы основные задачи по построению информационного общества?
3. В чем заключается роль образовательных учреждений в построении информационного общества?
4. Назовите основные положения «Окинавской хартии глобального информационного общества».
5. Назовите основные цели и этапы реализации ФЦП «Электронная Россия».
6. Назовите основные цели и этапы реализации ФЦП «Развитие единой образовательной информационной среды».

ГЛАВА 2

ОСНОВЫ ТЕОРИИ ГРАФОВ

Введение. Происхождение теории графов

Существует большое количество практических задач, рассмотрение которых сводится к изучению совокупности объектов, существенные свойства которых описываются связями между ними. Например, на карте авиалиний интерес представляет лишь то, между какими городами имеется связь. При изучении электрических цепей на первый план выступает характер соединений различных ее элементов. Органические молекулы образуют структуры, характерными свойствами которых являются связи между атомами. В компьютерных сетях важным является характер связей между узлами. Интерес могут представлять различные экономические связи, связи и отношения между людьми, событиями, состояниями, и вообще, между любыми объектами.

В подобных случаях удобно изображать рассматриваемые объекты точками, называя их в е р ш и н а м и, а связи между ними – линиями (произвольной конфигурации), называя их р е б р а м и. Множество вершин *V,* связи между которыми определены множеством ребер *E,* называют г р а ф о м и обозначают *G(V, E).*

Допустим, пять государств A, B, C, D, E, чтобы договориться о сотрудничестве, послали своих представителей на конференцию. Результатом конференции явилось подписание следующих договоров: между A и C, B и C, A и D, D и B, E и A, B и E. Данной ситуации соответствует граф, имеющий пять вершин и шесть ребер. Примеры геометрической реализации этого графа приведены на рис. 2.1.

Первая работа по графам была выполнена Л. Эйлером в 1736 г. и посвящалась решению знаменитой задачи о кенигсбергских мостах. Идеи, предложенные Эйлером в этой работе, легли в

основу теории уникурсальных графов. Наряду с решением этой задачи, Эйлер получил также ряд результатов, которые легли в

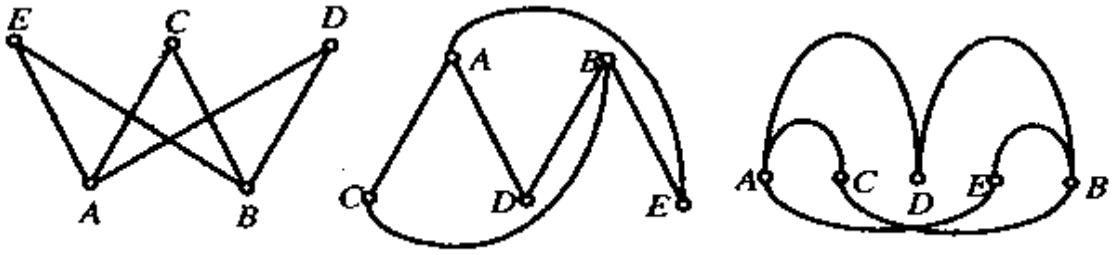


Рис. 2.1. Геометрическая реализация графа

основу проблемы планарности графов. В своих работах Эйлер не использовал термин «граф». Впервые этот термин в 1936 г. ввел Д. Кёниг, назвав графами схемы, состоящие из множества точек и связывающих эти точки отрезков прямых и кривых линий. Теория графов связана с именами многих известных математиков. До конца XIX в. графы применялись лишь при решении некоторых занимательных задач. Однако в начале XX в. теория графов оформилась в виде самостоятельной математической дисциплины. Наряду с многочисленными головоломками и играми на графах появились важные практические приложения графов, многие из которых требовали тонких математических методов. Так, Кирхгоф применил графы для анализа электрических цепей.

В настоящее время теория графов широко применяется в различных областях науки и техники. К числу прикладных задач, решаемых при помощи графов, относятся, например, анализ и синтез цепей и систем, проектирование каналов связи и исследование процессов передачи информации, построение контактных схем и исследование конечных автоматов, сетевое планирование и управление, исследование математических операций, выбор оптимальных потоков в сетях, моделирование нервной системы живых организмов, исследование случайных процессов и многие другие задачи. Теория графов тесно связана с геометрией и топологией, теорией множеств и математической логикой, теорией вероятностей и математической статистикой, теорией матриц и другими разделами математики.

2.1. Неориентированные графы

2.1.1. Абстрактное определение графа

Строгое абстрактное определение графа можно дать в терминах теории множеств. Пусть X – произвольное непустое множество и $X\times X$ – его декартов квадрат, т.е. множество всех упорядоченных пар (x_1, x_2) из элементов множества X. Если множество X – конечно и состоит из n элементов, то его декартов квадрат $X\times X$ содержит n^2 пар, и пары (x_1, x_2) и (x_2, x_1) являются различными элементами множества $X\times X$ при $x_1\neq x_2$. Иногда множество $X\times X$ называют *упорядоченным произведением множества X на себя.*

Рассмотрим теперь так называемое *неупорядоченное произведение X&X множества X на себя,* которое определяется как множество всех неупорядоченных пар из элементов множества X. Элементы из $X\&X$ будем обозначать $(x_1\&x_2)$. Ясно, что во множестве $X\&X$ пары $(x_1\&x_2)$ и $(x_2\&x_1)$ не различимы. Если множество X – конечно и состоит из n элементов, то множество $X\&X$ содержит $n(n+1)/2$ элементов.

Графом $G(V, E, f)$ называется совокупность непустого множества V, изолированного от него произвольного множества E и отображения $f: E\to V\&V$ множества E в $V\&V$, которое каждому элементу из E ставит в соответствие некоторый элемент из $V\&V$. При этом множества V и E называются соответственно множеством вершин и множеством ребер графа $G(V, E, f)$, а отображение f называется отображением инциденции этого графа. Граф называется конечным, если множества V и E содержат конечное число элементов.

Рассмотрим пример. Пусть множество V состоит из 7 точек, $V=\{A,B,C,D,F,H,P\}$, а множество E – из 10 линий $E=\{a,b,c,d,e,f,g,h,p,l\}$ (см. рис. 2.2).

Тогда отображение $f: E\to$V&V, определяемое по закону

$f: a\to(H\&H),\ b\to(P\&F),\ c\to(B\&C),\ d\to(A\&B),\ e\to(P\&F),$

$f\to(B\&H),\ g\to(B\&H),\ h\to(A\&H),\ p\to(A\&B),\ l\to(A\&B)$

является отображением инциденции для графа $G(V, E, f)$. Этот граф имеет 7 вершин и 10 ребер.

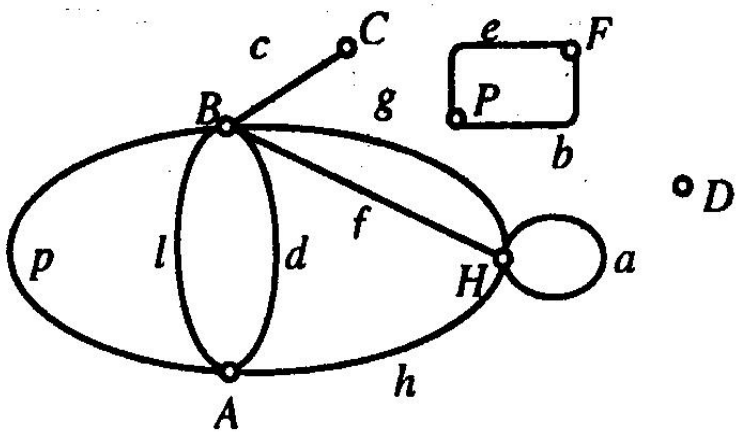


Рис. 2.2. Представление множеств графом

В некоторых случаях, если отображение инциденции явно не задано, для графа *G(V, E, f)* будем использовать обозначение *G(V, E)*. В случаях, когда множества вершин и ребер известны из контекста задачи, граф *G(V, E, f)* будем обозначать через *G*. Заметим, что часто вершины и ребра графа объединяются одним общим термином – э л е м е н т ы г р а ф а .

На первый взгляд может показаться, что данное абстрактное определение графа является сложным и граф достаточно мыслить как совокупность точек и кривых, соединяющих некоторые из этих точек. Но на самом деле это не так. Определение абстрактного графа позволяет избавиться от случайных характеристик его геометрических моделей и сохранить все существенные свойства графа. Кроме того, абстрактное определение позволяет расширить область применения теории графов, так как очень многие реальные объекты можно рассматривать как элементы некоторого графа.

2.1.2. Определение геометрического графа

Для определения геометрического графа напомним два важных понятия из евклидовой геометрии. Пусть *U* – трехмерное евклидово пространство или двумерная евклидова плоскость.

П р о с т о й н е з а м к н у т о й к р и в о й в *U* называется непрерывная самонепересекающаяся кривая, соединяющая две различ-

ные точки в U (т.е. кривая, непрерывно деформируемая в отрезок с концами в этих точках).

Простой замкнутой кривой в U называется непрерывная самонепересекающаяся кривая, концевые точки которой совпадают (т.е. кривая, непрерывно деформируемая в окружность).

Пусть $V=\{A_1, A_2, ...\}$ – любое непустое (конечное или бесконечное) множество точек и $E=\{e_1, e_2, ...\}$ – любое множество простых кривых в U, удовлетворяющих следующим трем условиям:

1. Каждая замкнутая кривая из E содержит ровно одну точку из V;

2. Каждая незамкнутая кривая из E содержит ровно две точки из V, *являющиеся ее граничными точками;*

3. Кривые из E могут пересекаться только в точках из V.

Рассмотрим отображение $f: E \rightarrow V\&V$, определяемое по следующему закону. Каждой незамкнутой кривой поставим в соответствие неупорядоченную пару ее граничных точек (существующих по условию 2), а каждой замкнутой кривой сопоставим пару, состоящую из дважды взятой точки, лежащей на этой кривой (эта точка существует по условию 1). Тогда множество точек V, множество кривых E и отображение f будут удовлетворять абстрактному определению графа.

Граф, состоящий из точек и простых кривых, удовлетворяющих условиям 1 – 3, называется геометрическим графом. Если элементы геометрического графа G (т.е. вершины и ребра) лежат в плоскости (т.е. U – плоскость), то граф G называется плоским графом, если же элементы графа G лежат в пространстве, то граф G называется пространственным.

2.1.3. Инцидентность и смежность элементов графа

Определение инцидентности

Пусть задан абстрактный граф $G(V, E, f)$. Если отображение инциденции f сопоставляет ребру e пару вершин $(x_1\&x_2)$, т.е. $f(e) = (x_1\&x_2)$, то говорят, что ребро e *инцидентно* вершинам x_1 и x_2. Употребляют также следующие выражения: *«ребро e соединяет вершины* x_1 *и* x_2*»* или *«вершины* x_1 *и* x_2 *являются граничными точками ребра e».* Если граничные точки ребра e совпадают, т.е.

f(e) = (x&x), то это ребро называется *петлей* в вершине *x*. Так, например, ребро *a* на рис. 2.2 является петлей в вершине *H*. Из определения графа следует, что каждое ребро, не являющееся петлей, может быть инцидентно ровно двум вершинам, являющимся его граничными точками. Остальные вершины графа считаются *не инцидентными* этому ребру. Точно так же каждая петля графа инцидентна лишь одной своей вершине и не инцидентна остальным вершинам графа. Для геометрического графа ребра, не являющиеся петлями, соответствуют простым незамкнутым кривым, а петли – простым замкнутым кривым.

Определение смежности

Две вершины x_1 и x_2 графа *G(V, E, f)* называются смежными, если в графе существует ребро *e*, инцидентное этим вершинам. Вершина графа смежна самой себе в том и только том случае, если в графе существует петля с вершиной в этой точке. Другими словами, две вершины графа называются смежными, если они инцидентны одному и тому же ребру. Так, например, на рис. 2.2 вершины *A* и *B* являются смежными (их соединяет, в частности, ребро *p*), вершины *C* и *H* – не смежны, а вершина *H* – смежна сама с собой.

Два ребра графа называются смежными, если существует вершина, инцидентная обоим этим ребрам. Так, на рисунке 2.2 ребра *f* и *h* являются смежными, так как они инцидентны вершине *H*.

Два ребра графа называются параллельными, если они инцидентны одним и тем же вершинам, т.е. если они соединяют одну и ту же пару вершин. Так, например, на рис. 2.2 вершинам *A* и *B* инцидентны три параллельных ребра *p, l* и *d*. Ясно, что параллельные ребра являются также и смежными.

Заметим, что отношение инцидентности связывает разнородные элементы графа (вершины и ребра), а отношение смежности – однородные элементы (либо вершины, либо ребра).

2.1.4. Степени вершин графа

Степенью вершины графа называется количество инцидентных ей ребер (для петли степень подсчитывается дважды).

Через *Q(x)* будем обозначать степень вершины *x*. Для графа на рис. 2.2 вершины имеют следующие степени:
Q(A) = 4, Q(B) = 6, Q(C) = 1, Q(D) = 0, Q(F) =Q(P) = 2, Q(H) = 5.

Ясно, что степень любой вершины конечного графа есть целое неотрицательное число. Вообще, определенное нами понятие степени имеет смысл лишь для вершин, инцидентных конечному числу ребер, при этом множество вершин и множество ребер графа могут быть бесконечными. Так, на рис. 2.3 представлен бесконечный граф, все вершины которого имеют степень 4 (кроме первой вершины, имеющей степень 2). Этот граф моделирует так называемые процессы «гибели-размножения».

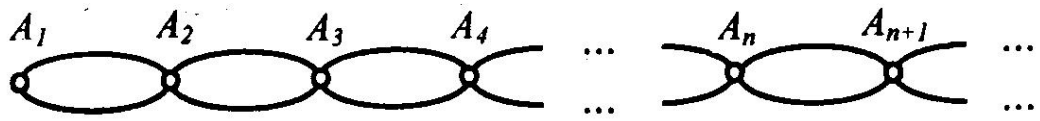


Рис. 2.3. Бесконечный граф

Вершина графа степени 0 называется изолированной. Если степень вершины равна 1, то она называется концевой или висячей вершиной. Вершина, степень которой больше или равна 2, называется промежуточной или проходной. Так, на рис. 2.2 вершина *D* – изолированная, вершина *C* – висячая, а остальные вершины – проходные.

Вершины графа называются четными или нечетными в зависимости от четности их степеней. Так, в графе на рис. 2.3 все вершины – четные. Граф на рис. 2.2 имеет две нечетные вершины (*C* и *H*), а остальные вершины этого графа – четные.

Теорема 1. В любом конечном графе *G(V, E)* количество нечетных вершин – четно.

Действительно, каждое ребро добавляет по единице к степеням своих граничных вершин, а каждая петля добавляет двойку *к* степени своей вершины. Поэтому сумма степеней всех вершин равна удвоенному числу ребер графа:

$$\sum Q(x)=2|E| \quad (1.4.1)$$

Здесь через $|E|$ обозначено число элементов во множестве *E*, т.е. количество ребер графа *G*. Формула 1.4.1 показывает, что

сумма степеней всех вершин графа есть четное число. Поэтому в эту сумму может входить лишь четное количество нечетных слагаемых, т.е. количество нечетных вершин графа *G* есть четное число.

Следствие. Сумма степеней всех вершин конечного графа равна удвоенному числу его ребер.

Граф называется элементарным, если он не содержит петель и параллельных ребер.

Элементарный конечный граф называется полным, если его любая пара различных вершин соединена ребром. Полный граф с *N* вершинами содержит *(N-1)×N/2* ребер.

Граф называется однородным (регулярным) степени k, если все его вершины имеют одинаковую степень *k*. Однородный граф нулевой степени называется нуль-графом или пустым графом. Он не имеет ребер и состоит только из изолированных вершин. Однородный граф третьей степени называется кубическим графом. В силу теоремы 1, любой однородный граф нечетной степени (в частности кубический граф) содержит четное число вершин. Полный граф с *n* вершинами является однородным степени *n-1*, а полный граф с петлями – однородным степени *n+1*.

Задачи и упражнения

1. Докажите, что число перекрестков любого города, в которых встречается нечетное число улиц, четно.

2. У марсиан бывает произвольное число рук. Однажды все марсиане взялись за руки так, что свободных рук не осталось. Докажите, что количество марсиан с нечетным числом рук четно.

3. Докажите, что число зрителей, пришедших на стадион смотреть футбольный матч и имеющих нечетное число знакомых (среди того же множества зрителей) четно.

4. Докажите, что число людей, когда-либо живших на Земле и сделавших нечетное число рукопожатий, четно.

5. В классе 30 человек. Может ли быть так, что 9 из них имеют по 5 друзей каждый, 11 – по 4 друга и 10 – по 3 друга?

6. В офисе 15 телефонов. Можно ли их соединить между собой проводами так, чтобы каждый был соединен с 3 другими?

7. Можно ли нарисовать на плоскости 11 отрезков так, чтобы каждый пересекался ровно с тремя другими?

8. В государстве 100 городов, и из каждого из них выходит по 4 дороги. Сколько всего дорог в государстве?

9. Может ли в государстве, в котором из каждого города выходит ровно по три дороги, быть 100 дорог?

10. На радиостанции каждый радиоузел соединен ровно с 15 другими. Может ли быть число проводов на радиостанции равно 200?

Ответы и пояснения

Во всех задачах нужно смоделировать условия при помощи графов. Задачи 1–7 решаются при помощи теоремы 1, а при решении задач 8–10 нужно использовать следствие из этой теоремы.

Доказательство утверждений в задачах 1–4 дословно повторяет доказательство теоремы 1.

В задачах 5–7 ответ отрицательный, так как ситуации, соответствующие условиям каждой из этих задач, противоречат теореме 1.

7. Нужно рассмотреть граф, вершины которого соответствуют отрезкам, а ребра соединяют вершины, которым соответствуют пересекающиеся отрезки.

8. Рассмотрим граф $G\ (V, E)$, у которого множество вершин V состоит из 100 городов, а множество ребер E состоит из всех дорог государства. По условию задачи каждая вершина этого графа имеет степень 4. Применяя формулу (1.4.1), получим, что $4\times100 = 2\times|E|$. Следовательно, количество дорог $|E|$ равно 200.

9. Моделируя условие задачи так же, как в задаче 8, и применяя следствие из теоремы 1, получим: $3\times|V|=2\times100$. Так как количество вершин $|V|$ должно быть натуральным числом, то ответ на вопрос задачи – отрицательный.

10. Ответ к задаче – отрицательный. Ее решение аналогично решению задачи 9.

2.1.5. Изоморфизм графов

Два графа G и G_1 называются изоморфными (или равными), если между их однотипными элементами можно устано-

вить взаимно-однозначные соответствия, сохраняющие отношение инциденции.

Пример. Рассмотрим два графа G и G_1. изображенные на рис. 2.4.

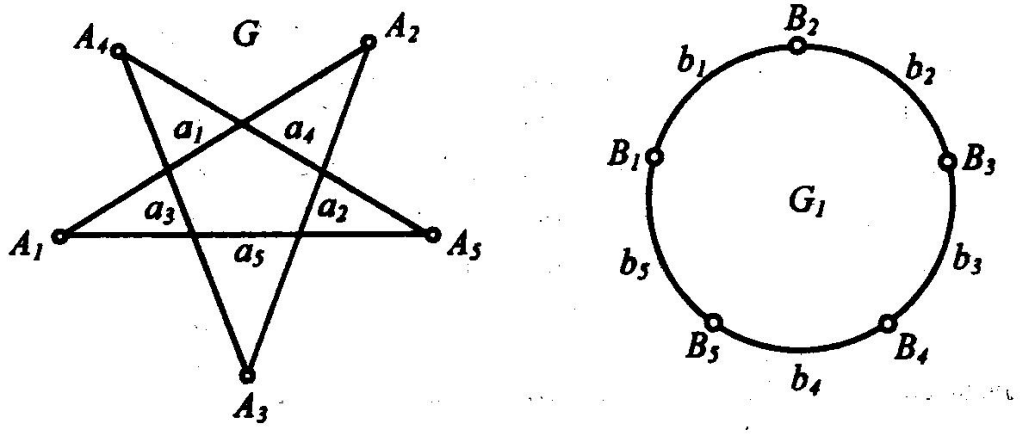


Рис. 2.4. Изоморфные графы

Граф G имеет множество вершин $V=\{A_i\}$, i = 1,2,3,4,5 и множество ребер $E = \{a_i\}$ i=1,2,3,4,5, а граф G_1 состоит из множества вершин $V_1=\{B_i\}$ i=1,2,3,4,5 и множества ребер $E_1=\{b_i\}$ i=1,2,3,4,5. Определим взаимно-однозначное соответствие I между элементами этих графов при помощи пары отображений $I_1:V\rightarrow V_1$, и $I_2:E\rightarrow E_1$, заданных по формулам:

$$I_1(A_i)=B_i\,;\quad I_2(a_i)=b_i$$

Легко видеть, что две вершины графа G соединены ребром тогда и только тогда, когда соответствующие вершины графа G_1 соединены соответствующим ребром. Поэтому построенное взаимно однозначное соответствие $I=(I_1;I_2)$ между элементами графов G и G_1 сохраняет отношение инциденции. Таким образом, можно утверждать, что графы G и G_1 изоморфны.

Описанное в примере взаимно однозначное соответствие $I=(I_1;I_2)$, состоящее из пары отображений I_1 и I_2 и обеспечивающее изоморфизм графов, называется отображением изоморфизма G на G_1. Таким образом, граф G изоморфен графу G_1 тогда и только тогда, когда существует отображение изоморфизма G на G_1. Для того чтобы доказать, что некоторые графы G и G_1 изоморфны, нужно построить конкретное отображение изоморфизма (как в приведенном примере).

Из определения изоморфизма следует, что изоморфные графы имеют одинаковое количество элементов. Вершины, соответствующие при изоморфизме, имеют одинаковую степень. При отображении изоморфизма петли переходят в петли, а параллельные ребра – в параллельные ребра. Вообще изоморфные графы имеют одинаковые комбинаторные свойства и, с точки зрения теории графов, неразличимы. В частности, изоморфизм графов сохраняет смежность вершин и смежность ребер.

Рассмотренное понятие важно в теории информационных сетей. Граф G можно рассматривать как топологию компьютерной сети с устройствами (узлами) в вершинах A_1, A_2, A_3, A_4, A_5, связанными отрезками линий связи a_1, a_2, a_3, a_4, a_5. На первый взгляд каждый узел сети связан с соседними, образуя топологию типа звезда. Граф G_1 наглядно показывает, что все узлы сети образуют топологию логического кольца.

2.1.6. Части графа

Пусть задан некоторый конечный граф $G(V, E, f)$. Существует ряд операций, называемых операциями разборки графа, позволяющих из исходного графа получать новые графы, множества вершин которых являются подмножествами множества V, а множества ребер – подмножествами множества E. При этих операциях должно сохраняться отношение инцидентности, имеющее место для исходного графа G, при выполнении разумного требования о том, что множество вершин графа G_1 должно включать все граничные точки множества его ребер. Существует два основных вида операций разборки графа G:

1) удаление ребра между двумя вершинами графа G с сохранением граничных вершин;

2) удаление вершины графа G вместе со всеми ей инцидентными ребрами.

Частным случаем второй операции разборки является операция

2 а) удаление изолированной вершины графа G.

Ясно, что после применения конечного числа операций разборки этих двух видов получится новый граф $G_1(V_1, E_1, f_1)$, не изоморфный исходному графу $G(V, E, f)$.

Граф G_1, полученный из графа G при помощи конечного числа операций разборки, называется частью графа G. В теории графов представляют интерес два наиболее важных вида частей графа – подграф и суграф. Подграфом графа G называется такая его часть G_1, которая получается из графа G при помощи конечного числа операций разборки вида 2, т.е. – при помощи удаления конечного числа вершин вместе со всеми примыкающими к ним ребрами. Граф G по отношению к своему подграфу G_1 называется надграфом.

Суграфом графа G называется такая его часть G_1, которая получается из графа G при помощи конечного числа операций разборки вида 1, т.е. – при помощи удаления конечного числа ребер (с сохранением вершин). Граф G по отношению к своему суграфу G_1 называется сверхграфом. Граф G по отношению к произвольной своей части G_1 называется объемлющим графом.

Пример. Пусть $G(V, E)$ – это граф автомобильных дорог некоторого государства. Здесь V – множество всех городов этого государства, а E – совокупность всех дорог между городами. Если удалить из графа G все второстепенные дороги, то получим граф главных дорог государства, который является суграфом графа G. Рассмотрим теперь некоторую губернию этого государства. Удалим из графа G все города, не находящиеся на территории этой губернии, вместе со всеми примыкающими к ним дорогами. В результате получим граф автомобильных дорог этой губернии, являющийся подграфом графа G.

Упражнение

Докажите, что графы G_1, G_2 и G_3 являются частями графа G (см. рис. 2.5). Какие из этих графов являются подграфами и какие – суграфами объемлющего графа G? Указать процессы разборки графа G, приводящие к графам G_1, G_2 и G_3.

Ответы и пояснения

1. Граф G_1 может быть получен из графа G только при помощи удаления ребер (т.е. с использованием операции разборки вида 1). Эта операция применяется 10 раз при удалении следующих ребер: $A_1\&A_1$, $A_2\&A_2$, $A_3\&A_3$, $A_4\&A_4$, $A_5\&A_5$, $A_1\&A_2$, $A_2\&A_3$, $A_3\&A_4$, $A_4\&A_5$, $A_5\&A_1$. Следовательно, G_1 является суграфом графа G (а,

следовательно, – и частью этого графа). Граф G_2 может быть получен из графа G, например, при помощи следующих операций разборки:

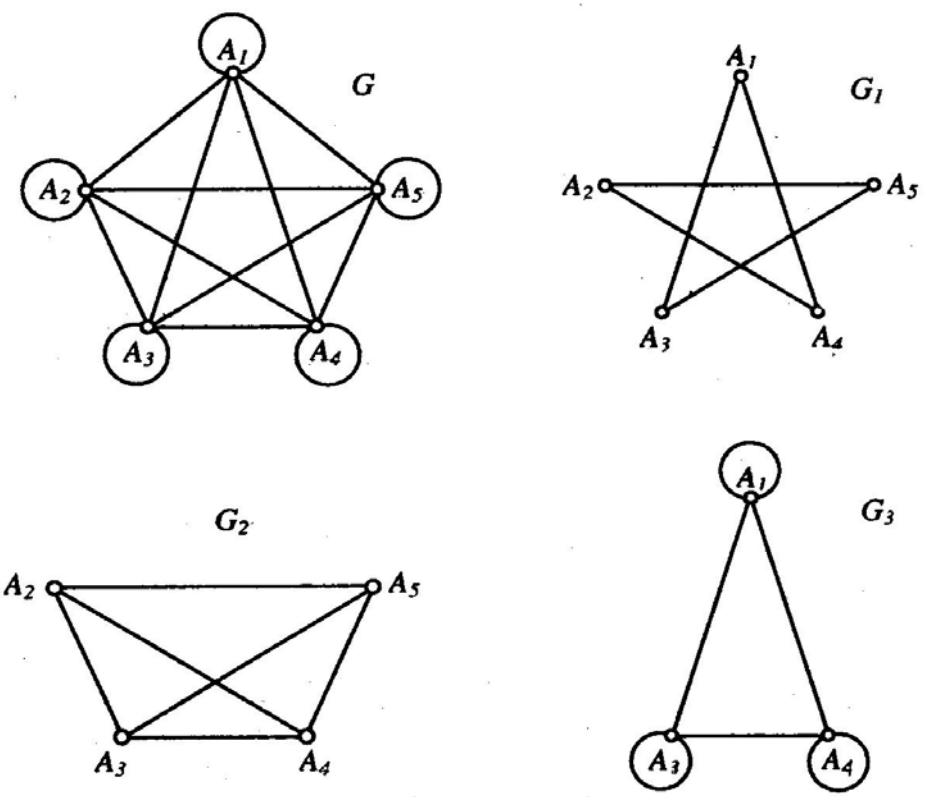


Рис. 2.5. Операции разборки графа

– удаление всех петель (пятикратное применение операции разборки вида 1);

– удаление вершины A_1 вместе со всеми ей инцидентными ребрами (операция разборки вида 2).

Таким образом, граф G_2 является частью графа G.

Граф G_3 может быть получен из графа G при помощи двукратного применения операции разборки вида 2 (удаление вершин A_2 и A_5 вместе со всеми инцидентными им ребрами). Следовательно, G_3 – подграф графа G.

Заметим, что G – это полный граф с петлями, содержащий 5 вершин; G_1 – граф, изоморфный правильному пятиугольнику; G_2 – полный граф с 4 вершинами; G_3 – полный граф с петлями, содержащий 3 вершины.

П о п о л н е н и е м элементарного графа G называется его сверхграф G_1, являющийся полным графом. Граф G является су-

графом своего пополнения G_1 и получается из последнего при помощи операции удаления ребер. Переход от графа G к его пополнению можно осуществить при помощи обратной операции, называемой операцией добавления ребер. Каждая такая операция увеличивает количество ребер графа на единицу, не меняя числа вершин графа. Разность между количествами ребер графов G_1 и G называется степенью неполноты графа G.

Рис. 2.6. Пополнение графа

Пример. На рис. 2.6 представлен элементарный граф G и его пополнение G_1. Добавляемые ребра изображены пунктиром, их количество равно степени неполноты графа G.

2.1.7. Непрерывные последовательности ребер графа

Пусть задан некоторый граф G. Каждое ребро этого графа можно интерпретировать как связующее звено между двумя смежными вершинами. Если зафиксировать некоторую вершину графа и последовательно переходить по связующим ребрам из вершины в вершину, то по прошествию конечного числа таких переходов можно перейти в другую вершину или вернуться в исходную. В геометрическом графе описанный процесс интерпретируется как непрерывное движение по последовательности простых кривых от одной вершины *к* другой. Опишем наиболее важные непрерывные последовательности ребер графа.

Маршруты

Пусть граф $G\ (V, E, f)$ имеет не более чем счетные множества вершин $V=\{A_1, A_2,..., A_n\}$ и ребер $E=\{a_1, a_2,..., a_n\}$. Конечная последовательность ребер графа $a_1, a_2,..., a_k$ (не обязательно различных) называется маршрутом длины k, если граничные точки двух соседних ребер этой последовательности совпадают. Первая и последняя вершины называются соответственно начальной и конечной вершиной маршрута. Остальные вершины последовательности называются промежуточными вершинами этого маршрута. Также говорят, что *маршрут* $a_1, a_2,..., a_k$ *соединяет вершины* A_1, *и* A_k.

Заметим, что любое ребро (или петля) является маршрутом длины 1, соединяющим свои граничные вершины. Маршрут называется замкнутым, если его начальная и конечная вершины совпадают. В противном случае маршрут называется незамкнутым.

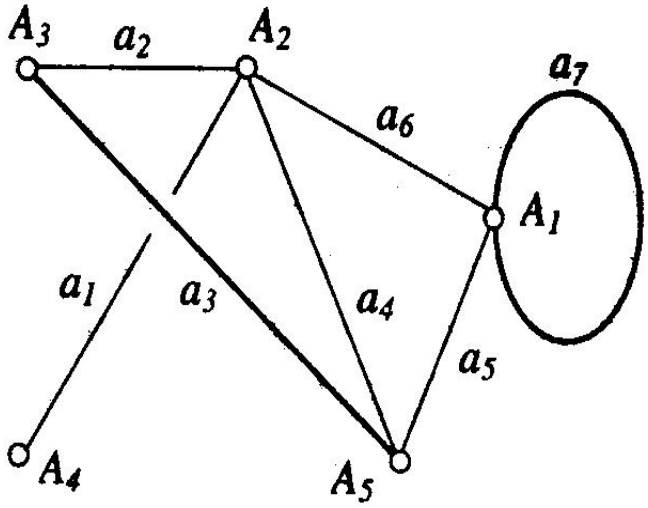


Рис. 2.7. Маршруты

Пример. На рис. 2.7 последовательность ребер a_1,a_4,a_5,a_6,a_2,a_2 образует незамкнутый маршрут длины 6, соединяющий вершины A_4 и A_2, а последовательность ребер a_7,a_6,a_4,a_5,a_7 определяет незамкнутый маршрут длины 5, который начинается и заканчивается в вершине A_1.

Цепи и циклы

Цепью называется незамкнутый маршрут, состоящий из последовательности различных ребер. Замкнутый маршрут, состоящий из последовательности различных ребер, называется циклом. Так, маршрут a_1,a_4,a_5,a_6,a_2 на рис. 2.7 является цепью, а замкнутый маршрут a_7,a_6,a_4,a_5 представляет собой цикл. Заметим, что маршрут a_1,a_4,a_5,a_6,a_2,a_2 не является цепью, а замкнутый маршрут a_7,a_6,a_4,a_5,a_7 не является циклом.

Частным случаем цепей являются такие маршруты, которые не проходят дважды через одну и ту же вершину. Такие маршруты называются простыми цепями. Ясно, что если маршрут не проходит дважды через одну и ту же вершину, то он не проходит дважды и через одно и то же ребро.

Простым циклом называется маршрут, в котором начальная и конечная вершины совпадают, а все остальные вершины различны.

2.1.8. Связность графов

Граф $G(V, E)$ называется связным, если для любой пары различных вершин этого графа существует цепь, соединяющая эти вершины. Если для графа $G(V, E)$ можно указать пару различных вершин, которые не соединяются цепью (простой цепью), то граф называется несвязным.

Граф называется k-связным, если его любая пара различных вершин A и B соединяется по меньшей мере k простыми цепями, не имеющими общих вершин, кроме A и B.

2.1.9. Древовидные графы

Различные определения деревьев

Определение 1. Деревом называется конечный связный граф без циклов.

Из определения 1 следует, что если граф является деревом, то любая пара его вершин соединяется единственной цепью. Очевидно, что это свойство деревьев является не только необходимым, но и достаточным, так как если любая пара вершин графа

соединяется единственной цепью, то этот граф связный и не имеет циклов. В силу этого можно дать следующее определение.

Определение 2. Деревом называется конечный граф, любые две вершины которого соединяются единственной цепью.

Определение 3. Деревом называется конечный связный граф, для которого количество ребер на единицу меньше количества вершин.

Пример дерева представлен на рис. 2.8. В качестве несложного упражнения можно убедиться в корректности еще одного определения.

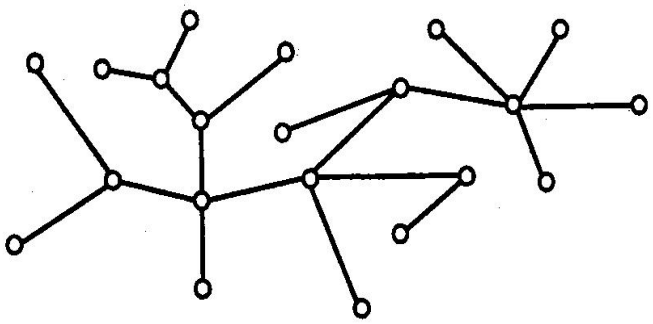


Рис. 2.8. Древовидный граф

Определение 4. Деревом называется конечный граф, обладающий свойством: граф не содержит циклов, но добавление ребра между любыми не смежными вершинами приводит к появлению цикла.

2.1.10. Уникурсальные графы

Задача Эйлера о кенигсбергских мостах

В 1736 г. Эйлером была выполнена работа, в которой содержалось решение знаменитой задачи о кенигсбергских мостах.

Из письма Л. Эйлера от 13 марта 1736 г.: *«Мне была предложена задача об острове, расположенном в городе Кенигсберге и окруженном рекой, через которую перекинуто 7 мостов. Спрашивается, может ли кто-нибудь непрерывно обойти их, проходя только однажды через каждый мост. И тут же мне было сообщено, что никто еще до сих пор не смог это проделать, но никто и не доказал, что это невозможно. Вопрос этот, хотя и банальный, показался мне достойным внимания тем, что для его*

решения недостаточны ни геометрия, ни алгебра, ни комбинаторное искусство. После долгих размышлений я нашел легкое правило, основанное на вполне убедительном доказательстве, при помощи которого можно во всех задачах такого рода тотчас же определить, может ли быть совершен такой обход через какое угодно число и как угодно расположенных мостов или не может».

Идеи Эйлера, использованные им при решении этой задачи, явились фундаментом теории, впоследствии названной теорией графов. Суть этой задачи заключается в следующем: можно ли пройти по всем мостам, изображенным на рис. 2.9, так, чтобы на каждом из них побывать лишь один раз и вернуться к тому месту, откуда началась прогулка?

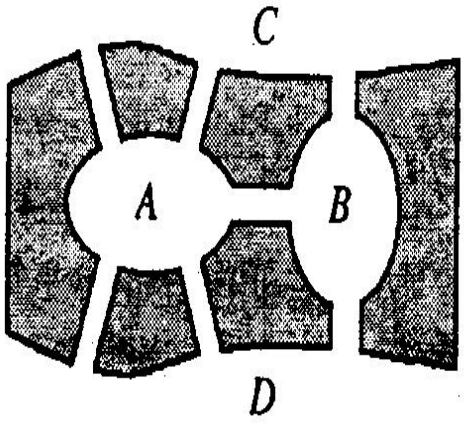


Рис. 2.9. Схема мостов

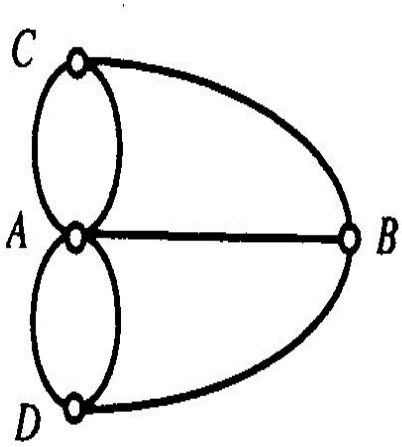


Рис. 2.10. Граф схемы

Ясно, что по условию задачи не имеет значения, как проходит путь по частям суши *A, B, C, D,* поэтому их можно изобразить точками. А так как связи между этими частями суши осуществляются только через семь мостов, то каждый из мостов можно изобразить линией, соединяющей соответствующие вершины. В результате получается граф, изображенный на рис. 2.10. Если бы существовал маршрут движения, удовлетворяющий условию задачи, то этот граф было бы возможно нарисовать **«одним росчерком»** (т.е. – без отрыва карандаша от бумаги, проводя по каждому ребру только один раз), начиная и заканчивая рисование в одной точке. Эйлером было доказано, что это невозможно. Возникает вопрос: будет ли задача о кенигсбергских мостах иметь решение, если отказаться от того, чтобы маршрут движения на-

чинался и заканчивался в одной точке? В этом случае мы вновь приходим к задаче об изображении графа одним росчерком. Как будет показано ниже, граф на рис. 2.10 одним росчерком изобразить невозможно.

Определение уникурсальных графов

Граф называется уникурсальным графом (или эйлеровой линией), если все его ребра можно включить либо в простой цикл, либо в простую цепь. Другими словами, граф называется уникурсальным, если он рисуется одним росчерком. Если все ребра графа можно включить в простой цикл, то такой уникурсальный граф называется эйлеровым циклом. Уникурсальный граф, не являющийся эйлеровым циклом, называется эйлеровой цепью. При изображении одним росчерком эйлеров цикл начинается и заканчивается в одной точке, а эйлерова цепь – в различных точках.

Чтобы привести примеры уникурсальных графов, достаточно на листе бумаги отметить произвольную точку A и, не отрывая карандаша от бумаги, провести произвольную самопересекающуюся кривую так, чтобы она начиналась в этой точке, не имела отрезков самопересечения и заканчивалась в некоторой точке R (см. рис. 2.11).

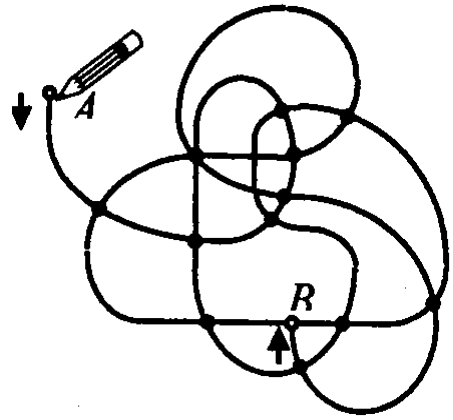


Рис. 2.11. Эйлерова цепь

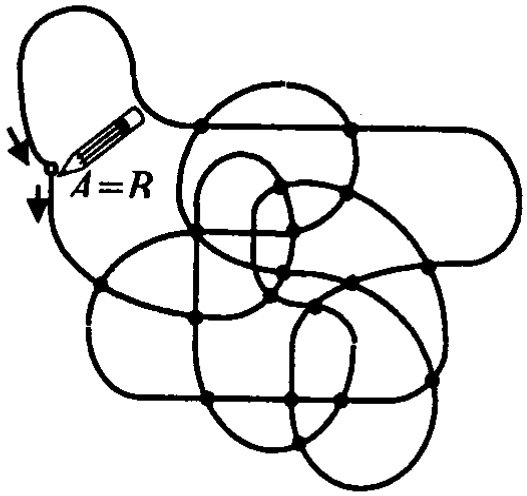


Рис. 2.12. Эйлеров цикл

Ясно, что граф, вершинами которого являются точки самопересечения кривой вместе с точками A и R, является уникурсаль-

ным. При этом если точки A и R совпадают, то мы получим эйлеров цикл (см. рис. 2.12), если же точки A и R различны, то мы получим эйлерову цепь (см. рис. 2.11).

Упражнение. На рис. 2.13 приведено 4 примера эйлеровых циклов. Попробуйте изобразить эти графы одним росчерком.

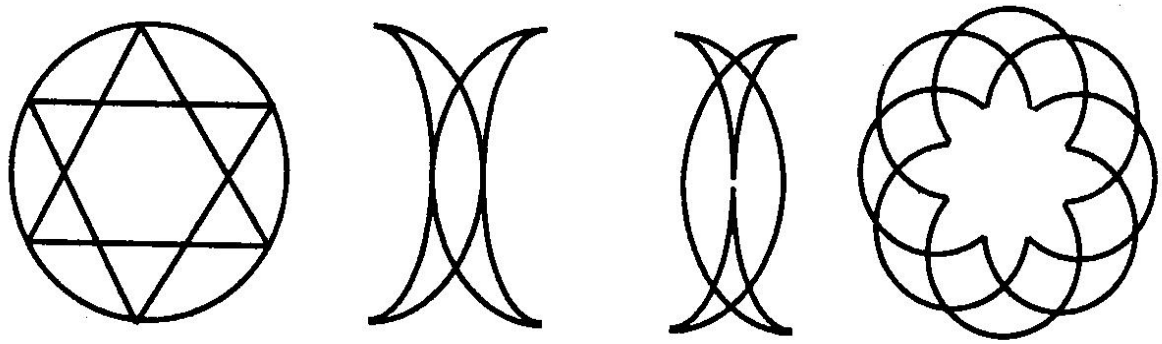


Рис. 2.13. Примеры Эйлеровых циклов

Признаки уникурсальных графов

Очевидно, что связность графа является необходимым условием его уникурсальности. К сожалению, для изображения графа одним росчерком одной его связности недостаточно. Для того чтобы найти признаки уникурсальности связных графов, понаблюдаем за свойствами эйлеровых линий. Если подсчитать степени всех вершин графов, полученных одним росчерком (см. рис. 2.11 – 2.13), то можно заметить, что все эйлеровы циклы имеют только четные вершины (см. рис. 2.12 и 2.13), а все эйлеровы цепи (см. рис. 2.11), имеют ровно две нечетные вершины, а все их остальные вершины – четны. Приведем без доказательства несколько теорем.

Лемма. Если связный граф имеет более двух нечетных вершин, то он не уникурсален. Действительно, если граф рисуется одним росчерком, то его нечетная вершина может служить либо началом, либо концом пути.

Теорема 1. Связный граф является эйлеровым циклом тогда и только тогда, когда он имеет только четные вершины. При этом начало и конец уникурсального пути совпадают и могут находиться в любой вершине графа.

Теорема 2. Связный граф является эйлеровой цепью тогда и только тогда, когда он имеет ровно две нечетные вершины, а остальные вершины этого графа четны. При этом начало и конец уникурсального пути находятся в нечетных вершинах.

Граф, все вершины которого четны (и, значит, существует эйлеров цикл), называют эйлеровым графом. Обратившись к графу в задаче о кенигсбергских мостах, замечаем, что все четыре его вершины являются нечетными – в каждой из вершин *B, C, D* сходятся по три ребра, а в вершине А – пять ребер. Значит, этот граф не эйлеров. Найти эйлеров цикл (разумеется, после того, как вы убедились, что заданный граф эйлеров (все вершины четны)) совсем не трудно: существует универсальный и достаточно простой алгоритм, при помощи которого задача построения эйлерова цикла всегда разрешима.

Покажем эффективность этого алгоритма на конкретном примере (см. рис. 2.14).

Пример 1. Выйдя из вершины *A* и не пытаясь еще раз пройти по уже пройденному ребру, мы неизбежно вернемся в вершину *A*. Это объясняется тем, что, входя в любую вершину графа (кроме, быть может, вершины *A*), мы всегда имеем возможность выйти из нее (напомним, что в каждой вершине графа сходится четное число ребер). Следовательно, неутомимо продолжая перемещение, мы неизбежно вернемся в вершину *A*, а вернувшись, окажемся перед двумя возможными ситуациями: 1) в построенный нами цикл входят все ребра графа, 2) остались еще не пройденные ребра.

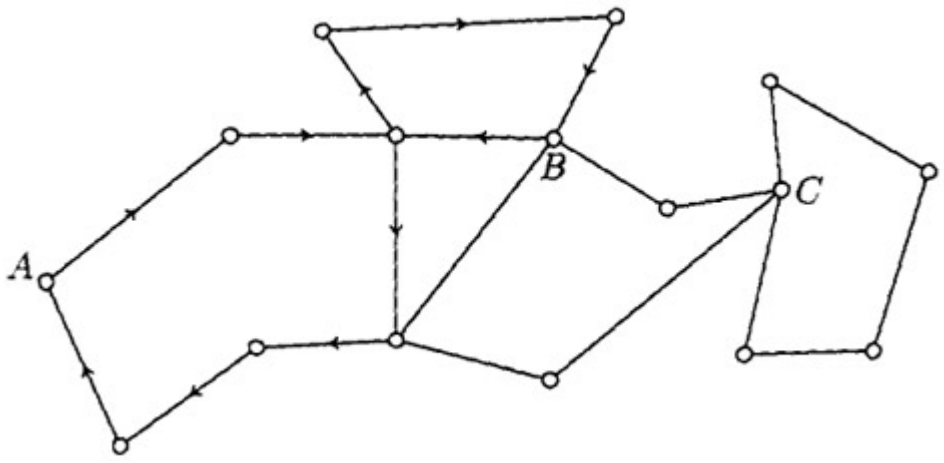


Рис. 2.14. Эйлеров цикл

Первый случай не так интересен: если в построенный цикл входят все ребра, то поставленная задача решена. Что же касается второго случая, то здесь в полученном нами цикле (обозначим его через ***A***) обязательно есть вершина, из которой выходит еще не пройденное нами ребро. Пусть это вершина *B*. Об этой вершине можно сказать даже больше: число выходящих из нее ребер, не принадлежащих построенному циклу ***A***, обязательно четно. И мы строим новую цепь из вершины *B,* привлекая только ранее не пройденные ребра. Ясно, что в результате мы вернемся в вершину *B* и получится новый цикл – ***B*** (рис. 2.15).

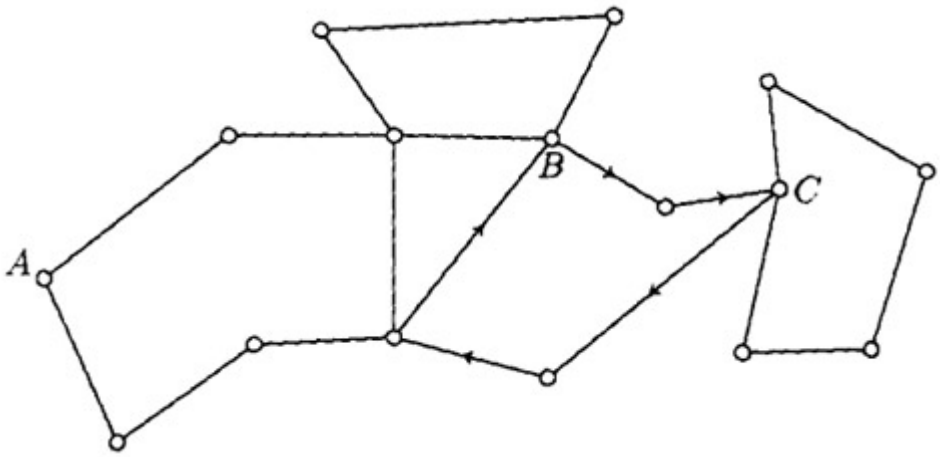


Рис. 2.15. Эйлеров цикл

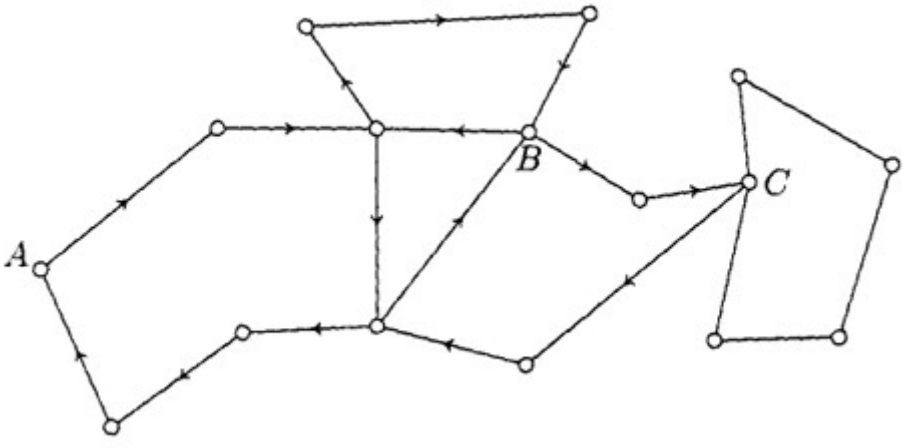


Рис. 2.16. Эйлеров цикл

Теперь легко получить цикл, начинающийся в вершине *A* и больший построенного ранее цикла *A*. Для этого мы сначала перемещаемся по маршруту ***A*** от вершины *A* до вершины *B,* затем

проходим по циклу ***B*** и, вернувшись в вершину *B*, завершаем перемещение в вершину *A* по оставшейся части цикла ***A*** (рис. 2.16).

Если мы и на этот раз не прошли по всем ребрам графа, то, выбрав вершину цикла, построенного по циклам ***A*** и ***B***, из которой исходят ребра, не входящие в этот цикл, расширяем его описанным выше способом. Повторяя в случае необходимости подобные рассуждения достаточное число раз, мы всегда сможем построить эйлеров цикл за конечное число шагов.

Пример 2. Устроители больших художественных выставок часто вынуждены решать одну и ту же задачу: как организовать осмотр, чтобы дать возможность в отведенное время ознакомиться со всей экспозицией наибольшему числу желающих.

Ясно, что для этого нужно расставить указатели таким образом, чтобы, перемещаясь в соответствии с предложенными в них рекомендациями, любой посетитель мог побывать у каждой картины ровно по одному разу. Если вход и выход совпадают, то разместить экспонаты следует так, чтобы схема экспозиции была эйлеровым графом. Что же касается указателей, то они должны 1) быть снабжены порядковыми номерами и 2) описывать эйлеров цикл. Если же вход и выход разные, то схема размещения экспонатов должна быть графом, у которого лишь две вершины, соответствующие входу и выходу, являются нечетными.

Эйлеровы циклы характеризуются тем свойством, что они проходят через каждое ребро графа в точности по одному разу. Аналогичным образом, но только по отношению к вершинам определяются для конечных связных графов так называемые *гамильтоновы циклы*: цикл называется гамильтоновым, если он проходит через каждую вершину графа ровно по одному разу.

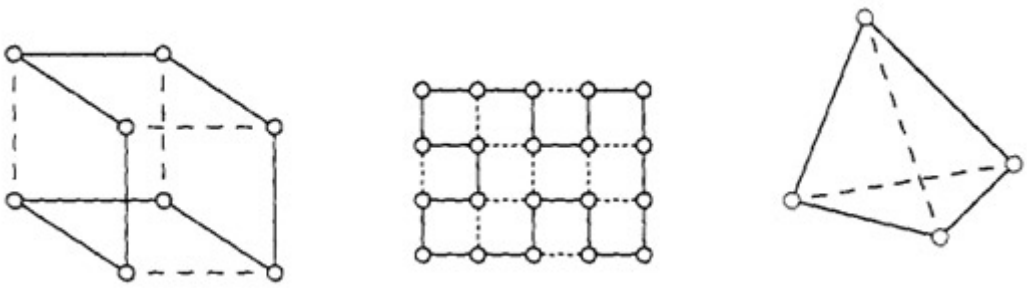


Рис. 2.17. Гамильтоновы циклы

На рис. 2.17 приведены гамильтоновы циклы для нескольких простых графов. Между эйлеровым и гамильтоновым циклами легко просматривается довольно прозрачная аналогия: первый проходит ровно один раз по каждому ребру, второй – ровно один раз через каждую вершину.

На первый взгляд естественно ожидать того, что задача проверки, допускает ли данный граф гамильтонов цикл, должна быть по сложности сравнима с аналогичной задачей для эйлерова цикла (где достаточно подсчитать четность каждой вершины). Однако на деле все обстоит значительно сложнее: несмотря на практическую важность этой проблемы, до сих пор не найдено ни общего критерия, позволяющего устанавливать, является ли заданный граф гамильтоновым, ни универсального эффективного алгоритма построения гамильтонова цикла.

Одной из практических задач, связанных с построением гамильтонова цикла, является задача о коммивояжере, в которой нужно найти кратчайший путь, проходящий через заданные пункты (все расстояния известны) и возвращающийся в исходный пункт.

Так как число пунктов конечно, то в принципе задача может быть решена простым перебором.

Пример 3. Торговец, живущий в городе A, намерен посетить города B, C и D, расстояния между которыми ему известны: $AB = 11$, $AC = 13$, $AD = 17$, $BC = 6$, $BD = 9$, $CD = 10$ (рис. 2.18). Требуется указать кратчайший циклический маршрут из города A, проходящий через три других города.

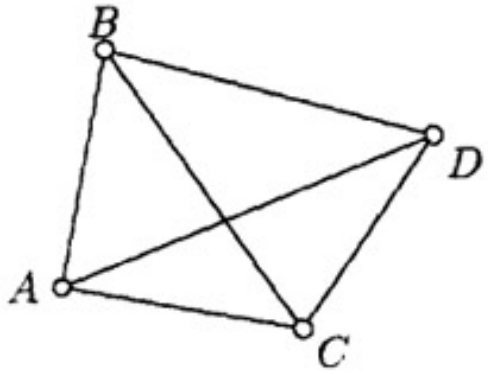


Рис. 2.18. Граф соединения городов

Возможных циклических маршрутов шесть: *ABCDA, ACDBA, ADBCA, ACBDA, ABDCA, ADCBA*. Однако для решения задачи достаточно сравнить длины только первых трех: *ABCDA, ACDBA, ADBCA.*

Эти длины равны соответственно:

11+6+10+17=44, 13+10+9+11=43, 17+9+6+13=45.

Тем самым, кратчайшим является любой из маршрутов длиной 43 - *ACDBA* или *ABDCA.*

2.2. Ориентированные графы. Основные понятия и свойства

Как было отмечено ранее, при помощи неориентированных графов моделируются различные задачи, в которых изучаются совокупности объектов, между парами которых установлены связи. Сопоставив каждому объекту вершину, а каждой связи ребро, мы приходим к некоторому графу. Однако в ряде задач связь между парами объектов может носить направленный характер, и существование связи между объектами *A* и *B,* вообще говоря, не означает существование связи между *B* и *A*. В подобных случаях, чтобы подчеркнуть направленный характер связей, ребра в соответствующем графе удобно наделять стрелками. Граф, на ребрах которого расставлены стрелки, называется ориентированным графом. Остановимся на изучении ориентированных графов.

Орграф и его элементы

Абстрактное определение ориентированного графа (орграфа) формулируется аналогично определению обычного графа, данному в пункте 2.1.

Ориентированным графом или орграфом *G(V, E, f)* называется совокупность непустого множества *V*, изолированного от него произвольного множества *E* и отображения *f: E→V×V* множества *E* в *V×V*, которое каждому элементу из *E* ставит в соответствие некоторый элемент из *V×V*, т.е. упорядоченную пару элементов из *V*. При этом множества *V* и *E* называются соответственно множеством вершин и множеством дуг

орграфа $G(V, E, f)$, а отображение f называется отображением инцидентции этого орграфа.

Если $f(e) = (A, B)$, то вершина A называется началом дуги e, а вершина B называется концом этой дуги. Также говорят, что дуга e идет от вершины A к вершине B.

Отличие орграфа от неориентированного графа состоит в том, что если $f(e)=(A, B)$, то отображение инциденции f указывает не просто пару вершин A и B, соединенных e (как это было в случае неориентированного графа), а еще к тому же сохраняет различие между A и B, так как пары (A, B) и (B, A) являются различными элементами множества $V \times V$.

Элементами орграфа являются вершины и дуги. Орграф называется конечным, если множества вершин V и ребер E содержат конечное число элементов.

Чтобы обеспечить наглядность графического изображения орграфа, его дуги (т.е. кривые, соединяющие соответственные вершины) снабжаются стрелками. На рис. 2.19 приведен пример орграфа $G(V, E, f)$. Этот граф имеет 5 вершин и 12 ребер: $V=\{A,B,C,D,P\}$, $E=\{a_1,a_2,\ldots,a_{12}\}$. Отображение инциденции f определяется следующим образом:

f: $a_1 \rightarrow (A, B)$; $a_2 \rightarrow (A, B)$; $a_3 \rightarrow (B, C)$; $a_4 \rightarrow (B, P)$; $a_5 \rightarrow (P, C)$; $a_6 \rightarrow (D, C)$; $a7 \rightarrow (D, C)$; $a_8 \rightarrow (A, P)$; $a_9 \rightarrow (P, D)$; $a_{10} \rightarrow (A, D)$; $a_{11} \rightarrow (D, D)$; $a_{12} \rightarrow (D, D)$.

Каждому орграфу G можно поставить в соответствие единственный неориентированный граф G_1, называемый симметризацией орграфа G, если каждую дугу в G, ведущую из одной вершины в другую, заменить неориентированным ребром, соединяющим ту же пару вершин. Разным орграфам может соответствовать одна и та же симметризация. Процесс перехода от неориентированного графа к орграфу, симметризация которого совпадает с исходным графом, называется ориентацией графа.

Вершина и дуга в орграфе называются инцидентными, если соответствующие им вершина и ребро инцидентны в его симметризации. Две вершины в орграфе называются смежными, если смежными являются соответствующие им вершины в его симметризации. Две дуги в орграфе называются смежными, если смежными являются два соответствующих им ребра в его сим-

метризации. Две дуги в орграфе называются параллельными, если параллельными являются два соответствующих им ребра в его симметризации.

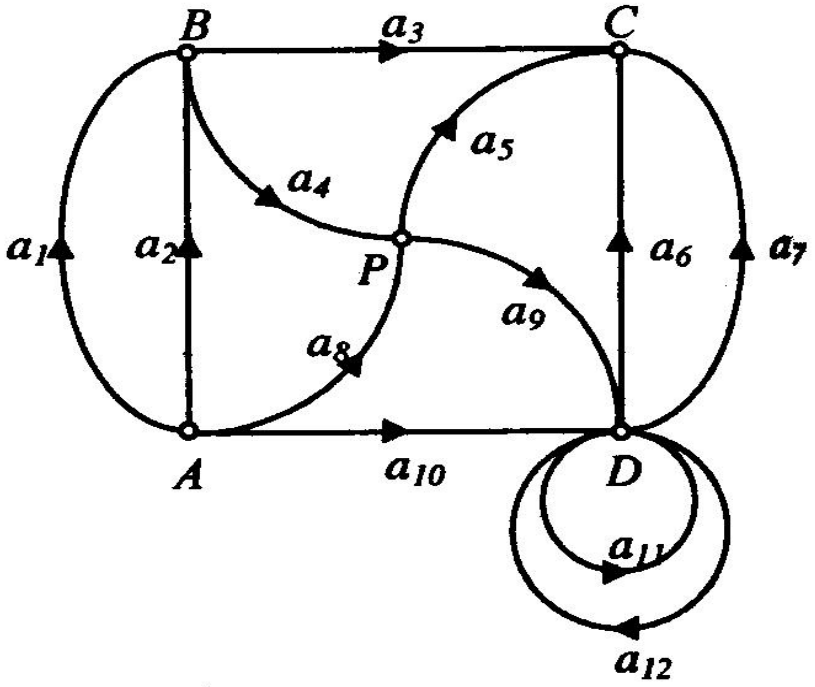


Рис. 2.19. Пример орграфа

В ориентированном графе параллельные дуги бывают двух типов – строго параллельные (одинаково ориентированные) и нестрого параллельные (ориентированные по-разному). На рис. 2.20 дуги *a* и *b* строго параллельны, а дуги *c* и *d* нестрого параллельны.

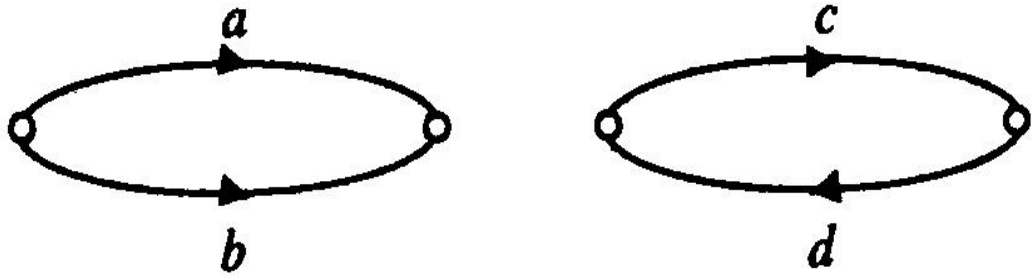


Рис. 2.20. Параллельные дуги

Степенью вершины орграфа называется количество инцидентных ей дуг. Ясно, что степень вершины орграфа равна степени соответствующей вершины в неориентированном графе,

который является симметризацией орграфа. Следовательно, для ориентированного графа, точно так же, как для неориентированного, будет выполняться равенство (1.4.1) и, следовательно, орграф может содержать лишь четное количество нечетных вершин.

В ориентированном графе *G (V, A)* дуги, инцидентные некоторой вершине *A*, можно разбить на два класса – входящие в эту вершину и выходящие из нее. В соответствии с этим степень вершины расщепляется на два слагаемых: положительная и отрицательная полустепень вершины. Положительной полустепенью называется количество дуг, входящих в вершину, а отрицательной полустепенью называется количество дуг, выходящих из вершины.

Разность положительной и отрицательной полустепеней вершины называется дефектом степени вершины. Вершина ориентированного графа называется уравновешенной, если она имеет нулевой дефект степени. Ясно, что уравновешенная вершина является четной. Орграф называется равновесным, если все его вершины уравновешены. Сумма абсолютных величин дефектов степеней всех вершин называется степенью неравновесности орграфа.

Формально изоморфизм орграфов определяется точно так же, как и изоморфизм неориентированных графов. Ориентированные графы *G* и G_1 называются изоморфными (или равными*)* если между их однотипными элементами можно установить взаимно однозначное соответствие, сохраняющее отношение инциденции. Заметим, что если два орграфа изоморфны, то изоморфными будут и неориентированные графы, являющиеся их симметризациями. Обратное, вообще говоря, неверно. Так, на рис. 2.21 представлены три попарно неизоморфных графа с изоморфными симметризациями.

Два ориентированных графа являются изоморфными, если изоморфны их симметризации и, кроме того, граничные точки соответствующих дуг упорядочены одинаково.

Изоморфные орграфы имеют одинаковые комбинаторные свойства. В частности, при изоморфизме соответствующие вершины имеют одинаковые положительные и одинаковые отрицательные полустепени, изоморфизм сохраняет строгую (и нестрогую) параллельность дуг.

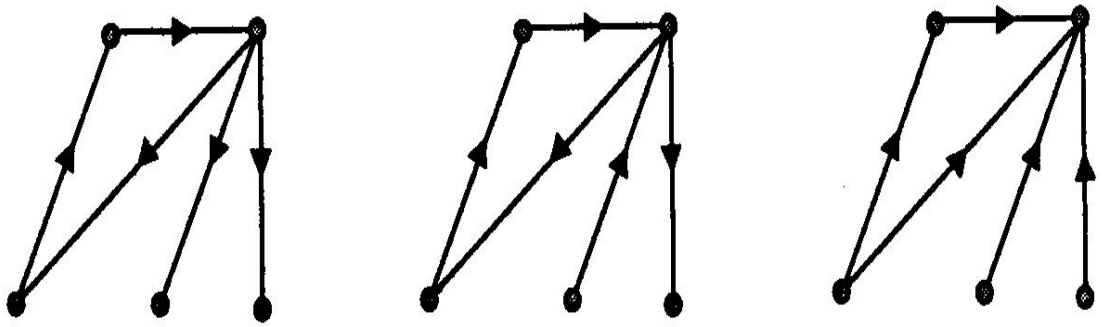


Рис. 2.21. Изоморфизм орграфа

Рассмотрим ориентированный граф $G(V, E, f)$ с множеством вершин $V=\{A_1,A_2,...,A_n,...\}$, множеством дуг $E\{a_1,a_2,...,a_n,...\}$ и отображением инциденции f.

Ориентированным маршрутом (или ормаршрутом) длины k называется последовательность из k (не обязательно различных) дуг $a_1,a_2,...,a_k$ графа G, если для каждой пары соседних дуг этой последовательности конечная вершина предыдущей дуги является начальной вершиной последующей. Первая и последняя вершины называются соответственно начальной и конечной точкой ормаршрута. Остальные вершины последовательности называются промежуточными точками этого ормаршрута. Также говорят, что ормаршрут $a_1,a_2,...,a_k$. соединяет вершины A_1 и A_k.

Ормаршрут называется замкнутым, если его начальная и конечная точки совпадают. В противном случае ормаршрут называется незамкнутым. Любая дуга в орграфе является незамкнутым ормаршрутом длины 1, соединяющим свои граничные вершины. Любая петля в орграфе – это замкнутый ормаршрут длины 1.

Любой ормаршрут (замкнутый или незамкнутый) в орграфе G однозначно определяет неориентированный маршрут в соответствующей симметризации G_1. Однако, если некоторая последовательность ребер в неориентированном графе G_1 образует маршрут, то это вовсе не означает, что в орграфе G (для которого G_1, служит симметризацией) соответствующая последовательность дуг определяет ормаршрут. Действительно, рассмотрим орграф G

и его симметризацию G_1, (см. рис. 2.22). Последовательность дуг a_1, a_2 в G не образует ормаршрута, но в симметризации G_1 им соответствующая последовательность ребер a_1, a_2, образует неориентированный маршрут длины 2, соединяющий вершины A и B.

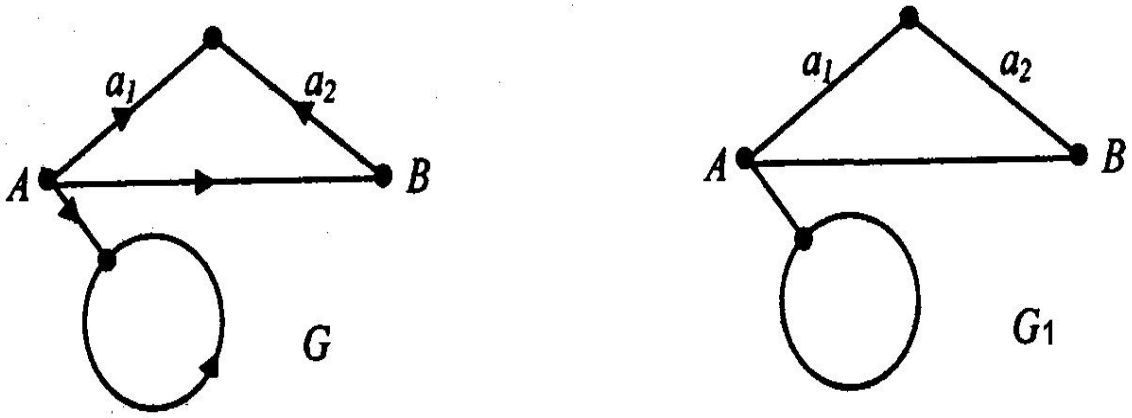


Рис. 2.22. Орграф и его симметризация

Ориентированный незамкнутый маршрут называется п у т е м (или у п о р я д о ч е н н о й ц е п ь ю), если в нем нет повторяющихся дуг; если же в незамкнутом ормаршруте нет повторяющихся вершин (а значит – и повторяющихся дуг), то он называется п р о с т ы м путем.

Ориентированный замкнутый маршрут называется к о н т у р о м (или у п о р я д о ч е н н ы м ц и к л о м), если в нем нет повторяющихся дуг; если же в замкнутом ормаршруте нет повторяющихся промежуточных вершин (а значит – и повторяющихся дуг), то он называется п р о с т ы м контуром.

Ориентированный граф G называется с в я з н ы м, если его симметризация G_1 является связным графом в смысле определения из пункта 2.1.8.

Сформулированное выше понятие связности для орграфов имеет один важный недостаток в приложениях. Если интерпретировать дугу орграфа как прямую связь между объектами, а путь из дуг – как сложную связь между начальным и конечным объектами, то связность орграфа, в общем случае, не будет означать, что между любыми двумя объектами существует связь, как это было для неориентированных связных графов. Дело в том, что связи в ориентированном графе имеют «направленный» характер

и существование связи между объектами A и B не гарантирует существование обратной связи между B и A.

В этой связи представим граф автомобильных дорог. Если этот граф связен, то от любого перекрестка к любому другому можно доехать по дорогам. Предположим теперь, что на всех дорогах разрешено движение только в одном направлении. Граф дорог в этом случае получит ориентацию. Он останется связным орграфом, но теперь может случиться так, что от какого-то перекрестка к некоторому другому будет невозможно доехать, двигаясь по дорогам только в разрешенных направлениях. Чтобы существовала «направленная» связь между любой парой перекрестков, необходимо потребовать, чтобы в орграфе дорог для любой пары вершин A и B существовал путь, ведущий от A к B, и путь, ведущий от B к A. Это требование к орграфу является более сильным, чем связность, и называется *сильной связностью*.

Итак, орграф называется *сильно связным*, если для любой пары различных вершин A и B существует путь, ведущий от A к B, и существует путь, ведущий от B к A. Если граф сильно связен, то он является связным. Обратное, вообще говоря, не верно.

Ориентированный граф называется *сильно k-связным*, если для любой пары различных вершин A и B существует по крайней мере k путей из A в B, которые не имеют общих вершин (а следовательно, и дуг), за исключением A и B. Если орграф сильно k-связен, то его симметризация также является k-связным графом в смысле определения из пункта 2.1.8. Очевидно, что обратное, вообще говоря, не верно. Если орграф автомобильных дорог сильно k-связен, то от любого перекрестка к любому другому можно проехать не менее чем k различными способами, не нарушая при этом правила одностороннего движения.

2.3. Сети

В приложениях граф обычно интерпретируется как сеть, а его вершины называют *узлами*. Рассмотрим несколько характерных задач. При принятии важных решений для выбора наилучшего направления действий из имеющихся вариантов используется так называемое *дерево решений*, представляющее собой

схематическое описание проблемы принятия решений. С деревьями связана одна из проблем минимального соединения, внешне напоминающая задачу о коммивояжере, но значительно проще разрешаемая (для решения этой проблемы построены эффективные алгоритмы). Имеется n городов – $A_1, A_2, ..., A_n$, которые нужно связать между собой сетью дорог. Стоимость сооружения дороги, соединяющей города A_i и A_k, известна и равна $C(A_i , A_k)$. Какой должна быть сеть дорог, связывающая все города, чтобы стоимость ее сооружения была минимальной?

Граф наиболее дешевой соединяющей сети непременно должен быть деревом. В противном случае в графе найдется хотя бы один цикл. При удалении любого из звеньев этого цикла стоимость сети уменьшится, а города все еще останутся соединенными. Тем самым, число ребер искомого графа должно быть равным $n-1$.

Алгоритм (план реализации)

На первом шаге связываем два города с наиболее дешевым соединяющим звеном e_1. На каждом следующем шаге добавляем самое дешевое из звеньев e_i (если имеется несколько звеньев с одинаковой стоимостью, выбираем любое из них), в результате присоединения которого к уже построенным звеньям найденная сеть удлиняется еще на одно звено, но никакого цикла не образуется. При поиске добавляемого звена надо перебирать все ребра, имеющие общую вершину с уже построенной сетью. Последний шаг алгоритма имеет номер $n-1$. Стоимость строительства полученной сети минимальна и равна

$$c(e_1)+c(e_2)+ ...+c(e_{n-1}).$$

Пример 1. Пусть, например, нужно соединить города *A, B, C* и *D*. Стоимость строительства дорог, соединяющих любые два города, известна и в условных единицах представлена в таблице:

	A	*B*	*C*	*D*
A	–	11	13	12
B	11	–	6	9
C	13	6	–	10
D	12	9	10	–

Сеть дорог минимальной стоимости состоит из 3 (4-1=3) звеньев и строится так: сначала выбирается самый дешевый участок дороги – *BC* (его цена равна 6), затем он удлиняется на самый дешевый из оставшихся – *BD* (его цена равна 9). И на последнем, третьем шаге вновь выбирается самый дешевый (но так, чтобы не образовалось никакого цикла) – *AB* (его цена равна 11) (рис. 2.23). Таким образом, стоимость строительства равна 26 (6+9+11).

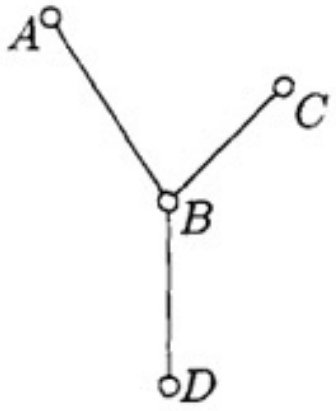


Рис. 2.23. Граф соединения городов

С теорией графов связана задача выбора кратчайшего пути (маршрута) до узлов сети. Допустим, дана сеть, каждое ребро которой помечено числом, равным его длине. Требуется найти кратчайший маршрут, ведущий от выделенного узла к каждому из узлов сети. На практике алгоритмы выбора кратчайшего (оптимального) пути решают специальные устройства, называемые маршрутизаторами, автоматически по заданному алгоритму, либо администраторами сети. В качестве оптимального маршрута выбирается не только длина пути, но и другие параметры (пропускная способность, скорость и другие). Алгоритм решения этой задачи состоит из двух частей. Покажем, как он работает, на следующем примере.

Пример 2. Рассмотрим сеть, заданную на рис. 2.24, с выделенным узлом 1.

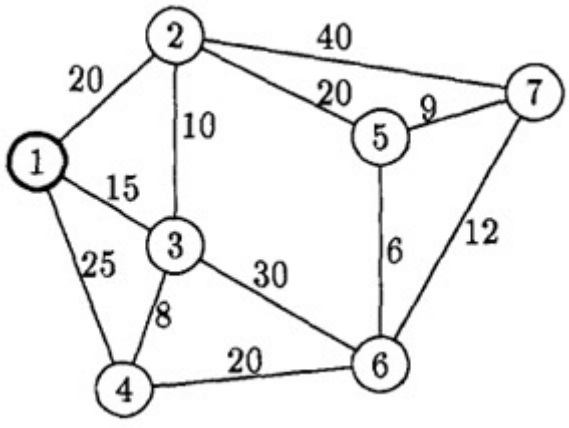


Рис. 2.24. Граф сети

Прямой ход алгоритма

1-й шаг. Все узлы, которые соединены с выделенным узлом 1 одним ребром, метятся так, как это показано на рис. 2.25 – первое число в метке равно расстоянию от помеченного узла до узла 1. Ребро, связывающее узлы 1 и 3, является кратчайшим маршрутом от узла 1 к узлу 3 (любой другой маршрут от узла 1 к узлу 3 длиннее), и поэтому узлу 3 приписывается постоянная метка (15,1). Таким образом, по окончании 1-го шага узлы 1 и 3 имеют постоянные метки, узлы 2 и 4 – временные метки, а узлы 5, б и 7 никаких меток не имеют (рис. 2.26).

Замечание. При получении постоянной метки узел 3 выделяется так же, как и узел 1.

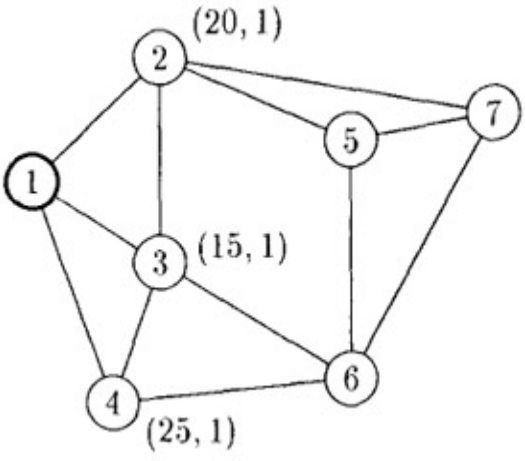


Рис. 2.25. Шаг 1 (начало)

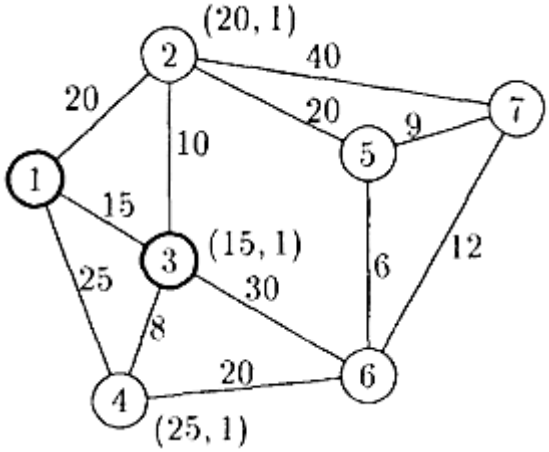


Рис. 2.26. Шаг 1 (конец)

2-й шаг. Отбираются все узлы, которые соединены с узлом 3 одним ребром и не имеют постоянных меток. Это узлы 2, 4 и 6. Сравнивая длины маршрутов 1-2 и 1-3-2, замечаем, что длина первого (20) меньше длины второго (15+10=25). Поэтому метка (20,1) узла 2 остается неизменной.

Сравнивая длины маршрутов 1-4 и 1-3-4, замечаем, что длина первого (25) больше длины второго (15 + 8 = 23). Поэтому временная метка (25,1) узла 4 меняется на метку (23,3). Узел 6 получает метку (45,3).

Замечание. Первое число в метке указывает длину маршрута от узла 1, а второе – номер предшествующего узла.

Ребро, связывающее узлы 1 и 2, является кратчайшим маршрутом от узла 1 к узлу 2 (любой другой маршрут от узла 1 к узлу 2 длиннее), и поэтому узлу 2 приписывается постоянная метка

(20,1). Таким образом, по окончании 2-го шага узлы 1, 2 и 3 имеют постоянные метки, узлы 4 и 6 – временные метки, а узлы 5 и 7 никаких меток не имеют (рис. 2.27).

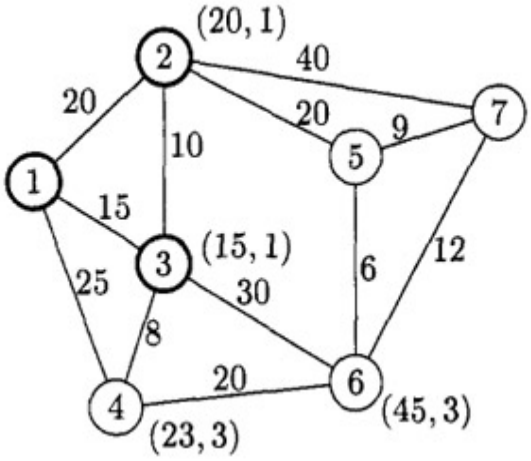


Рис. 2.27. Шаг 2

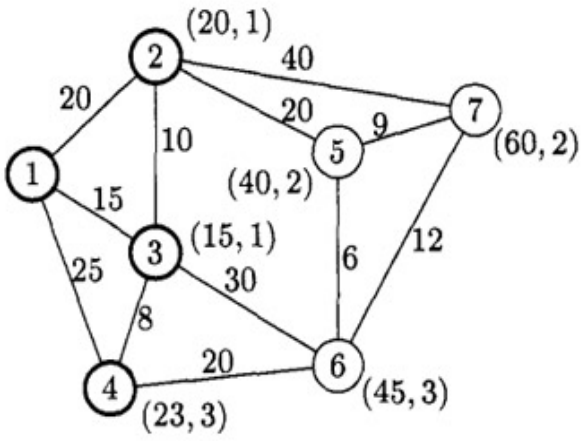


Рис. 2.28. Шаг 3

3-й шаг. Отбираются все узлы, которые соединены с узлом 2 одним ребром и не имеют постоянных меток. Это узлы 5 и 7. Узел 5 получает метку (40,2). Узел 7 получает метку (60,2). Маршрут 1-3-4, связывающий узлы 1 и 4, является кратчайшим маршрутом от узла 1 к узлу 4 (любой другой маршрут от узла 1 к узлу 4 длиннее); поэтому узлу 4 приписывается постоянная метка (23,3). Таким образом, по окончании 3-го шага узлы 1, 2, 3 и 4 имеют постоянные метки, а узлы 5, 6 и 7 – временные метки (рис. 2.28).

4-й шаг. Отбираются все узлы, которые соединены с узлом 4 одним ребром и не имеют постоянных меток. Это узел 6.

Сравнивая длины маршрутов 1-3-6 и 1-3-4-6, замечаем, что длины первого (45) и третьего (45) больше длины второго (43). Поэтому временная метка (45,3) узла 6 меняется на метку (43,4). Маршрут 1-2-5, связывающий узлы 1 и 5, является кратчайшим маршрутом от узла 1 к узлу 5 (любой другой маршрут от узла 1 к узлу 5 длиннее), и поэтому узлу 5 приписывается постоянная метка (40,2). Таким образом, по окончании 4-го шага узлы 1, 2, 3, 4 и 5 имеют постоянные метки, а узлы 6 и 7 – временные метки (рис. 2.29).

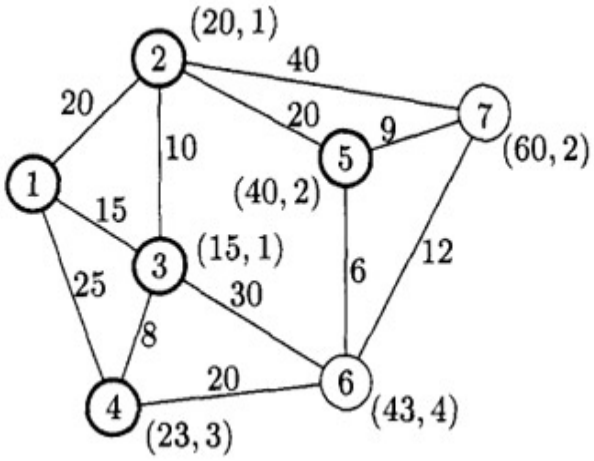


Рис. 2.29. Шаг 4

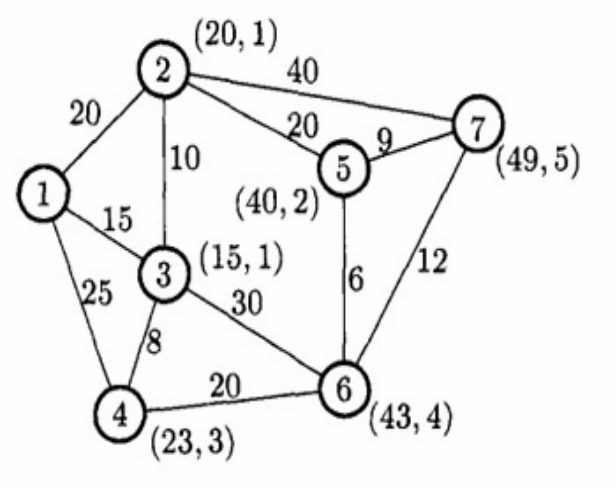


Рис. 2.30. Шаг 5

Следующие два шага позволяют дать постоянные метки узлам 6 и 7 – (43,4) и (49,5) соответственно (рис. 2.30).

Замечание. На каждом шаге временная метка одного из узлов меняется на постоянную по следующему правилу: рассматриваются все узлы с временными метками и выбирается тот из них, длина маршрута до которого от узла 1 является наименьшей.

Обратный ход алгоритма

Используя вторую компоненту метки, определяем последовательность вершин в каждом кратчайшем маршруте. Например:

метка (49,5) узла 7 указывает на предшествующий узел 5,

метка (40,2) узла 5 указывает на предшествующий узел 2,

метка (20,1) узла 2 указывает на предшествующий узел 1.

В результате обратная последовательность узлов кратчайшего маршрута от узла 1 к узлу 7 имеет вид 7→5→2→1.

Ответ:

Узел	**Маршрут**	**Длина**
2	1-2	20
3	1-3	15
4	1-3-4	23
5	1-2-5	40
6	1-3-4-6	43
7	1-2-5-7	49

Задания

1. Телефонная компания планирует соединить подземным кабелем шесть городов, расстояния между которыми заданы при помощи таблицы:

	A	**B**	**C**	**D**	**E**	**F**
A	–	10	9	30	27	20
B	10	–	15	18	17	20
C	9	15	–	25	21	16
D	30	18	25	–	8	17
E	27	17	21	8	–	13
F	20	20	16	17	13	–

Найдите минимальную длину кабеля, позволяющего жителям любых двух городов связаться друг с другом по телефону.

2. Найдите кратчайшие маршруты, ведущие из узла A во все другие узлы сети, представленной на рис. 2.31.

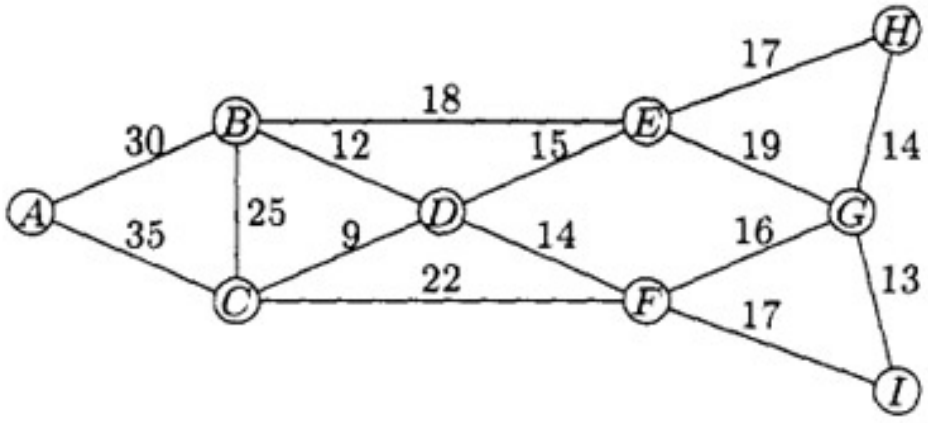


Рис. 2.31. Задача нахождения кратчайшего пути

ГЛАВА 3

ОСНОВЫ ПОСТРОЕНИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ

3.1. Основные понятия

Каждое из трех прошедших столетий ознаменовалось преобладанием одной господствующей технологии. Восемнадцатое столетие было веком индустриальной революции и механизации. В XIX веке наступила эпоха паровых двигателей. В течение XX века главной технологией стали сбор, обработка и распространение информации. Среди прочих разработок следует отметить создание глобальных телефонных сетей, изобретение радио и телевидения, рождение и небывалый рост компьютерной индустрии, запуск спутников связи.

Благодаря высокой скорости технологического прогресса эти области очень быстро проникают друг в друга, при этом различия между сбором, транспортировкой, хранением и обработкой информации продолжают быстро исчезать. Организации с сотнями офисов, разбросанных по всему миру, должны иметь возможность получать информацию о текущем состоянии своего самого удаленного офиса мгновенно, нажатием кнопки. По мере роста нашего умения собирать, обрабатывать и распространять информацию, потребности в средствах еще более сложной обработки информации растут все быстрее,

Хотя компьютерная индустрия еще довольно молода по сравнению с другими производствами (например, автомобильной или авиационной промышленностью), прогресс в сфере производства компьютеров был весьма впечатляющим. В первые два десятилетия своего существования компьютерные системы были сильно централизованными, как правило, в пределах одного помещения.

Часто эта комната оборудовалась стеклянными стенами, сквозь которые посетители могли полюбоваться на великое электронное чудо. Компания среднего размера или университет могли позволить себе один-два компьютера, тогда как у крупных организаций их было по нескольку десятков. Сама мысль о том, что через какие-нибудь 20 лет столь же мощные компьютеры будут иметь размеры меньше почтовой марки и производиться миллионами, тогда казалась чистой фантастикой.

Объединение компьютеров и средств связи оказало глубокое влияние на принцип организации компьютерных систем. Концепция «компьютерного центра» в виде комнаты, в которой помещался большой компьютер, и куда пользователи приносили свои программы, сегодня полностью устарела. Модель, в которой один компьютер выполнял всю необходимую работу по обработке данных, уступила место модели, представляющей собой большое количество отдельных, но связанных между собой компьютеров. Такие системы называются *компьютерными сетями*.

Каждый компьютер в сети может иметь периферийные устройства, доступные другим компьютерам сети. Поэтому можно привести еще одно, более общее, определение компьютерной сети. Компьютерной сетью называется совокупность узлов (компьютеров, терминалов, периферийных устройств), имеющих возможность информационного взаимодействия друг с другом с помощью коммуникационного оборудования и программного обеспечения.

Два компьютера называются связанными между собой, если они могут обмениваться информацией. Связь не обязательно должна осуществляться при помощи медного провода. Могут использоваться самые разнообразные средства связи, включая волоконную оптику, радиоволны высокой частоты и спутники связи.

Компьютерные сети отнюдь не являются единственным видом сетей, созданным человеческой цивилизацией. Даже водопроводы Древнего Рима можно рассматривать как один из наиболее древних примеров сетей, покрывающих большие территории и обслуживающих многочисленных клиентов. Другой, менее экзотический пример – электрические сети. В них легко можно найти все компоненты любой территориальной сети: источники ресурсов – электростанции, магистрали – высоковольтные линии электропе-

редач, сеть доступа – трансформаторные подстанции, клиентское оборудование – осветительные и бытовые электроприборы.

Размеры сетей варьируются в широких пределах – от пары соединенных между собой компьютеров, стоящих на соседних столах, до миллионов компьютеров, разбросанных по всему миру (часть из них может находиться и на космических объектах). По широте охвата принято деление сетей на несколько категорий. *Локальные вычислительные сети, ЛВС* или *LAN* (Local Area Network), позволяют объединять компьютеры, расположенные в ограниченном пространстве. Для локальных сетей, как правило, прокладывается специализированная кабельная система, и положение возможных точек подключения абонентов ограничено этой кабельной системой. Иногда в локальных сетях используют и беспроводную связь (wireless), но и при этом возможности перемещения абонентов сильно ограничены.

Локальные сети можно объединять в более крупномасштабные образования – *CAN* (Campus Area Network – *кампусная* сеть, объединяющая локальные сети близко расположенных зданий), *MAN* (Metropolitan Area Network – сеть городского масштаба), *WAN* (Wide Area Network – широкомасштабная сеть), *GAN* (Global Area Network – глобальная сеть). Сетью сетей в наше время называют глобальную сеть Интернет.

Для более крупных сетей также устанавливаются специальные проводные или беспроводные линии связи или используется инфраструктура существующих публичных средств связи, например, телефонные линии. В последнем случае абоненты компьютерной сети могут подключаться к сети в относительно произвольных точках, охваченных сетью телефонии, кабельного телевидения.

В сетях применяются различные сетевые технологии, из которых в локальных сетях наиболее распространены *Ethernet, Token Ring, 100VG-AnyLAN, ARCnet, FDDI*. В глобальных сетях применяются иные технологии. Каждой технологии соответствуют свои типы оборудования.

Оборудование сетей подразделяется на активное – интерфейсные карты компьютеров, повторители, концентраторы и т.п. и пассивное – кабели, соединительные разъемы, коммутационные панели и т. п. Кроме того, имеется вспомогательное обо-

рудование – устройства бесперебойного питания, кондиционирования воздуха и аксессуары – монтажные стойки, шкафы, кабелепроводы различного вида. С точки зрения физики, активное оборудование – это устройства, которым необходима подача энергии для генерации сигналов, пассивное оборудование подачи энергии не требует.

Оборудование компьютерных сетей подразделяется на конечные системы (устройства), являющиеся источниками и/или потребителями информации, и промежуточные системы, обеспечивающие прохождение информации по сети. К *конечным системам, ES* (End Systems), относятся компьютеры, терминалы, сетевые принтеры, факс-машины, кассовые аппараты, считыватели штрих-кодов, средства голосовой и видеосвязи и любые другие периферийные устройства, снабженные тем или иным сетевым интерфейсом. К *промежуточным системам, IS* (Intermediate Systems), относятся концентраторы (повторители, мосты, коммутаторы), маршрутизаторы, модемы и прочие телекоммуникационные устройства, а также соединяющая их кабельная и/или беспроводная инфраструктура.

Действием, «полезным» для пользователей, является обмен информацией между конечными устройствами. Поток информации, передаваемый по сети, называют сетевым трафиком. Трафик кроме полезной информации включает и служебную ее часть – неизбежные накладные расходы на организацию взаимодействия узлов сети. Пропускная способность линий связи, называемая также полосой пропускания, определяется как количество информации, проходящей через линию за единицу времени. Она измеряется в специальных единицах *бит/с* (bps – bit per second), *Кбит/с* (kbps), *Мбит/с* (Mbps), *Гбит/с* (Gbps), *Тбит/с* (Tbps)...

Для активного коммуникационного оборудования применимо понятие производительность, причем в двух различных аспектах. Кроме «валового» количества неструктурированной информации, пропускаемого оборудованием за единицу времени (бит/с), интересуются и скоростью обработки пакетов (*pps* – packets per second), кадров (*fps* – frames per second) или ячеек (*cps* – cells per second). Естественно, при этом оговаривается и размер структур (пакетов, кадров, ячеек), для которых измеряется ско-

рость обработки. В идеале производительность коммуникационного оборудования должна быть столь высокой, чтобы обеспечивать обработку информации, приходящей на все интерфейсы (порты) на их полной скорости.

Для организации обмена информацией должен быть разработан комплекс программных и аппаратных средств, распределенных по разным устройствам сети. Поначалу разработчики и поставщики сетевых средств пытались идти каждый по своему пути, решая весь комплекс задач с помощью собственного набора протоколов, программ и аппаратуры. Однако решения различных поставщиков оказывались несовместимыми друг с другом, что вызывало массу неудобств для пользователей, которых по разным причинам не удовлетворял набор возможностей, предоставляемых только одним из поставщиков. По мере развития техники и расширения ассортимента предоставляемых сервисов назрела необходимость декомпозиции сетевой задачи – разбивки ее на несколько взаимосвязанных подзадач с определением правил взаимодействия между ними. Разбивка задачи и стандартизация протоколов позволяет принимать участие в ее решении большому количеству сторон – разработчиков программных и аппаратных средств, изготовителей коммуникационного и вспомогательного (например, тестового) оборудования и инсталляторов, доносящих все эти плоды прогресса до конечных потребителей. Применение открытых технологий и следование общепринятым стандартам позволяет избегать эффекта вавилонского столпотворения. Конечно, в какой-то момент стандарт становится тормозом развития, но кто-то делает прорыв, и его новая фирменная технология со временем выливается в новый стандарт.

3.2. Применение компьютерных сетей

Современные организации обычно используют большое количество компьютеров, часто довольно удаленных друг от друга. Например, компания, состоящая из нескольких офисов, может иметь по компьютеру в каждом из офисов для обеспечения производственных процессов. Поначалу все эти компьютеры могут работать изолированно друг от друга, однако в какой-то момент

администрация может принять решение соединить их, чтобы иметь возможность быстрого доступа к информации по всей компании.

Если посмотреть на эту проблему с более общих позиций, то вопросом здесь является **совместное использование ресурсов,** а целью – предоставление доступа к программам, оборудованию и особенно данным для любого пользователя сети, независимо от физического расположения ресурса и пользователя. Другими словами, то, что пользователь находится на расстоянии 1000 км от данных, не должно помешать ему воспользоваться этими данными так же, как если бы они находились рядом. То есть целью сетей является борьба с географическим разбросом.

Вторая цель заключается в обеспечении **высокой надежности** при помощи альтернативных источников информации. Например, все файлы могут быть реплицированы на двух или трех машинах, так что, если одна из них недоступна (из-за отказа аппаратуры), могут быть использованы другие копии. Кроме того, наличие нескольких процессоров означает, что если один из них выйдет из строя, другие могут выполнить его работу, хотя возможно и с уменьшенной производительностью. Возможность продолжать работу, несмотря на аппаратные проблемы, имеет чрезвычайно большое значение для военных и банковских задач, в управлении воздушным транспортом, безопасностью ядерных реакторов, управлении непрерывными технологическими процессами и т.п.

Еще одной целью является экономия средств. Небольшие компьютеры обладают значительно лучшим соотношением производительности и цены, нежели большие. Универсальные вычислительные машины размером с комнату работают быстрее персональных компьютеров примерно в десятки раз, однако их стоимость больше в тысячу раз. Это несоответствие заставляет многих разработчиков создавать системы, состоящие из персональных компьютеров, по одному на пользователя, с данными, хранящимися на одном или нескольких совместно используемых **файл-серверах**. В такой модели пользователи называются **клиентами**, а вся система – **клиент-серверной моделью.**

В клиент-серверной модели обмен информацией обычно принимает форму запросов от клиента к серверу, при помощи кото-

рых клиент просит сервер выполнить какие-либо действия. Сервер выполняет работу и отсылает обратно ответ. Обычно в сети количество клиентов значительно больше числа используемых ими серверов. На рисунке 3.1 представлена принципиальная схема клиент-серверной модели.

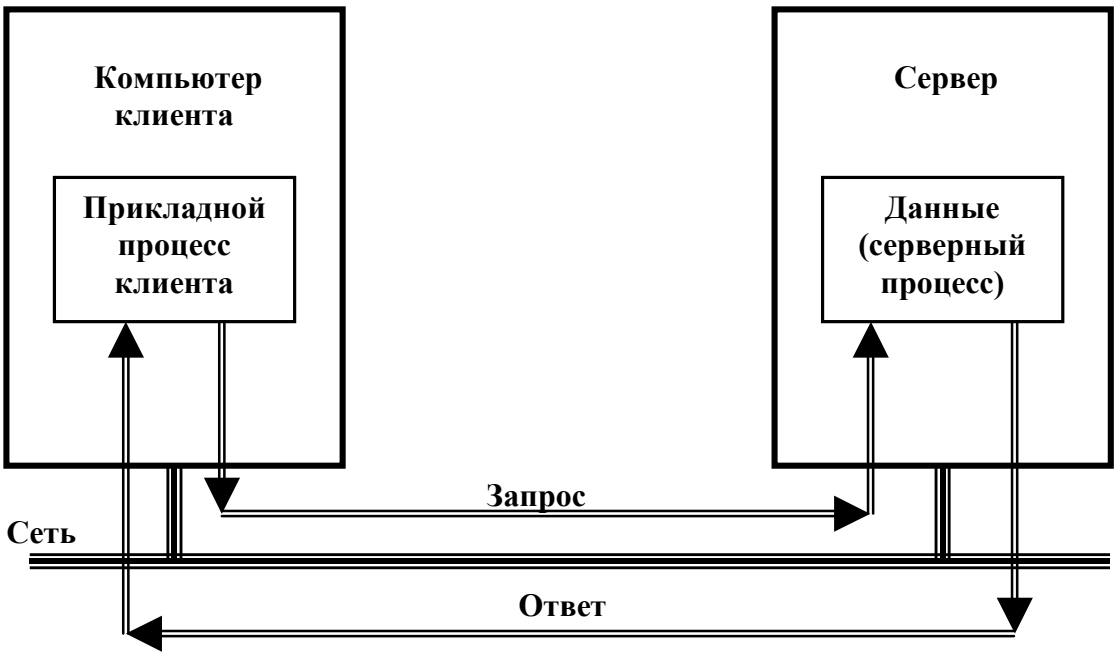
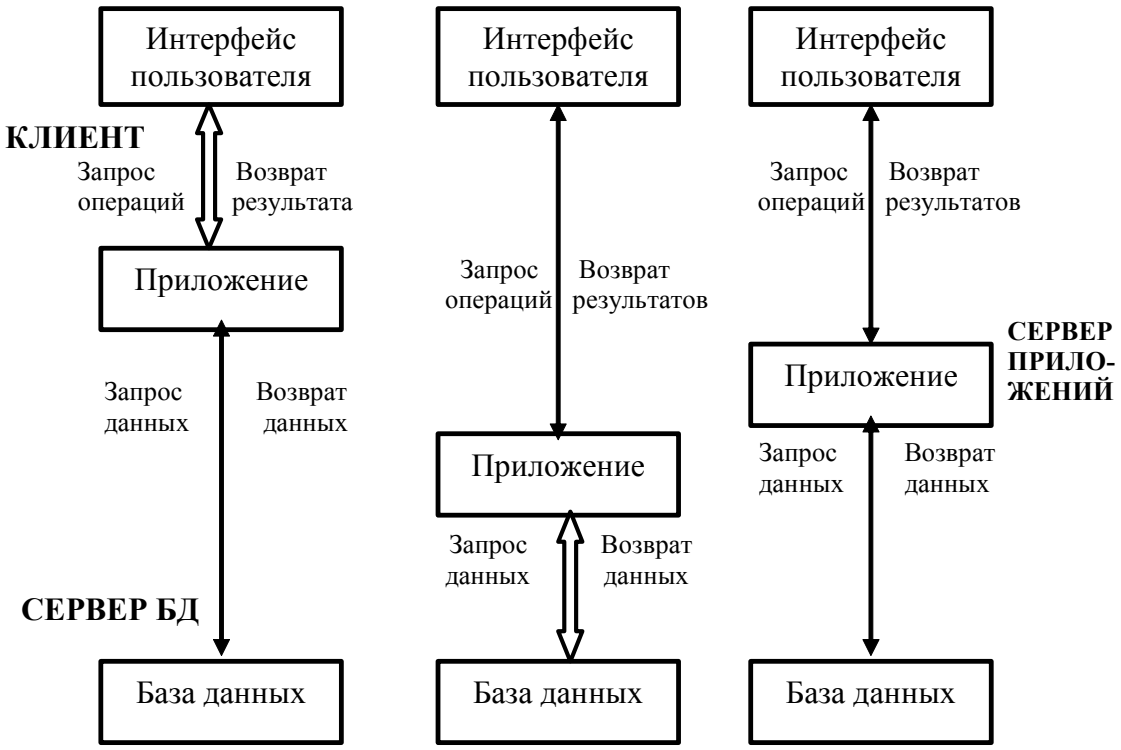


Рис. 3.1. Модель «клиент-сервер»

В системах, построенных по принципу клиент-сервер, выделяются три логических уровня: уровень пользовательского интерфейса, уровень обработки информации, уровень данных. Двухзвенная архитектура предполагает наличие двух машин: клиентской (рабочей станции) и сервера. Распределение логических уровней может быть различным. Возможен вариант, когда вся прикладная часть информационной системы выполняется на компьютерах пользователей системы (клиентов), а на стороне серверов осуществляется только доступ к базе данных (Рис. 3.2, *а*). В случаях, когда логика прикладной части системы достаточно сложна, каждый пользовательский компьютер должен обладать достаточным набором ресурсов, чтобы быть в состоянии произвести обработку данных, поступающих от пользователя и из базы данных.

Противоположным является вариант, когда на клиентской машине реализован только пользовательский интерфейс, а вся обра-

ботка данных и сами данные находятся на сервере (Рис. 3.2, *б*). Возможны промежуточные варианты, когда пользовательский интерфейс, обработка данных и база данных могут быть частично реализованы на клиентской машине, а частично на сервере.



а) б) в)

Рис. 3.2. Варианты реализации модели «клиент-сервер»

Для повышения общей эффективности системы все чаще применяются трехзвенные архитектуры. В этой архитектуре, кроме клиентской части системы и сервера базы данных, вводится промежуточный сервер приложений (Рис. 3.2, *в*). На машине клиента выполняются только интерфейсные действия, вся логика обработки информации поддерживается сервером приложений, а данные располагаются на сервере баз данных.

В последние годы все чаще применяются системы с распределенными базами данных. В этом случае необходимые данные расположены одновременно на нескольких серверах. В этом случае серверные процессы производят запросы данных с других серверов по сети.

Еще одной целью компьютерной сети является масштабируемость, то есть способность увеличивать производитель-

ность системы по мере роста нагрузки на систему за счет простого добавления процессоров. Когда перестает хватать возможностей мэйнфрейма, всю систему требуется заменить на более производительную, что обычно влечет очень большие финансовые затраты и неудобство для пользователей. В случае клиент-серверной модели новые клиенты и новые серверы могут добавляться по мере надобности.

И, наконец, еще одна цель установки компьютерной сети имеет мало общего с технологией вообще. Компьютерная сеть является мощным средством связи между удаленными друг от друга сотрудниками организации. При помощи сети два или более удаленных друг от друга сотрудника могут легко составить совместный отчет. Если один из сотрудников изменяет документ, находящийся на сервере, в подключенном режиме (on-line), остальные сотрудники могут немедленно увидеть эти изменения, а не ждать письма в течение нескольких дней. Подобное ускорение передачи информации делает возможным сотрудничество удаленных друг от друга групп людей. На длительном отрезке времени использование сетей для общения между людьми может оказаться даже важнее, чем любая из технических целей, как, например, увеличение надежности.

Все приведенные выше цели построения компьютерных сетей имеют экономическую или технологическую природу. В 90-х годах компьютерные сети стали предоставлять услуги частным лицам на дому. Можно выделить три наиболее важных причины популярности использования сетей частными лицами: доступ к удаленной информации, общение, интерактивные развлечения.

Доступ к удаленной информации может осуществляться в различной форме. В качестве примера можно привести доступ к финансовым учреждениям. Люди оплачивают счета, управляют банковскими счетами и вкладами при помощи компьютерных сетей. Кроме того, становятся популярными Интернет-магазины с возможностью просмотра в подключенном режиме (*on-line*) каталогов тысяч компаний. Важным является доступ к электронным источникам информации (газеты, библиотеки, базы данных и т.д.). Все приведенные возможности применения сетей включают взаимодействие между пользователем и удаленной базой данных.

Следующей категорией применения сетей является общение между частными лицами, что можно назвать ответом XXI века веку XIX с его изобретением телефона. Электронная почта уже широко используется миллионами людей. Электронная почта реального времени позволит удаленным пользователям без задержки также видеть и слышать друг друга. Подобная технология делает возможными виртуальные собрания, называемые видеоконференциями, в которых могут принимать участие люди, находящиеся далеко друг от друга.

Третья категория – развлечения – является гигантской индустрией, продолжающей развиваться. По оценкам специалистов рынок игровой индустрии в мире (компьютерные, мобильные телефоны, игровые приставки) оценивается в настоящее время в 20 биллионов долларов в год.

Вместе с тем, широкое распространение сетей вызовет новые социальные, этические и политические проблемы. Взгляды, излагаемые в сети одними людьми, могут оказаться оскорбительными для других. Некоторые люди придерживаются точки зрения «живи и дай жить другим», однако другие считают, что помещение в сети некоторых материалов просто недопустимо. Таким образом, возможны различные конфликтные ситуации с непредсказуемыми последствиями. Еще одной областью конфликтов является соблюдение авторских прав на информацию, размещаемую в сети. Компьютерные сети предоставляют также возможности для посылки анонимных сообщений, дезинформации, информации оскорбительного содержания и для других нежелательных действий.

Итак, подобно печатному станку 500 лет назад, компьютерные сети предоставляют новые способы распространения гражданами их точек зрения среди самой различной аудитории. Новая свобода распространения информации несет с собой и новые нерешенные политические, юридические, психологические и социальные проблемы.

3.3. Эволюция компьютерных систем

Обратимся сначала к компьютерному корню вычислительных сетей. Первые компьютеры 50-х годов – большие, громоздкие и

дорогие – предназначались для очень небольшого числа избранных пользователей. Часто эти монстры занимали целые здания. Такие компьютеры не были предназначены для интерактивной работы пользователя, а использовались в режиме пакетной обработки. Системы пакетной обработки, как правило, строились на базе **мэйнфрейма** – мощного и надежного компьютера универсального назначения. Пользователи подготавливали перфокарты, содержащие данные и команды программ, и передавали их в вычислительный центр. Операторы вводили эти карты в компьютер, а распечатанные результаты пользователи получали обычно только на следующий день. Таким образом, одна неверно набитая карта означала как минимум суточную задержку.

Конечно, для пользователей интерактивный режим работы, при котором можно с терминала оперативно руководить процессом обработки своих данных, был бы гораздо удобней. Но интересами пользователей на первых этапах развития вычислительных систем в значительной степени пренебрегали, поскольку пакетный режим – это самый эффективный режим использования вычислительной мощности, так как он позволяет выполнить в единицу времени больше пользовательских задач, чем любые другие режимы. Во главу угла ставилась эффективность работы самого дорогого устройства вычислительной машины – процессора, в ущерб эффективности работы использующих его специалистов.

По мере удешевления процессоров в начале 60-х годов появились новые способы организации вычислительного процесса, которые позволили учесть интересы пользователей. Начали развиваться интерактивные многотерминальные системы разделения времени. В таких системах компьютер отдавался в распоряжение сразу нескольким пользователям. Каждый пользователь получал собственный терминал, с помощью которого он мог вести диалог с компьютером. Причем время реакции вычислительной системы было достаточно мало для того, чтобы пользователю была не слишком заметна параллельная работа с компьютером и других пользователей. Разделяя таким образом компьютер, пользователи получили возможность за сравнительно небольшую плату пользоваться преимуществами компьютеризации.

Терминалы, выйдя за пределы вычислительного центра, рассредоточились по всему предприятию. И хотя вычислительная мощность оставалась полностью централизованной, некоторые функции, такие как ввод и вывод данных, стали распределенными. Подобные многотерминальные централизованные системы внешне уже были очень похожи на локальные вычислительные сети. Действительно, рядовой пользователь работу за терминалом мэйнфрейма воспринимал примерно так же, как сейчас он воспринимает работу за подключенным к сети персональным компьютером. Пользователь мог получить доступ к общим файлам и периферийным устройствам, при этом у него поддерживалась полная иллюзия единоличного владения компьютером, так как он мог запустить нужную ему программу в любой момент и почти сразу же получить результат.

Таким образом, многотерминальные системы, работающие в режиме разделения времени, стали первым шагом на пути создания локальных вычислительных сетей. Но до появления локальных сетей нужно было пройти еще большой путь, так как многотерминальные системы, хотя и имели внешние черты распределенных систем, все еще сохраняли сущность централизованной обработки данных.

С другой стороны, и потребность предприятий в создании локальных сетей в это время еще не созрела – в одном здании просто нечего было объединять в сеть, так как из-за высокой стоимости вычислительной техники предприятия не могли себе позволить роскошь приобретения нескольких компьютеров. В этот период был справедлив так называемый «закон Гроша», который эмпирически отражал уровень технологии того времени. В соответствии с этим законом производительность компьютера была пропорциональна квадрату его стоимости, отсюда следовало, что за одну и ту же сумму было выгоднее купить одну мощную машину, чем две менее мощных, так как их суммарная мощность оказывалась намного ниже мощности дорогой машины.

А вот потребность в соединении компьютеров, находящихся на большом расстоянии друг от друга, к этому времени вполне назрела. Началось все с решения более простой задачи доступа к компьютеру с терминалов, удаленных от него на многие сотни, а то и тысячи километров. Терминалы соединялись с компьютера-

ми через телефонные сети с помощью модемов. Такие сети позволяли многочисленным пользователям получать удаленный доступ к разделяемым ресурсам нескольких мощных компьютеров класса супер-ЭВМ. Затем появились системы, в которых наряду с удаленными соединениями типа терминал–компьютер были реализованы и удаленные связи типа компьютер–компьютер. Компьютеры получили возможность обмениваться данными в автоматическом режиме, что, собственно, и является базовым механизмом любой вычислительной сети. На основе этого механизма в первых сетях были реализованы службы обмена файлами, синхронизации баз данных, электронной почты и другие, ставшие теперь традиционными сетевые службы.

Таким образом, хронологически первыми появились *глобальные сети (Wide Area Networks, WAN),* то есть сети, объединяющие территориально рассредоточенные компьютеры, возможно находящиеся в различных городах и странах. Именно при построении глобальных сетей были впервые предложены и отработаны многие основные идеи и концепции современных вычислительных сетей. Такие, например, как многоуровневое построение коммуникационных протоколов, технология коммутации пакетов, маршрутизация пакетов в составных сетях.

Глобальные компьютерные сети очень многое унаследовали от других, гораздо более старых и распространенных глобальных телефонных сетей. Главным результатом создания первых глобальных компьютерных сетей был отказ от принципа коммутации каналов, на протяжении многих десятков лет успешно использовавшегося в телефонных сетях. Выделяемый на все время сеанса связи составной канал с постоянной скоростью не мог эффективно использоваться пульсирующим трафиком компьютерных данных, у которого периоды интенсивного обмена чередуются с продолжительными паузами. Натурные эксперименты и математическое моделирование показали, что пульсирующий и в значительной степени не чувствительный к задержкам компьютерный трафик гораздо эффективней передается сетями, использующими принцип коммутации пакетов, когда данные разделяются на небольшие порции – пакеты, которые самостоятельно перемещаются по сети за счет встраивания адреса конечного узла в заголовок пакета.

Так как прокладка высококачественных линий связи на большие расстояния обходится очень дорого, то в первых глобальных сетях часто использовались уже существующие каналы связи, изначально предназначенные совсем для других целей. Например, в течение многих лет глобальные сети строились на основе телефонных каналов, способных в каждый момент времени вести передачу только одного разговора в аналоговой форме. Поскольку скорость передачи дискретных компьютерных данных по таким каналам была очень низкой (десятки килобит в секунду), набор предоставляемых услуг в глобальных сетях такого типа обычно ограничивался передачей файлов, преимущественно в фоновом режиме, и электронной почтой. Помимо низкой скорости такие каналы имеют и другой недостаток – они вносят значительные искажения в передаваемые сигналы. Поэтому протоколы глобальных сетей, построенных с использованием каналов связи низкого качества, отличаются сложными процедурами контроля и восстановления данных. Типичным примером таких сетей являются сети X.25, разработанные еще в начале 70-х годов, когда низкоскоростные аналоговые каналы, арендуемые у телефонных компаний, были преобладающим типом каналов, соединяющих компьютеры и коммутаторы глобальной вычислительной сети. Прогресс глобальных компьютерных сетей во многом определялся прогрессом телефонных сетей.

С конца 60-х годов в телефонных сетях все чаще стала применяться передача голоса в цифровой форме, что привело к появлению высокоскоростных цифровых каналов, соединяющих АТС и позволяющих одновременно передавать десятки и сотни разговоров.

К настоящему времени глобальные сети по разнообразию и качеству сервисов догнали локальные сети, которые долгое время были лидерами в этом отношении, хотя и появились на свет значительно позже.

Важное событие, повлиявшее на эволюцию компьютерных сетей, произошло в начале 70-х годов. В результате технологического прорыва в области производства компьютерных компонентов появились большие интегральные схемы (БИС). Их сравнительно невысокая стоимость и хорошие функциональные возможности привели к созданию мини-компьютеров, которые стали

реальными конкурентами мэйнфреймов. Эмпирический закон Гроша перестал соответствовать действительности, так как десяток мини-компьютеров, имея ту же стоимость, что и мэйнфрейм, выполнял некоторые задачи (как правило, хорошо распараллеливаемые) быстрее. Даже небольшие подразделения предприятий получили возможность иметь собственные компьютеры. Мини-компьютеры выполняли задачи управления технологическим оборудованием, складом и другие задачи уровня отдела предприятия. Таким образом, появилась концепция распределения компьютерных ресурсов по всему предприятию. Однако при этом все компьютеры одной организации по-прежнему продолжали работать автономно. Но шло время, потребности пользователей вычислительной техники росли. Их уже не удовлетворяла изолированная работа на собственном компьютере, им хотелось в автоматическом режиме обмениваться компьютерными данными с пользователями других подразделений. Ответом на эту потребность стало появление первых локальных вычислительных сетей, объединяющих компьютеры, сосредоточенные на небольшой территории, обычно в радиусе не более 1 – 2 км, хотя в отдельных случаях локальная сеть может иметь и более протяженные размеры, например, в несколько десятков километров. В общем случае локальная сеть представляет собой коммуникационную систему, принадлежащую одной организации.

На первых порах для соединения компьютеров друг с другом использовались нестандартные программно-аппаратные средства. Разнообразные устройства сопряжения, использующие свой собственный способ представления данных на линиях связи, свои типы кабелей и т. п., могли соединять только те конкретные модели компьютеров, для которых были разработаны, например, мини-компьютеры PDP-11 с мэйнфреймом IBM 360 или компьютеры «Наири» с компьютерами «Днепр».

В середине 80-х годов положение дел в локальных сетях стало кардинально меняться. Утвердились стандартные технологии объединения компьютеров в сеть: Ethernet, Arcnet, Token Ring, Token Bus, несколько позже FDDI. Мощным стимулом для их появления послужили персональные компьютеры. Эти массовые продукты явились идеальными элементами для построения сетей. С одной стороны, они были достаточно мощными для работы се-

тевого программного обеспечения, а с другой – явно нуждались в объединении своей вычислительной мощности для решения сложных задач, а также разделении дорогих периферийных устройств и дисковых массивов. Поэтому персональные компьютеры стали преобладать в локальных сетях, причем не только в качестве клиентских компьютеров, но и в качестве центров хранения и обработки данных, то есть сетевых серверов, потеснив с этих привычных ролей мини-компьютеры и мэйнфреймы.

Все стандартные технологии локальных сетей опирались на тот же принцип коммутации, который был с успехом опробован и доказал свои преимущества при передаче трафика данных в глобальных компьютерных сетях – принцип коммутации пакетов. Для создания сети достаточно было приобрести сетевые адаптеры соответствующего стандарта, например Ethernet, стандартный кабель, присоединить адаптеры к кабелю стандартными разъемами и установить на компьютер одну из популярных сетевых операционных систем, например, Novell NetWare. После этого сеть начинала работать и последующее присоединение каждого нового компьютера не вызывало никаких проблем, если на нем был установлен сетевой адаптер той же технологии.

Разработчики локальных сетей привнесли много нового в организацию работы пользователей. Так, намного проще и удобнее стало получать доступ к совместно используемым сетевым ресурсам. В отличии от глобальной, в локальной сети пользователь освобождается от запоминания сложных идентификаторов разделяемых ресурсов. Для этих целей система предоставляет ему список ресурсов в удобной для восприятия форме, например, в виде древовидной графической структуры. Еще один прием, рационализирующий работу пользователя в локальной сети, состоит в том, что после соединения с удаленным ресурсом пользователь получает возможность обращаться к нему с помощью тех же команд, которые он использовал при работе с локальными ресурсами. Последствием и одновременно движущей силой такого прогресса стало появление огромного числа непрофессиональных пользователей, освобожденных от необходимости изучать специальные (и достаточно сложные) команды для сетевой работы.

Может возникнуть вопрос: почему все эти удобства пользователи получили только с приходом локальных сетей? Главным об-

разом, это связано с использованием в локальных сетях качественных кабельных линий связи, на которых даже сетевые адаптеры первого поколения обеспечивали скорость передачи данных до 10 Мбит/с. При небольшой протяженности, свойственной локальным сетям, стоимость таких линий связи была вполне приемлемой. Поэтому экономное расходование пропускной способности каналов, которое было одной из главных целей технологий ранних глобальных сетей, никогда не выходило на первый план при разработке протоколов локальных сетей. В таких условиях основным механизмом прозрачного доступа к сетевым ресурсам локальных сетей стали периодические широковещательные объявления серверов о своих ресурсах и услугах. На основании таких объявлений клиентские компьютеры составляли списки имеющихся в сети ресурсов и предоставляли их пользователю.

Конец 90-х выявил явного лидера среди технологий локальных сетей – семейство Ethernet, в которое вошли классическая технология Ethernet 10 Мбит/с, а также Fast Ethernet 100 Мбит/с и Gigabit Ethernet 1000 Мбит/с. Простые алгоритмы работы предопределили низкую стоимость оборудования Ethernet. Широкий диапазон иерархии скоростей позволяет рационально строить локальную сеть, применяя ту технологию семейства, которая в наибольшей степени отвечает задачам предприятия и потребностям пользователей. Важно также, что все технологии Ethernet очень близки друг к другу по принципам работы, что упрощает обслуживание и интеграцию этих сетей.

3.4. Конвергенция сетей

В конце 80-х годов отличия между локальными и глобальными сетями проявлялись весьма отчетливо по многим технологическим параметрам и видам предоставляемых услуг.

Протяженность и качество линий связи. Локальные компьютерные сети по определению отличаются от глобальных сетей небольшими расстояниями между узлами сети. Это в принципе делает возможным использование в локальных сетях более качественных линий связи.

Сложность методов передачи данных. В условиях низкой надежности физических каналов в глобальных сетях требуются более сложные, чем в локальных сетях, методы передачи данных и соответствующее оборудование.

Скорость обмена данными в локальных сетях (10, 16 и 100 Мбит/с) в то время была существенно выше, чем в глобальных (от 2,4 кбит/с до 2 Мбит/с).

Разнообразие услуг. Высокие скорости обмена данными породили в локальных сетях широкий набор услуг – это различные виды услуг файловой службы, услуги печати, услуги баз данных, электронная почта и другие, в то время как глобальные сети в основном предоставляли почтовые услуги и иногда файловые услуги с ограниченными возможностями.

Масштабируемость. «Классические» локальные сети обладают плохой масштабируемостью из-за жесткости базовых топологий, определяющих способ подключения станций и длину линии. При этом характеристики сети резко ухудшаются при достижении определенного предела по количеству узлов или протяженности линий связи. Глобальным сетям свойственна хорошая масштабируемость, так как они изначально разрабатывались в расчете на работу с произвольными топологиями и сколь угодно большим количеством абонентов.

Постепенно различия между локальными и глобальными типами сетевых технологий стали сглаживаться. Изолированные ранее локальные сети начали объединять друг с другом, при этом в качестве связующей среды использовались глобальные сети. Тесная интеграция локальных и глобальных сетей привела к значительному взаимопроникновению соответствующих технологий.

Сближение в методах передачи данных происходит на платформе цифровой передачи данных по волоконно-оптическим линиям связи. Эту среду передачи данных используют практически все технологии локальных сетей для скоростного обмена информацией на расстояниях свыше 100 м, на ней же построены современные магистрали сетей, предоставляющих свои цифровые каналы для объединения оборудования глобальных компьютерных сетей.

Высокое качество цифровых каналов изменило требования к протоколам глобальных компьютерных сетей. На первый план

вместо процедур обеспечения надежности вышли процедуры обеспечения гарантированной средней скорости доставки информации пользователям, а также механизмы приоритетной обработки пакетов особенно чувствительного к задержкам трафика, например, голосового.

Большой вклад в сближение локальных и глобальных сетей внесло доминирование протокола IP. Этот протокол сегодня используется поверх любых технологий локальных и глобальных сетей – Ethernet, Token Ring, ATM, frame relay– для создания из различных подсетей единой составной сети.

Компьютерные глобальные сети 90-х годов, работающие на основе скоростных цифровых каналов, существенно расширили набор своих услуг и догнали в этом отношении локальные сети. Стало возможным создание служб, работа которых связана с доставкой пользователю больших объемов информации в реальном времени – изображений, видеофильмов, голоса, в общем, всего того, что получило название мультимедийной информации. Наиболее яркий пример – гипертекстовая информационная служба World Wide Web (WWW), ставшая основным поставщиком информации в Интернете. Ее интерактивные возможности превзошли возможности многих аналогичных служб локальных сетей, так что разработчикам локальных сетей пришлось просто позаимствовать эту службу у глобальных сетей. Процесс переноса служб и технологий из глобальной сети Интернет в локальные приобрел такой массовый характер, что появился даже специальный термин – *intranet-технологии* (intra – внутренний).

Понятие интранет обозначает внутреннюю сеть организации, где важны два момента: 1) изоляция или защита внутренней сети от внешней (Интернет); 2) использование сетевого протокола IP и Web-технологий (прикладного протокола HTTP). В аппаратном аспекте применение технологии интранет означает, что все абоненты сети в основном обмениваются данными с одним или несколькими серверами, на которых сосредоточены основные информационные ресурсы предприятия.

В локальных сетях в последнее время уделяется такое же большое внимание методам обеспечения защиты информации от несанкционированного доступа, как и в глобальных сетях. Это обусловлено тем, что локальные сети перестали быть изолиро-

ванными, чаще всего они имеют выход в «большой мир» через глобальные связи. Защита локальных сетей часто строится на тех же методах – шифрование данных, аутентификация и авторизация пользователей.

И, наконец, появляются новые технологии, изначально предназначенные для обоих видов сетей. Примером может служить семейство технологий Ethernet, имеющее явные «локальные» корни.

Одним из проявлений сближения локальных и глобальных сетей является появление сетей масштаба большого города, занимающих промежуточное положение между локальными и глобальными сетями. Эти сети используют цифровые линии связи. Они обеспечивают экономичное соединение локальных сетей между собой, а также выход в глобальные сети. Эти сети первоначально были разработаны для передачи данных, но сейчас они поддерживают и такие услуги, как видеоконференции и интегральную передачу голоса и текста.

Ярко выраженная в последнее время тенденция сближения различных типов сетей характерна не только для локальных и глобальных компьютерных сетей, но и для телекоммуникационных сетей других типов. К телекоммуникационным сетям, кроме компьютерных, относятся телефонные сети, радиосети и телевизионные сети. Во всех них в качестве ресурса, предоставляемого клиентам, выступает информация.

Телефонные сети оказывают интерактивные услуги, так как два абонента, участвующие в разговоре (или несколько абонентов, если это конференция), попеременно проявляют активность.

Радиосети и телевизионные сети оказывают широковещательные услуги, при этом информация распространяется только в одну сторону – из сети к абонентам, по схеме «один ко многим».

Конвергенция телекоммуникационных сетей идет по многим направлениям. Прежде всего, наблюдается *сближение видов услуг,* предоставляемых клиентам. Компьютерные сети изначально разрабатывались для передачи алфавитно-цифровой информации, которую часто называют просто данными, в результате у компьютерных сетей имеется и другое название – *сети передачи данных*. Телефонные сети и радиосети созданы для передачи только голосовой информации, а телевизионные сети передают

голос и изображение. Сегодня на роль глобальной мультисервисной сети нового поколения претендует Интернет. Особую привлекательность представляют собой новые виды комбинированных услуг, в которых сочетаются несколько традиционных услуг, например, услуга универсальной службы сообщений, объединяющей электронную почту, телефонию, факсимильную службу и пейджинговую связь.

Технологическое сближение сетей происходит сегодня на основе цифровой передачи информации различного типа, метода коммутации пакетов и программирования услуг. Телефония уже давно сделала ряд шагов навстречу компьютерным сетям. Прежде всего, за счет представления голоса в цифровой форме, что делает принципиально возможным передачу телефонного и компьютерного трафика по одним и тем же цифровым каналам. Сегодня пакетные методы коммутации постепенно теснят традиционные для телефонных сетей методы коммутации каналов даже при передаче голоса. У этой тенденции есть достаточно очевидная причина – на основе метода коммутации пакетов можно более эффективно использовать пропускную способность каналов связи и коммутационного оборудования. Например, паузы в телефонном разговоре могут составлять до 40 % общего времени соединения, однако только пакетная коммутация позволяет «вырезать» паузы и использовать высвободившуюся пропускную способность канала для передачи трафика других абонентов. Другой веской причиной перехода к коммутации пакетов является популярность сети Интернет, построенной на основе данной технологии.

Компьютерные сети также многое позаимствовали у телефонных и телевизионных сетей. Глобальные компьютерные сети строятся по такому же иерархическому принципу, что и телефонные, в соответствии с которым сети городов и районов объединяются в региональные сети, а те, в свою очередь, – в национальные и международные сети. Компьютерные сети берут на вооружение методы обеспечения отказоустойчивости телефонных сетей, за счет которых последние демонстрируют высокую степень надежности, так недостающую порой Интернету и корпоративным сетям.

Сегодня становится все более очевидным, что мультисервисная сеть нового поколения не может быть создана в результате

«победы» какой-нибудь одной технологии или подхода. Ее может породить только процесс конвергенции, когда от каждой технологии будет взято все самое лучшее и соединено в некоторый новый сплав, который и даст требуемое качество для поддержки существующих и создания новых услуг. Появился новый термин – инфокоммуникационная сеть, который прямо говорит о двух составляющих современной сети – информационной (компьютерной) и телекоммуникационной.

3.5. Компьютерные сети как частный случай распределенных вычислительных систем

Компьютерные сети относятся к распределенным (или децентрализованным) вычислительным системам. В литературе существует значительная путаница между понятиями *компьютерная сеть* и *распределенная система*. Основное их различие заключается в том, что в распределенной системе наличие многочисленных автономных компьютеров прозрачно (то есть незаметно) для пользователя. Он может набрать команду для запуска некой программы, и программа запустится. Однако какой выбрать процессор, где расположены необходимые для работы программы файлы, как их транспортировать и куда выдать результат, будет решать операционная система. Другими словами, пользователь распределенной системы не знает о существовании нескольких процессоров. Система выглядит как единый виртуальный процессор. Назначение заданий процессорам и файлов дискам, перемещение файлов с мест хранения к месту их использования, а также прочие системные функции должны быть автоматическими.

В сети пользователь должен *явно* зарегистрироваться на одной машине, *явно* указывать удаленные задания, *явно* перемещать файлы и управлять работой сети. В распределенной системе ничего не должно делаться явно, все производится системой автоматически, незаметно для пользователя. На самом деле распределенная система является программной системой, построенной на базе сети. Эта программная система обеспечивает высокую сте-

пень связности элементов и прозрачности. Таким образом, различие между компьютерной сетью и распределенной системой заключается в программном обеспечении (особенно в операционной системе), а не в аппаратуре. Тем не менее, эти два понятия имеют очень много общего. Например, как компьютерная сеть, так и распределенная система занимаются перемещением файлов. Разница заключается в том, кто вызывает эти перемещения – система или пользователь.

Компьютерные сети являются логическим результатом эволюции двух важнейших научно-технических отраслей современной цивилизации – компьютерных и телекоммуникационных технологий. С одной стороны, сети представляют собой частный случай распределенных вычислительных систем, в которых группа компьютеров согласованно выполняет набор взаимосвязанных задач, обмениваясь данными в автоматическом режиме. С другой стороны, компьютерные сети могут рассматриваться как средство передачи информации на большие расстояния, для чего в них применяются методы кодирования и мультиплексирования данных, получившие развитие в различных телекоммуникационных системах. Поскольку основным признаком распределенной вычислительной системы является наличие нескольких центров обработки данных, то наряду с компьютерными сетями к распределенным системам относят также мультипроцессорные компьютеры и многомашинные вычислительные комплексы.

3.6. Мультипроцессорные компьютеры

Принципиальная схема мультипроцессорного компьютера представлена на рисунке 3.3.

В мультипроцессорных компьютерах имеется несколько процессоров (П1, П2, …), каждый из которых может относительно независимо от остальных выполнять свою программу. В мультипроцессоре существует общая для всех процессоров операционная система, которая оперативно распределяет вычислительную нагрузку между процессорами. Взаимодействие между отдельными процессорами организуется наиболее простым способом – через общую оперативную память (ОП).

Сам по себе процессорный блок не является законченным компьютером и поэтому не может выполнять программы без остальных блоков мультипроцессорного компьютера – дисковой памяти (Д) и периферийных устройств, которые подключены через соответствующие интерфейсы (И1, И2, …). Все периферийные устройства являются для всех процессоров мультипроцессорной системы общими. Мультипроцессору не свойственна территориальная распределенность. Все его блоки располагаются в одном или нескольких близко расположенных конструктивах, как и у обычного компьютера. Основное достоинство мультипроцессора – его высокая производительность, которая достигается за счет параллельной работы нескольких процессоров.

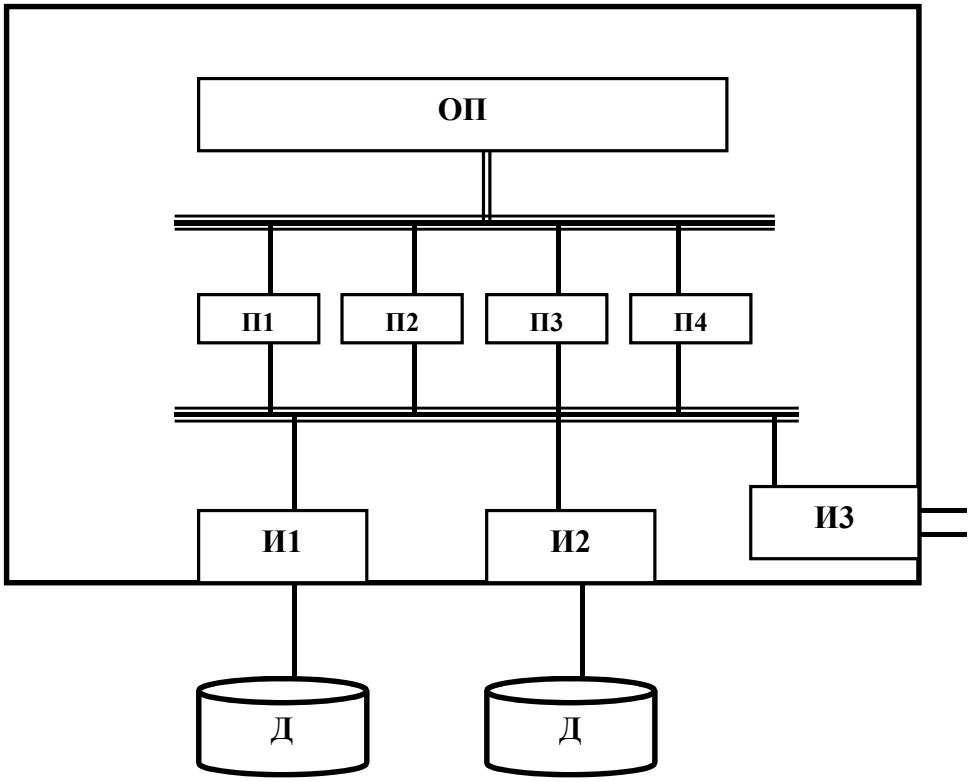


Рис. 3.3. Принципиальная схема мультипроцессорного компьютера

Еще одним важным свойством мультипроцессорных систем является отказоустойчивость, то есть способность к продолжению работы при отказах некоторых элементов, например процессоров или блоков памяти. При этом производительность, естественно, снижается, но не до нуля, как в обычных системах, в которых отсутствует избыточность. Однако для того, чтобы мультипроцессор мог продолжать работу после отказа одного из процессоров, необходимо

специальное программное обеспечение поддержки отказоустойчивости, которое может быть частью операционной системы или же представлять собой дополнительные служебные программы.

3.7. Кластеры

Кластер (многомашинная система) – это вычислительный комплекс, состоящий из нескольких компьютеров (каждый из которых работает под управлением собственной операционной системы), а также программные и аппаратные средства связи компьютеров, которые обеспечивают работу всех компьютеров комплекса как единого целого.

В отличие от мультипроцессора, в котором избыточность реализована на уровне процессорных блоков, кластер состоит из нескольких законченных, способных работать автономно, как правило, стандартных компьютеров, каждый из которых имеет обычную структуру, включающую один или несколько процессорных блоков, оперативную память и периферийные устройства (рис. 3.4).

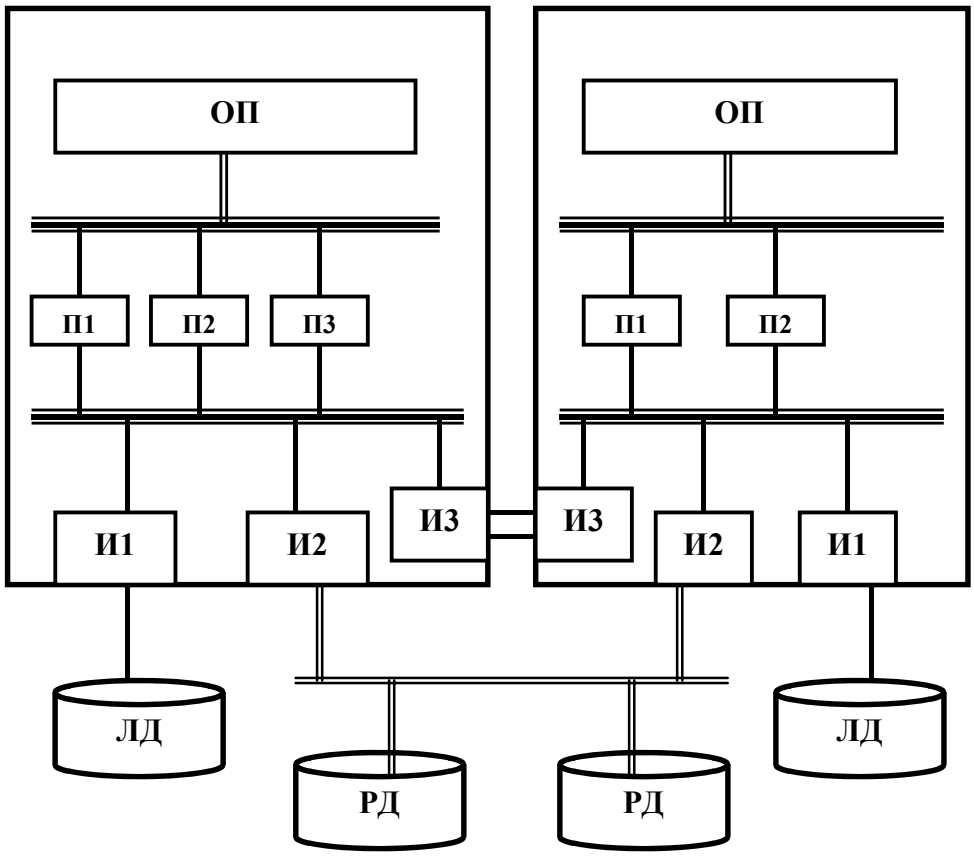


Рис. 3.4. Принципиальная схема кластера

Однако благодаря специальному программному и аппаратному обеспечению межкомпьютерных связей для пользователя кластер выглядит как единый компьютер. При этом каждый компьютер (называемый также узлом кластера) может быть как однопроцессорным, так и мультипроцессорным – на организацию кластера это влияния не оказывает. Компьютеры кластера могут иметь как локальные диски (ЛД), так и общие (разделяемые) дисковые накопители (РД).

Кластеры применяют для повышения надежности и производительности вычислительной системы. Надежность повышается за счет того, что при отказе одного из узлов кластера вычислительная нагрузка (или часть ее) переносится на другой узел. Для выполнения этой операции в кластере используется два типа связей между узлами: *межпроцессорные* связи и связи за счет *разделяемых дисков*.

Межпроцессорные связи используются узлами для обмена служебной информацией. В частности, с помощью этих связей каждый узел кластера периодически проверяет состояние других узлов и выполняемых ими вычислительных задач. Если какой-либо узел или одна из его задач (входящая в набор защищаемых от отказов задач) изменили свое состояние на неработоспособное, то начинается процедура перемещения (реконфигурации) нагрузки на один из работоспособных узлов. В этой процедуре важную роль играют разделяемые диски. Защищаемая задача должна хранить свои данные на одном из таких дисков, чтобы новый узел смог продолжать их использовать после отказа основного. Так как надежность дисковых накопителей достаточно высока (ее можно повысить за счет дополнительных мер, например зеркалирования разделяемого диска), то существенно повышается и надежность кластера по сравнению с отдельным компьютером.

Если кластер применяется для повышения производительности, то каждая задача распараллеливается на несколько ветвей, которые выполняются одновременно на нескольких узлах кластера. Для организации межпроцессорных связей в кластерах часто используются специализированные технологии, приспособленные к решению специфических задач взаимодействия компьютеров в кластере. Однако в последнее время все чаще для

этой цели применяются стандартные технологии локальных сетей, например Fast Ethernet и Gigabit Ethernet.

Выводы

Вычислительная сеть – это совокупность компьютеров и периферийных устройств, соединенных линиями связи. Линии связи образованы кабелями, сетевыми адаптерами и другими коммуникационными устройствами. Все сетевое оборудование работает под управлением системного и прикладного программного обеспечения.

Вычислительные сети стали логическим результатом эволюции компьютерных и телекоммуникационных технологий. С одной стороны, они являются частным случаем распределенных вычислительных систем, а с другой стороны, могут рассматриваться как средство передачи информации на большие расстояния, для чего в них применяются методы кодирования и мультиплексирования данных, получившие развитие в различных телекоммуникационных системах.

Классифицируя сети по территориальному признаку, различают **глобальные** (*WAN*), **локальные** (*LAN*) и **городские** (*MAN*) сети.

Хронологически первыми появились **глобальные сети**. Они объединяют компьютеры, рассредоточенные на расстоянии сотен и тысяч километров. Традиционные глобальные компьютерные сети очень многое унаследовали от телефонных сетей. В основном они предназначены для передачи данных. В них часто используются уже существующие не очень качественные линии связи, что приводит к более низким, чем в локальных сетях, скоростям передачи данных и ограничивает набор предоставляемых услуг передачей файлов, преимущественно не в оперативном, а в фоновом режиме, с использованием электронной почты.

Локальные сети сосредоточены на территории не более 1 – 2 км. Они построены с использованием дорогих высококачественных линий связи, которые позволяют, применяя более простые методы передачи данных, чем в глобальных сетях, достигать высоких скоростей обмена данными порядка 100 Мбит/с. Предос-

тавляемые услуги отличаются широким разнообразием и обычно предусматривают реализацию в режиме подключения (on-line).

Важнейший этап в развитии сетей – появление стандартных сетевых технологий: Ethernet, FDDI, Token Ring, позволяющих быстро и эффективно объединять компьютеры различных типов.

В конце 80-х годов локальные и глобальные сети имели существенные отличия по протяженности и качеству линий связи, сложности методов передачи данных, скорости обмена данными, разнообразию услуг и масштабируемости.

В дальнейшем в результате тесной интеграции локальных и глобальных сетей произошло взаимопроникновение соответствующих технологий.

Одним из проявлений сближения локальных и глобальных сетей является появление сетей масштаба большого города, занимающих промежуточное положение между локальными и глобальными сетями. **Городские сети** (MAN) предназначены для обслуживания территории крупного города. При достаточно больших расстояниях между узлами (десятки километров) они обладают качественными линиями связи и высокими скоростями обмена, иногда даже более высокими, чем в традиционных локальных сетях. MAN обеспечивают экономичное соединение локальных сетей между собой, а также выход в глобальные сети.

Тенденция сближения различных типов сетей характерна не только для локальных и глобальных компьютерных сетей, но и для телекоммуникационных сетей других типов. К телекоммуникационным сетям, кроме компьютерных, относятся телефонные сети, радиосети и телевизионные сети.

Компьютерные сети представляют собой частный случай распределенных вычислительных систем, в которых группа компьютеров согласованно выполняет набор взаимосвязанных задач, обмениваясь данными в автоматическом режиме. Наряду с компьютерными сетями к распределенным системам относят также мультипроцессорные компьютеры и многомашинные вычислительные комплексы.

В **мультипроцессорных компьютерах** имеется несколько процессоров, каждый из которых может независимо от остальных обращаться к общей памяти и выполнять собственную программу. Все периферийные устройства являются для всех процессо-

ров мультипроцессорной системы общими. В мультипроцессоре существует общая для всех процессоров операционная система, которая распределяет вычислительную нагрузку между процессорами. Мультипроцессору не свойственна территориальная распределенность – все его блоки располагаются в одном или нескольких близко расположенных конструктивах, как и у обычного компьютера.

Многомашинный комплекс (кластер) – это вычислительная система, состоящая из нескольких компьютеров (каждый из которых работает под управлением собственной операционной системы), а также программные и аппаратные средства связи компьютеров.

Разделение локальных ресурсов каждого компьютера между всеми пользователями сети достигается с помощью программных модулей двух типов: *клиентов,* которые формируют запросы на доступ к удаленным компьютерам, и *серверов,* принимающих эти запросы из сети и предоставляющих запрашиваемые ресурсы. Несколько клиентов могут обращаться к одному серверу. Набор модулей «клиент-сервер» представляет собой распределенную программу, реализующую сетевую службу.

Термины «клиент» и «сервер» используются для обозначения не только программных модулей, но и компьютеров, подключенных к сети. Если компьютер предоставляет свои ресурсы другим компьютерам сети, то он называется сервером, а если он их потребляет – клиентом. Иногда один и тот же компьютер может одновременно играть роли и сервера, и клиента.

Контрольные вопросы к главе 3

1. Что такое компьютерная сеть?
2. Дайте классификацию сетей по широте охвата.
3. Что такое пропускная способность сети, в каких единицах она измеряется?
4. Назовите основные цели построения компьютерных сетей.
5. Что такое клиент-серверная модель?
6. Почему глобальные сети появились раньше локальных?
7. В чем заключались главные отличия первых глобальных и локальных сетей?

8. Каковы основные тенденции сближения локальных и глобальных сетей?
9. В чем заключаются отличия мультипроцессорного компьютера от однопроцессорного?
10. В чем заключается различие между многопроцессорным компьютером и кластером?

ГЛАВА 4

ОБЩИЕ ПРИНЦИПЫ ПОСТРОЕНИЯ СЕТЕЙ

4.1. Связь двух узлов

Основные принципы взаимодействия компьютеров в сети во многом позаимствованы от схемы взаимодействия компьютера с периферийными устройствами. Фактически эта схема является прообразом сетей. Связь двух устройств физическим каналом (например, компьютер и периферийное устройство) является простейшим случаем соединения, называемым связью точка-точка. Для обмена данными между компьютером и периферийным устройством (ПУ) в компьютере предусмотрен интерфейс, который представляет собой физический канал (провода, соединяющие компьютер и ПУ) и правила обмена информацией по каналу. В качестве примера стандартных интерфейсов можно привести параллельный интерфейс Centronics (как правило, для связи с принтерами) и последовательный порт RS232C (для подключения мониторов, манипуляторов «мышь» и других устройств). Принципиальная схема такого соединения представлена на рис. 4.1.

Со стороны компьютера интерфейс состоит из контроллера ПУ (аппаратная часть) и драйвера соответствующего ПУ (программная часть). Со стороны ПУ интерфейс реализуется аппаратным (иногда аппаратно-программным) устройством управления (УУ). Интерфейс в основном является двунаправленным и передает не только данные (например, печатаемую на принтер информацию), но и команды управления для ПУ.

Приложение, которому требуется передать некоторые данные на периферийное устройство, обращается с запросом на выпол-

нение операции ввода-вывода к операционной системе. В запросе указываются: адрес данных в оперативной памяти, идентифицирующая информация о периферийном устройстве и операция, которую надо выполнить. Получив запрос, операционная система запускает соответствующий драйвер, передавая ему в качестве параметра адрес выводимых данных. Дальнейшие действия по выполнению операции ввода-вывода со стороны компьютера реализуются совместно драйвером и контроллером ПУ. Контроллер работает под управлением драйвера. Контроллеры ПУ принимают команды и данные от драйвера в свой внутренний буфер, который часто называется регистром, или портом, а затем производят необходимые преобразования данных и команд, полученных от драйвера, в соответствии с форматами, понятными устройству управления ПУ, и выдают их на внешний интерфейс.

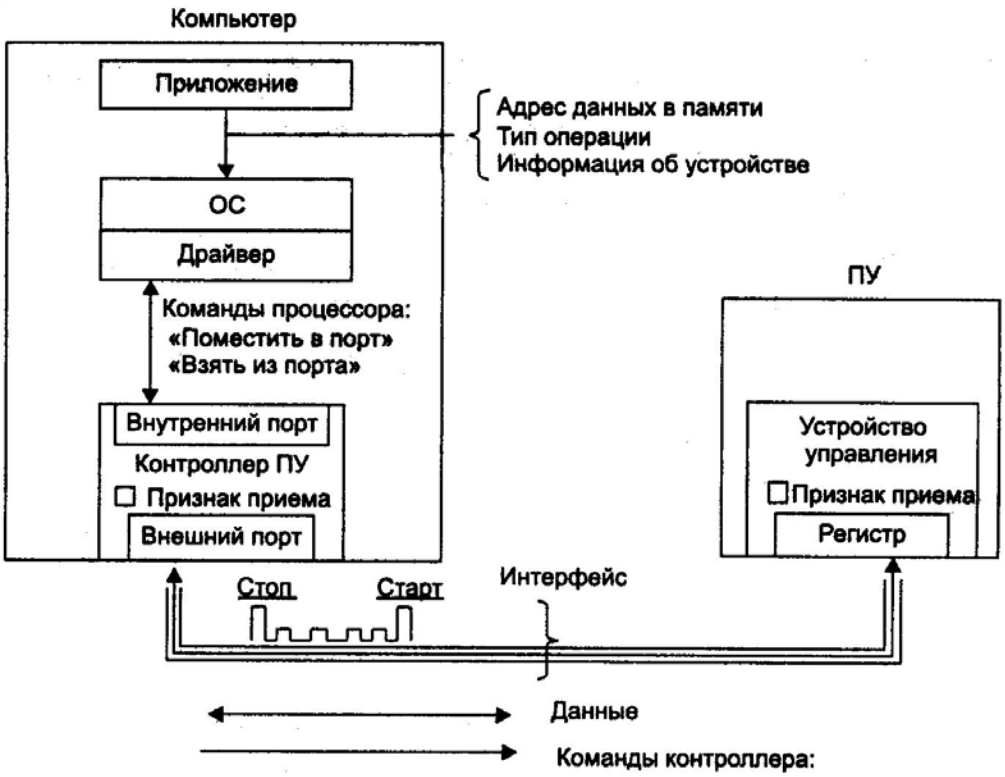


Рис. 4.1. Схема связи компьютера с периферийным устройством

Информация к ПУ передается байтами, которые последовательно загружаются драйвером в контроллер ПУ. Контроллер последовательно передает каждый бит в виде электрического сигнала по линии связи. Чтобы устройству управления ПУ стало понятно, что начинается передача байта, перед передачей первого

бита информации контроллер ПУ формирует стартовый сигнал специфической формы, а после передачи последнего информационного бита – стоповый сигнал. Эти сигналы *синхронизируют* передачу байта.

Кроме информационных битов, контроллер может передавать бит контроля четности для повышения достоверности обмена. Устройство управления, обнаружив на соответствующей линии стартовый бит, выполняет подготовительные действия и начинает принимать информационные биты, формируя из них байт в своем приемном буфере. Если передача сопровождается битом четности, то выполняется проверка правильности передачи: при правильно выполненной передаче в соответствующем регистре устройства управления устанавливается признак завершения приема информации.

Аналогичным способом организуется простейшая связь двух компьютеров. В отличие от предыдущего случая, когда программа (приложение) работает только с одной стороны (на компьютере), в этом случае передача информации происходит при взаимодействии программ на двух соединенных компьютерах. Программа одного компьютера с помощью соответствующих сообщений обращается к программе на другом компьютере с просьбой выполнить некоторые действия. На рис. 4.2. представлена простейшая схема взаимодействия двух компьютеров при выполнении запроса компьютера А прочитать файл, расположенный на диске компьютера В. Для примера предполагается, что компьютеры А и В связаны через COM-порты с помощью интерфейса RS-232C.

Драйвер COM-порта вместе с контроллером COM-порта работают примерно так же, как и в описанном выше случае взаимодействия ПУ с компьютером. Однако при этом роль устройства управления ПУ выполняют контроллер и драйвер COM-порта другого компьютера. Вместе они обеспечивают передачу по кабелю между компьютерами одного байта информации. (В «настоящих» локальных сетях подобные функции передачи данных в линию связи выполняются сетевыми адаптерами и их драйверами). Таким образом, в распоряжении программ компьютеров А и В имеется средство для побайтового обмена данными.

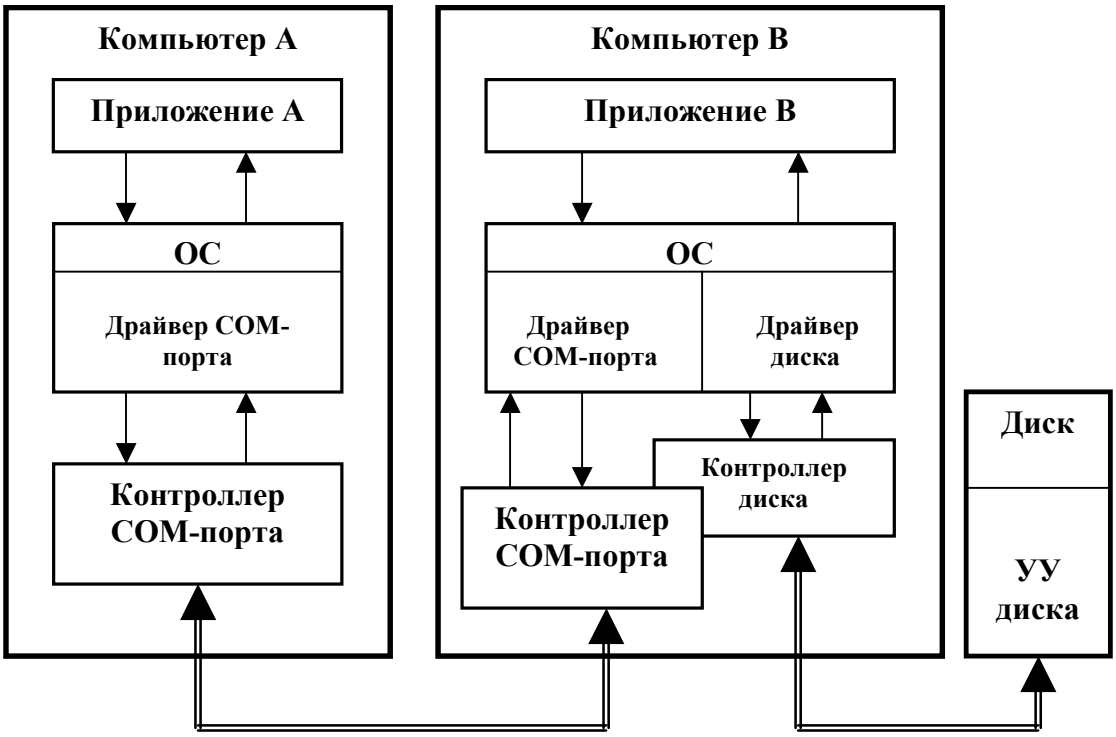


Рис. 4.2. Схема взаимодействия двух компьютеров

Однако рассматриваемая в нашем примере задача значительно сложнее, так как, во-первых, нужно получить из удаленного компьютера не отдельный байт, а файл, во-вторых, эти данные находятся не в оперативной памяти этого компьютера, а на его периферийном устройстве. Все связанные с этим дополнительные проблемы должны решить программы более высокого, чем драйверы COM-портов, уровня (приложение А и приложение В). Приложение А должно сформировать сообщение-запрос для приложения В, в котором необходимо указать имя файла и другую информацию. Этот запрос передается к приложению В через драйверы и COM-порты. Приложение В, получив сообщение, обращается к периферийному устройству, в данном случае диску, в соответствии с рассмотренной ранее схемой «локальная ОС – драйвер диска – контроллер диска – устройство управления диска». Считанные с диска данные приложение В с помощью драйвера COM-порта передает по каналу связи в компьютер А, где они и попадают к приложению А.

В сетевых операционных системах для обслуживания запросов к удаленным компьютерам и получения результатов существуют специальные программные модули, реализующие функции «клиента» и «сервера».

Кроме рассмотренных выше проблем связи компьютеров в сеть существует ряд проблем, связанных с физической передачей сигналов по линиям связи. Двоичный код (0 и 1), используемый в компьютерах для представления данных, преобразуется в соответствующие электрические или оптические сигналы (кодирование). При передаче информации по линиям связи резко увеличиваются расстояния и соответственно увеличиваются помехи. Поэтому кроме кодирования сигналов в сетях применяются методы модуляции сигналов (представление сигнала в виде синусоиды). Кроме того, встает проблема синхронизации передатчика и приемника. Для передачи данных в сетях используют специальные сетевые адаптеры, рассчитанные на конкретные передающие среды (коаксиальный кабель, витая пара, оптоволокно и т. п.) и учитывающие их электрические и иные характеристики. Кроме того, для повышения надежности передачи используется прием подсчета контрольной суммы после передачи блоков информации.

Выводы:

Наиболее простым случаем связи двух устройств является их непосредственное соединение физическим каналом, такое соединение называется связью «точка-точка» (point-to point).

Для обмена данными с внешними устройствами (как с собственной периферией, так и с другими компьютерами) в компьютере предусмотрены *интерфейсы*, или *порты*, то есть наборы проводов, соединяющих компьютер с устройствами, а также наборы правил обмена информацией по этим проводам.

Логикой передачи сигналов на внешний интерфейс управляют аппаратное устройство компьютера – *контроллер* и программный модуль – *драйвер*.

Для того чтобы компьютер мог работать в сети, его операционная система должна быть дополнена клиентским и/или серверным модулем, а также средствами передачи данных между компьютерами. В результате такого добавления операционная система компьютера становится *сетевой*.

При соединении «точка-точка» на первый план выходит задача физической передачи данных по линиям связи. Эта задача среди прочего включает *кодирование* и *модуляцию* данных, взаимную *синхронизацию* передатчика одного компьютера с приемни-

ком другого, а также подсчет *контрольной суммы* и передачу ее по линиям связи после каждого байта или после некоторого блока байтов.

4.2. Топология физических связей

Как только компьютеров становится больше двух, появляется проблема выбора конфигурации физических связей, или *топологии*. Под топологией сети понимается конфигурация графа, вершинам которого соответствуют конечные узлы сети (например, компьютеры) и коммуникационное оборудование (например, маршрутизаторы), а ребрам – электрические и информационные связи между ними.

Число возможных вариантов конфигураций резко возрастает при увеличении числа связываемых устройств. Так, если три компьютера мы можем связать двумя способами (рис. 4.3, а), то для четырех компьютеров можно предложить уже шесть топологически разных конфигураций, что и иллюстрирует рис. 4.3 б.

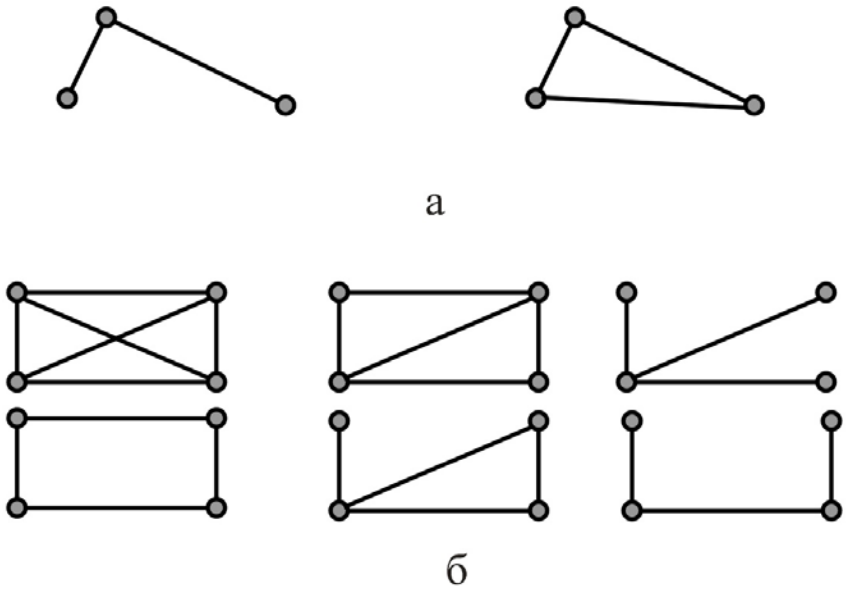


Рис. 4.3. Варианты соединений узлов сети

Мы можем соединять каждый компьютер с каждым или же связывать их последовательно, предполагая, что они будут общаться, передавая сообщения друг другу «транзитом». От выбора топологии связей существенно зависят многие характеристики сети. Например, наличие между узлами нескольких путей повы-

шает надежность сети и делает возможным балансировку загрузки отдельных каналов. Простота присоединения новых узлов, свойственная некоторым топологиям, делает сеть легко расширяемой. Экономические соображения часто приводят к выбору топологий, для которых характерна минимальная суммарная длина линий связи.

Среди множества возможных конфигураций различают полносвязные и неполносвязные.

Полносвязная топология (в виде графа представлена на рис. 4.4, а) соответствует сети, в которой каждый компьютер непосредственно связан со всеми остальными. Несмотря на логическую простоту, этот вариант оказывается громоздким и неэффективным. Действительно, в таком случае каждый компьютер в сети должен иметь большое количество коммуникационных портов, достаточное для связи с каждым из остальных компьютеров сети. Для каждой пары компьютеров должна быть выделена отдельная физическая линия связи. Полносвязные топологии в крупных сетях применяются редко, так как из теории графов известно, что для связи N узлов требуется $N\ (N–1)/2$ физических линий связи, то есть имеет место квадратичная зависимость. Чаще этот вид топологии используется в многомашинных комплексах или в сетях, объединяющих небольшое количество компьютеров.

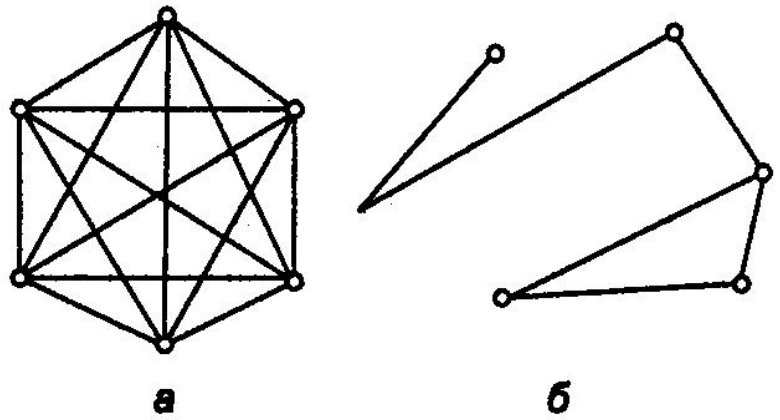


Рис. 4.4. Полносвязная (а) и неполнозвязная (б) топологии

Все другие варианты основаны на *неполносвязных* топологиях, когда для обмена данными между двумя компьютерами может

потребоваться промежуточная передача данных через другие узлы сети.

Ячеистая топология получается из полносвязной путем удаления некоторых возможных связей (рис. 4.4, б). Ячеистая топология допускает соединение большого количества компьютеров и характерна, как правило, для крупных сетей.

В топологии *общая шина* (рис. 4.5, а) в качестве центрального элемента выступает пассивный кабель, к которому по схеме «монтажного ИЛИ» подключается несколько компьютеров (такую же топологию имеют многие сети, использующие беспроводную связь – роль общей шины здесь играет общая радиосреда). Передаваемая информация распространяется по кабелю и доступна одновременно всем компьютерам, присоединенным к этому кабелю. Основными преимуществами такой схемы являются ее дешевизна и простота наращивания – то есть присоединения новых узлов к сети. Самый серьезный недостаток общей шины заключается в ее низкой надежности: любой дефект кабеля или какого-нибудь из многочисленных разъемов полностью парализует всю сеть. Другим недостатком общей шины является ее невысокая производительность, так как при таком способе подключения в каждый момент времени только один компьютер может передавать данные по сети, поэтому пропускная способность канала связи всегда делится здесь между всеми узлами сети. До недавнего времени общая шина являлась одной из самых популярных топологий для локальных сетей и поддерживается технологиями ARCNET и ETHERNET.

Топология *звезда* (рис. 4.5, б) образуется в случае, когда каждый компьютер подключается отдельным кабелем к общему центральному устройству, называемому *концентратором.* В функции концентратора входит направление передаваемой компьютером информации одному или всем остальным компьютерам сети. В качестве концентратора может выступать как компьютер, так и специализированное устройство, такое как многовходовый повторитель, коммутатор или маршрутизатор. К недостаткам топологии типа звезда относится более высокая стоимость сетевого оборудования из-за необходимости приобретения специализированного центрального устройства. Кроме того, возможности по наращиванию количества узлов в сети ограничиваются количест-

вом портов концентратора. Топология звезда поддерживается технологией Ethernet.

В сетях с *кольцевой* конфигурацией (рис. 4.5, в) данные передаются по кольцу от одного компьютера к другому. Главным достоинством кольца является то; что оно по своей природе обладает свойством резервирования связей. Действительно, любая пара узлов соединена здесь двумя путями – по часовой стрелке и против нее. Кольцо представляет собой очень удобную конфигурацию и для организации обратной связи – данные, сделав полный оборот, возвращаются к источнику. Кольцевую топологию поддерживают технологии Token Ring и FDDI.

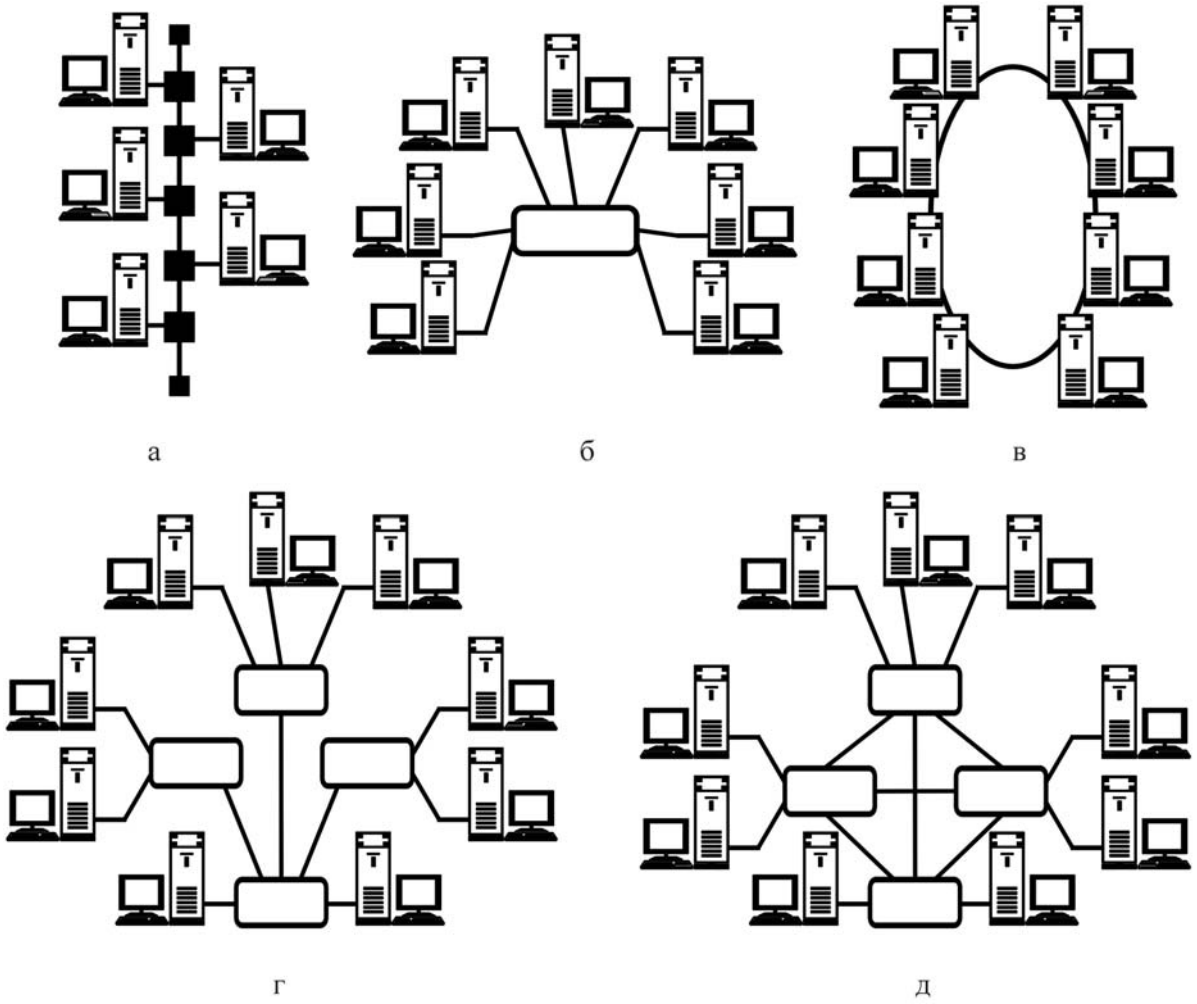


Рис. 4.5. Топологии: а – общая шина, б – звезда, в – кольцо, г – дерево, д – сетка

Иногда имеет смысл строить сеть с использованием нескольких концентраторов, иерархически соединенных между собой связями типа звезда (рис. 4.5, г). Получаемую в результате струк-

туру называют также *деревом*. В настоящее время дерево является самым распространенным типом топологии связей, как в локальных, так и глобальных сетях. Добавлением некоторых связей в топологию типа дерево получается топология *сетка* (рис.4.5, д).

В то время как небольшие сети, как правило, имеют типовую топологию – звезда, кольцо или общая шина, для крупных сетей характерно наличие произвольных связей между компьютерами.

В таких сетях можно выделить отдельные, произвольно связанные фрагменты (подсети), имеющие типовую топологию, поэтому их называют сетями со *смешанной топологией* (рис. 4.6).

На практике различают *физическую топологию*, определяющую правила физических соединений узлов (прокладку кабелей), и *логическую топологию*, определяющую направление потоков данных между узлами сети. Логические связи представляют собой маршруты передачи данных между узлами сети и образуются путем соответствующей настройки коммуникационного оборудования. Логическая и физическая топологии сети относительно независимы друг от друга и в общем случае не совпадают. Крупные сети практически никогда не строятся без логической структуризации. Логическая структуризация сети направлена на повышение производительности и безопасности сети. Средствами логической структуризации служат такие коммуникационные устройства, как мосты, коммутаторы, маршрутизаторы.

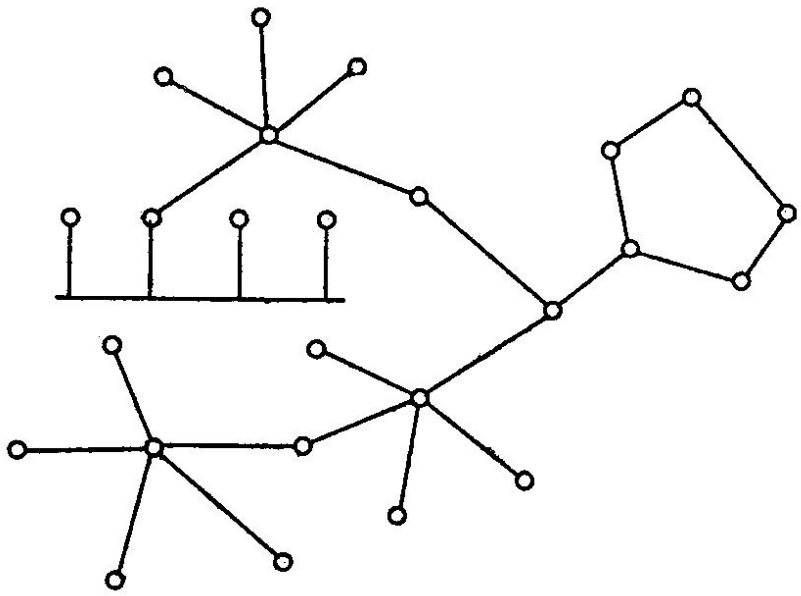


Рис. 4.6. Смешанная топология

4.3. Классификация топологических элементов сетей

Информационные сети состоят из конечных устройств и промежуточных устройств, соединенных кабельной системой. Определим некоторые основные понятия.

Узлы сети – конечные и промежуточные устройства, наделенные сетевыми адресами. К узлам сети относятся компьютеры с сетевым интерфейсом, выступающие в роли рабочих станций, серверов или в обеих ролях; сетевые периферийные устройства (принтеры, плоттеры, сканеры); сетевые телекоммуникационные устройства (модемные пулы, модемы коллективного использования); маршрутизаторы.

Кабельный сегмент – отрезок кабеля или цепочка отрезков кабелей, электрически (оптически) соединенных друг с другом, обеспечивающие соединение двух или более узлов сети.

Сегмент сети (или просто сегмент) – совокупность узлов сети, использующих общую (разделяемую) среду передачи. Применительно к технологии Ethernet это совокупность узлов, подключенных к одному коаксиальному кабельному сегменту, применительно к Token Ring это одно кольцо.

Сеть – совокупность узлов сети, имеющих единую систему адресации. Примерами могут быть IPX-сеть, IP-сеть. Каждая сеть имеет свой собственный адрес, этими адресами оперируют маршрутизаторы для передачи пакетов между сетями. Сеть может быть разбита на подсети. Сеть может состоять из множества сегментов, причем один и тот же сегмент может входить в несколько разных сетей.

По способу использования кабельных сегментов различают:

Двухточечные соединения (point-to-point connection) – между двумя узлами. Для таких соединений в основном используются симметричные электрические (витая пара) и оптические кабели.

Многоточечные соединения (multi point connection) – к одному кабельному сегменту подключается более двух узлов. Типичная среда передачи – несимметричный электрический кабель (коаксиальный кабель), возможно применение и других кабелей, в том

числе и оптических. Соединение устройств отрезками кабеля друг за другом называется цепочечным.

Связь между конечными узлами, подключенными к различным кабельным и логическим сегментам, обеспечивается промежуточными системами – *активными коммуникационными устройствами*. Эти устройства имеют не менее двух портов (интерфейсов). Эти устройства классифицируются следующим образом:

Повторитель (repeater) – устройство, позволяющее преодолевать топологические ограничения (длины) кабельных сегментов. Информация из одного кабельного сегмента в другой передается *побитно*, анализ информации не производится.

Мост (bridge) – средство объединения сегментов сетей, обеспечивающее передачу информации из одного сегмента в другой (другие). Информация, пришедшая из одного сегмента, может быть передана в другой или отфильтрована.

Мост MAC-подуровня (MAC Bridge) позволяет объединять сегменты сети в пределах одной технологии.

Мост LLC-подуровня (LLC Bridge), он же транслирующий мост, позволяет объединять сегменты сетей и с разными технологиями (например, Ethernet – Fast Ethernet, Ethernet – Token Ring, Ethernet – FDDI).

Коммутатор (switch) выполняет функции, аналогичные функциям мостов, но используется для *сегментации* – разбиения сетей на мелкие сегменты с целью повышения пропускной способности.

Маршрутизатор (router) используется для передачи *пакетов* между сетями. В отличие от повторителей и мостов/коммутаторов, присутствие маршрутизатора известно узлам сетей, подключенных к его интерфейсам. Каждый порт маршрутизатора имеет свой сетевой адрес, на этот адрес узлы посылают пакеты, предназначенные узлам других сетей. С другой стороны, маршрутизатор, анализируя адрес назначения пакета, направляет его на свой соответствующий порт для дальнейшей его доставки в нужную сеть. При определенных условиях маршрутизатор может отбросить (уничтожить) пакет данных. Это зависит от результатов анализа информации, содержащейся в заголовке пакета.

4.4. Адресация узлов, маршрутизация

При объединении в сеть более двух компьютеров возникает проблема их адресации (адрес узла сети или адрес сетевого интерфейса). Адреса могут быть числовыми (например, 165.22.255.255) или символьными (например, ssu.samara.ru). Адреса могут использоваться для идентификации не только конкретных узлов, но и групп узлов (групповые адреса). С помощью групповых адресов данные могут направляться сразу нескольким узлам (широковещательные адреса). Множество адресов, допустимых в рамках некоторой схемы адресации называется адресным пространством. Адресное пространство может иметь плоскую или иерархическую организацию. В первом случае адреса не структурированы. При иерархической схеме адреса организованы в виде вложенных друг в друга подгрупп, последовательно сужая область вплоть до конкретного узла. Примером такой адресации служит обычный почтовый адрес: страна, город, улица и т. д. Иерархическая система позволяет при перемещении информации по сети до определенного момента пользоваться только старшей составляющей, затем следующей частью вплоть до самой младшей.

К адресу сетевого интерфейса можно предъявить следующие требования:

– адрес должен уникально идентифицировать сетевой интерфейс в сети любого масштаба;

– схема назначения адресов должна сводить к минимуму ручной труд администратора и вероятность дублирования адресов;

– желательно, чтобы адрес имел иерархическую структуру, удобную для построения больших сетей;

– адрес должен быть удобен для пользователей сети, а это значит, что он должен допускать символьное представление, например Server3;

– адрес должен быть по возможности компактным, чтобы не перегружать память коммуникационной аппаратуры – сетевых адаптеров, маршрутизаторов и т.п.

Нетрудно заметить, что эти требования противоречивы – например, адрес, имеющий иерархическую структуру, скорее всего,

будет менее компактным, чем плоский. Символьные имена удобны для людей, но из-за переменного формата и потенциально большой длины их передача по сети не очень экономична. Так как все перечисленные требования трудно совместить в рамках какой-либо одной схемы адресации, на практике обычно используется сразу несколько схем, так что сетевой интерфейс компьютера может одновременно иметь несколько адресов-имен. Каждый адрес задействуется в той ситуации, когда соответствующий вид адресации наиболее удобен. А для преобразования адресов из одного вида в другой используются специальные вспомогательные протоколы, которые называют иногда *протоколами разрешения адресов* (address resolution protocols).

Примером плоского числового адреса является *MAC-адрес*, предназначенный для однозначной идентификации сетевых интерфейсов в локальных сетях. Такой адрес обычно используется только аппаратурой, поэтому его стараются сделать по возможности компактным и записывают в виде двоичного или шестнадцатеричного значения, например 0081005e24a8. При задании MAC-адресов не требуется выполнение ручной работы, так как они обычно встраиваются в аппаратуру компанией-изготовителем, поэтому их называют также *аппаратными* (hardware) *адресами*. Использование плоских адресов является жестким решением – при замене аппаратуры, например, сетевого адаптера, изменяется и адрес сетевого интерфейса компьютера.

Типичным представителем иерархической схемы являются IP-адреса и доменные адреса в сети Интернет. IP-адрес любого узла сети поддерживает двухуровневую иерархию и делится на старшую часть (номер сети) и младшую часть (номер узла). При написании IP-адрес состоит из четырех чисел в диапазоне 0–255, разделяемых точками. Такое деление позволяет передавать сообщения между сетями только на основании номера сети, а номер узла используется после доставки сообщения в нужную сеть. Конечному пользователю применять такую систему из четырех чисел неудобно. Для этих целей принята символьная адресация, построенная по иерархическому доменному принципу.

Символьные адреса или имена предназначены для запоминания людьми и поэтому обычно несут смысловую нагрузку. Например, адрес www.ssu.samara.ru означает:

– “ru” – имя домена верхнего уровня (в сети Интернет это Россия). Он регистрируется в организации Internet NIC (Network Information Center). Внутри этого домена может содержаться сколько угодно узлов и доменов, каждый из которых имеет свое имя;

– “samara” – домен внутри домена “ru”;

– “ssu” – домен внутри домена samara;

– “www” – узел внутри домена ssu (WEB-сервер).

В каждом домене имеется свой DNS-сервер, который хранит таблицу соответствия символических имен и IP-адресов.

Если топология сети неполносвязная, то обмен данными между парой узлов должен идти в общем случае через транзитные (промежуточные) узлы. Последовательность транзитных узлов на пути от отправителя к получателю называется *маршрутом*. Задача соединения конечных узлов через транзитные узлы называется задачей маршрутизации.

Основными целями маршрутизации являются обеспечение:

– минимальной задержки пакета при его передаче от узла отправителя к адресату;

– максимальной пропускной способности сети;

– максимальной защиты пакета от угроз безопасности;

– надежности доставки пакета адресату;

– оптимизации стоимости передачи пакета между узлами сети.

Понятно, что через один транзитный узел может проходить несколько маршрутов. Транзитный узел должен уметь распознавать потоки данных, которые на него поступают, для того чтобы отрабатывать их передачу именно на тот свой интерфейс, который ведет к нужному узлу.

Информационным потоком, или *потоком данных*, называют непрерывную последовательность байтов (которые могут быть объединены в более крупные единицы данных – пакеты, кадры, ячейки), объединенных набором общих признаков, выделяющих его из общего сетевого трафика. Например, все данные, поступающие от одного компьютера, можно определить как единый поток, а можно представить их как совокупность нескольких подпотоков, каждый из которых в качестве дополнительного признака имеет адрес назначения. Каждый же из этих подпотоков, в свою очередь, можно разделить на подпотоки данных, относя-

щихся к разным сетевым приложениям – электронной почте, копированию файлов, обращению к web-серверу. В качестве обязательного признака при коммутации выступает адрес назначения данных, поэтому весь поток входящих в транзитный узел данных, должен разделяться как минимум на подпотоки, имеющие различные адреса назначения. Тогда каждой паре конечных узлов будет соответствовать один поток и один маршрут.

Однако поток данных между двумя конечными узлами в общем случае может быть представлен несколькими разными потоками, причем для каждого из них может быть проложен свой особый маршрут. Действительно, на одной и той же паре конечных узлов может выполняться несколько взаимодействующих по сети приложений, которые предъявляют к ней свои особые требования. В таком случае выбор пути должен осуществляться с учетом характера передаваемых данных, например, для файлового сервера важно, чтобы передаваемые им большие объемы данных направлялись по каналам, обладающим высокой пропускной способностью.

Определение пути – сложная задача, особенно когда конфигурация сети такова, что между парой взаимодействующих сетевых интерфейсов существует множество путей. Выбор останавливают на одном *оптимальном* по некоторому критерию маршруте. В качестве критериев оптимальности могут выступать, например, номинальная пропускная способность; загруженность каналов связи; задержки, вносимые каналами; количество промежуточных транзитных узлов; надежность каналов и транзитных узлов.

Маршрут может определяться эмпирически («вручную») администратором сети, который, анализирует топологию сети и определяет последовательность интерфейсов, которую должны пройти данные, чтобы достичь получателя. Среди побудительных мотивов выбора того или иного пути могут быть: особые требования к сети со стороны различных типов приложений, решение передавать трафик через сеть определенного поставщика услуг, предположения о пиковых нагрузках на некоторые каналы сети, соображения безопасности. Однако эвристический подход к определению маршрутов мало пригоден для большой сети со сложной топологией.

Задача маршрутизации решается чаще всего автоматически с помощью соответствующего программного обеспечения, реализующего некоторый алгоритм маршрутизации. Алгоритм маршрутизации – это правило назначения выходной линии связи узла сети для передачи пакета, базирующееся на информации, содержащейся в заголовке пакета.

Однако даже оптимальные алгоритмы не всегда эффективны на практике. Топология сети может постоянно изменяться в результате отказов узлов и линий связи и при развитии сети (подключении новых узлов и линий связи). Наиболее динамичным фактором является нагрузка на линии связи, изменяющаяся довольно быстро и в трудно прогнозируемом направлении. Для выбора оптимального маршрута каждый узел связи должен располагать информацией о состоянии сети в целом. Узлы сети имеют данные о текущей топологии сети и пропускной способности линий связи. Однако нет возможности точно предсказать состояние нагрузки в сети на ближайшее время. Поэтому при решении задачи маршрутизации могут использоваться данные о состоянии нагрузки, запаздывающие по отношению к моменту принятия решения о направлении передачи пакетов. Следовательно, во всех случаях алгоритмы маршрутизации выполняются в условиях неопределенности текущего и будущего состояний сети.

Эффективность алгоритмов маршрутизации оценивается следующими показателями:

– временем доставки пакетов адресату;

– нагрузкой на сеть, которая создается при реализации данного алгоритма за счет передачи служебной информации (таблиц маршрутизации, сведений о топологии и загрузке узлов и линий связи и т.п.);

– затратами ресурсов коммуникационных узлов сети (время на обработку пакетов, емкости памяти, вычислительной мощности).

Различают следующие способы маршрутизации.

1. **Централизованная маршрутизация.** Выбор маршрута для каждого пакета осуществляется в центре управления сетью, а узлы сети только реализуют результаты решения задачи маршрутизации. Существенным недостатком такого способа маршрутизации является полная зависимость от центрального узла, и в случае его отказа сеть может быть парализована.

2. **Распределенная маршрутизация.** Функции управления маршрутизацией распределены между узлами сети, которые располагают для этого соответствующими аппаратно-программными средствами. Распределенная маршрутизация отличается большей гибкостью и надежностью.

3. **Смешанная маршрутизация** характеризуется тем, что в ней реализованы принципы централизованной и распределенной маршрутизации.

Различают три вида маршрутизации: *простую, фиксированную и адаптивную*. Принципиальная разница между ними заключается в степени учета изменения топологии и нагрузки сети при решении задачи выбора маршрута.

Простая маршрутизация отличается тем, что при выборе маршрута не учитывается ни изменение топологии сети, ни изменение нагрузки ее узлов. Она имеет низкую эффективность, но отличается простотой реализации алгоритма маршрутизации и устойчивой работой сети при выходе из строя отдельных элементов (узлов и линий связи). Разновидностями этого вида маршрутизации являются *случайная и лавинная маршрутизации*.

Случайная маршрутизация характеризуется тем, что для передачи пакета из узла сети выбирается одно из возможных случайно выбранных направлений. При этом виде маршрутизации не обеспечивается оптимальное время доставки пакета и эффективное использование пропускной способности сети.

Лавинная маршрутизация предусматривает передачу пакета из узла по всем свободным выходным линиям. Поскольку это происходит в каждом узле, имеет место явление «размножения» пакета, что резко ухудшает использование пропускной способности сети. Основным преимуществом такого метода является гарантированное обеспечение оптимального времени доставки пакета адресату, так как из всех направлений, по которым передается пакет, хотя бы одно обеспечивает такое время.

Фиксированная маршрутизация характеризуется тем, что при выборе маршрута учитывается изменение топологии сети и не учитывается изменение ее нагрузки. Маршрут до каждого узла сети выбирается по таблице, определяющей кратчайшие пути. Отсутствие адаптации к изменению нагрузки приводит к задерж-

кам пакетов в сети. Фиксированная маршрутизация применяется в сетях с мало изменяющейся топологией и установившимися потоками пакетов.

Адаптивная маршрутизация отличается тем, что выбор маршрута передачи пакетов осуществляется с учетом изменения как топологии, так и нагрузки сети. Существуют несколько модификаций адаптивной маршрутизации, различающихся тем, какая именно информация используется при выборе маршрута. Получили распространение такие модификации, как *локальная, распределенная, централизованная и гибридная* адаптивные маршрутизации.

Локальная адаптивная маршрутизация основана на использовании информации, имеющейся в данном узле: таблица возможных маршрутов, данные о состоянии выходных линий связи (работают или не работают), длину очереди пакетов. Информация о состоянии других узлов связи не используется. Таблица маршрутов определяет кратчайшие маршруты, обеспечивающие доставку пакета адресату за минимальное время. Преимущество такого метода состоит в том, что принятие решения о выборе маршрута производится с использованием самых последних данных о состоянии узла. Недостаток метода заключается в том, что выбор маршрута осуществляется без учета глобального состояния всей сети.

Распределенная адаптивная маршрутизация основана на использовании информации, указанной для локальной маршрутизации, и данных, получаемых от соседних узлов сети. В каждом узле формируется таблица маршрутов ко всем узлам назначения с указанием времени задержки пакетов. До начала работы сети это время оценивается, исходя из топологии сети. В процессе работы сети узлы периодически обмениваются с соседними узлами таблицами задержки, в которых указывается нагрузка (длина очереди пакетов) узла. После обмена таблицами задержки каждый узел производит перерасчет задержки и корректирует маршруты с учетом поступивших данных. Учет состояния соседних узлов при выборе маршрута существенно повышает эффективность алгоритмов маршрутизации, но это достигается за счет увеличения загрузки сети служебной информацией.

Централизованная адаптивная маршрутизация характеризуется тем, что задача маршрутизации для каждого узла сети решается в центре маршрутизации. Каждый узел периодически формирует сообщение о своем состоянии и передает его в центр. По этим данным в центе для каждого узла составляется таблица маршрутов. Передача этих сообщений, формирование и рассылка таблиц маршрутов вызывают временные задержки и снижают эффективность такого метода, особенно при большой пульсации нагрузки в сети. Кроме того, есть опасность потери управления сетью при отказе центра маршрутизации.

Гибридная адаптивная маршрутизация основана на использовании таблиц маршрутов, рассылаемых центром маршрутизации узлам сети, в сочетании с анализом длины очередей в узлах. Следовательно, здесь реализуются принципы централизованной и локальной маршрутизации. Гибридная маршрутизация компенсирует недостатки централизованной и локальной маршрутизации и воспринимает их преимущества: маршруты центра соответствуют глобальному состоянию сети, а учет текущего состояния узла обеспечивает своевременность решения задачи.

4.5. Принципы соединения абонентов сети

После того как маршрут определен, должно произойти соединение (коммутация) абонентов. Устройство, функциональным назначением которого является выполнение коммутации, называется коммутатором. Если коммутаторы выполняют коммутацию на основе иерархических сетевых адресов, то их называют маршрутизаторами. Коммутатор выполняет коммутацию входящих информационных потоков в соответствующие выходные порты. Коммутатором может быть как специальное устройство, так и обычный компьютер со специальным программным обеспечением. Информация о маршрутах записывается в специальные таблицы коммутации.

Во многих случаях (особенно при сложной топологии сети) некоторые узлы сети выделяют специально для коммутации. Совокупность таких узлов и линий связи образуют коммутацион-

ную сеть (подсеть). В общем случае такую подсеть называют магистральной сетью. Пример схемы такой подсети представлен на рис. 4.7.

Комплекс технических решений задачи коммутации является основой любой сетевой технологии. От механизма прокладки маршрутов, продвижения данных по сети и совместного использования каналов связи зависят фундаментальные свойства сети.

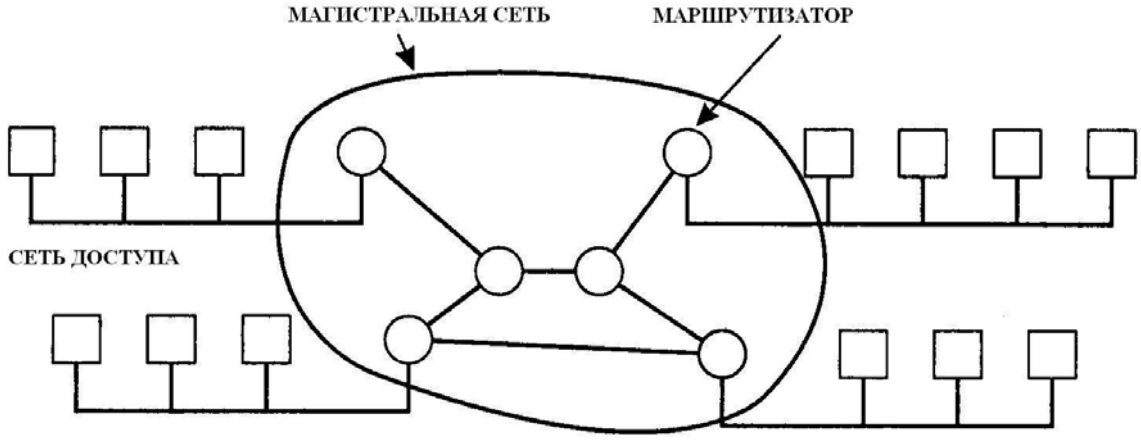


Рис. 4.7. Струтктура телекоммуникационной сети

Узлы коммутации осуществляют один из трех возможных видов коммутации при передаче данных:

– коммутацию каналов;

– коммутацию сообщений;

– коммутацию пакетов.

Сообщения и пакеты часто называют дейтаграммами. Дейтаграмма – это самостоятельный пакет данных (сообщение), содержащий в своем заголовке достаточно информации, чтобы его можно было передать от источника к получателю независимо от всех предыдущих и последующих сообщений.

При коммутации каналов между пунктами отправления и назначения устанавливается непосредственное физическое соединение путем формирования составного канала из последовательно соединенных отдельных участков каналов связи. Такой сквозной физический составной канал организуется в начале сеанса связи, поддерживается в течение всего сеанса и разрывается после окончания передачи. Формирование сквозного канала обеспечивается путем последовательного включения ряда коммутационных устройств в нужное положение постоянно на все время

сеанса связи. Время создания такого канала сравнительно большое, и это один из недостатков этого метода коммутации. Образованный канал недоступен для посторонних абонентов. Монополизация взаимодействующими абонентами подканалов, образующих физический канал, обусловливает снижение общей пропускной способности сети передачи данных. И это притом, что образованный физический канал часто бывает недогружен. Основные достоинства метода: возможность работы и в диалоговом режиме, и в реальном масштабе времени; обеспечение полной прозрачности канала. Применяется этот метод коммутации чаще всего при дуплексной (двухсторонней) передаче аудиоинформации (обычная телефонная связь – типичный пример коммутации каналов).

При коммутации сообщений данные передаются в виде дискретных порций разной длины (сообщений), причем между источником и адресатом сквозной физический канал не устанавливается и ресурсы коммуникационной системы предварительно не распределяются. Отправитель лишь указывает адрес получателя. Узлы коммутации анализируют адрес и текущую занятость каналов и передают сообщение по свободному в данный момент каналу на ближайший узел сети в сторону получателя. В узлах коммутации имеются коммутаторы, управляемые связным процессором, который также обеспечивает временное хранение данных в буферной памяти, контроль достоверности информации и исправление ошибок, преобразование форматов данных, формирование сигналов подтверждения получения сообщения. Ввиду наличия буферной памяти имеется возможность устанавливать согласованную скорость передачи сообщения между двумя узлами. Ввиду этого затруднена работа в диалоговом режиме и в режиме реального времени. Некоторые возможности реализации этих режимов остаются лишь благодаря высокой скорости передачи и возможности выполнять приоритетное обслуживание заявок. Применяется этот вид коммутации в электронной почте, телеконференциях, электронных новостях и т.п.

В современных системах для повышения оперативности, надежности передачи, уменьшения емкости запоминающих устройств узлов коммутации длинные сообщения разделяются на несколько более коротких стандартной длины, называемых па-

кетами. Иногда наоборот, очень короткие сообщения объединяются вместе в пакет. Стандартность размера пакетов обусловливает соответствующую стандартную разрядность оборудования узлов связи и максимальную эффективность его использования. Пакеты могут следовать к получателю даже разными путями и непосредственно перед выдачей абоненту объединяются (разделяются) для формирования законченных сообщений. Этот вид коммутации обеспечивает большую пропускную способность сети и наименьшую задержку при передаче данных.

Недостатком коммутации пакетов является трудность, а иногда и невозможность его использования для систем, работающих в интерактивном режиме и в реальном масштабе времени. Хотя в последние годы в этом направлении достигнут заметный прогресс – активно развиваются технологии Интернет-телефонии. Одно из направлений этой технологии – создание *виртуального канала* для передачи пакетов путем мультиплексирования во времени использования каждого узла коммутации. Временной ресурс порта узла разделяется между несколькими пользователями так, что каждому пользователю отводится постоянно множество минимальных отрезков времени, и создается впечатление непрерывного доступа.

Коммутации сообщений и пакетов относятся к логическим видам коммутации, так как при их использовании формируется лишь логический канал между абонентами. При логической коммутации взаимодействие абонентов выполняется через запоминающее устройство, куда поступают сообщения от всех абонентов, обслуживаемых данным узлом. Каждое сообщение (пакет) имеет адресную часть, определяющую отправителя и получателя; в соответствии с адресом выбирается дальнейший маршрут и передается сообщение из запоминающего устройства узла коммутации. Способ передачи, использующий логическую коммутацию пакетов, часто требует наличия в центре коммутации специальных связных мини- или микрокомпьютеров, осуществляющих прием, хранение, анализ, разбиение, синтез, выбор маршрута и отправку сообщений адресату. Коммутаторы используются в узлах коммутации и в качестве межсетевого и внутрисетевого интерфейса, выполняя функции моста – соединителя нескольких сегментов сети воедино.

4.6. Структура сети

Компьютерная сеть представляет собой комплекс многослойных взаимосвязанных аппаратных и программных средств: компьютеров, коммуникационного оборудования, операционных систем, сетевых приложений.

Любая телекоммуникационная сеть в общем случае состоит из трех компонентов (Рис. 4.7):

– сеть доступа;

– магистральная сеть;

– информационные центры.

Как сеть доступа, так и магистральная, строятся на основе коммутаторов. Каждый коммутатор оснащен некоторым количеством портов, которые соединяются с портами других коммутаторов каналами связи. *Сеть доступа* составляет нижний уровень иерархии телекоммуникационной сети. К этой сети подключаются *конечные узлы* – оборудование, установленное у пользователей (абонентов, клиентов) сети. Основное назначение сети доступа – концентрация информационных потоков, поступающих по многочисленным каналам связи от оборудования пользователей, в сравнительно небольшом количестве узлов магистральной сети. Сеть доступа, как и телекоммуникационная сеть в целом, может состоять из нескольких уровней. Коммутаторы, установленные в узлах нижнего уровня передают ее коммутаторам верхнего уровня, чтобы те, в свою очередь, передали ее коммутаторам магистрали. Количество уровней сети доступа зависит от ее размера, небольшая сеть доступа может состоять из одного уровня, а крупная – из двух-трех. Следующие уровни осуществляют дальнейшую концентрацию трафика, собирая его и мультиплексируя в более скоростные каналы.

Информационные центры сети представляют собой собственные информационные ресурсы сети, на основе которых осуществляется обслуживание пользователей.

Компьютерные сети можно классифицировать по разным признакам. По территориальному признаку сети делятся на локальные и глобальные. Важным признаком классификации является также назначение предоставляемых услуг. Выделим два вида се-

тей: *сети операторов связи* и *корпоративные сети*. Сети операторов связи оказывают общедоступные телекоммуникационные услуги, например, услуги телефонии и доступ в Интернет. Операторы связи должны иметь соответствующие лицензии на право предоставления соответствующих услуг, а также свою или арендованную сетевую инфраструктуру.

Корпоративные сети предоставляют услуги в основном только сотрудникам предприятия, которому принадлежит сеть. Существуют некоторые классификации вычислительных сетей, в которых локальные сети определены как сети, обслуживающие нужды одного предприятия, одной корпорации. Поэтому корпоративные сети относят к особой разновидности локальных сетей, имеющих значительную территорию охвата. Среди таких вычислительных сетей выделяют: сети рабочих групп, сети отделов, сети кампусов.

Сети рабочих групп обычно объединяют ряд компьютеров, работающих под управлением одной операционной среды. В ряду компьютеров часто выделяются специализированные серверы, предназначенные для выполнения функций файлового сервера, сервера печати и т.п.

Сети отделов используются небольшой группой сотрудников предприятия, работающих в одном отделе (отдел кадров, бухгалтерия, и т.п.). Территориально они чаще всего расположены и в одном здании. В отделе может насчитываться до сотни компьютеров. Чаще всего такая сеть имеет несколько выделенных серверов, специализированных для таких ресурсов, как программы-приложения, базы данных, лазерные принтеры и т.д. Главной целью сети отдела является разделение локальных ресурсов, таких как приложения, данные, лазерные принтеры. В этих сетях локализуется большая часть трафика предприятия. Сети отделов обычно создаются на основе какой-либо одной сетевой технологии – Ethernet, Token Ring и не разделяются на подсети. Для такой сети характерен один или максимум два типа операционных систем. Задачи управления сетью на уровне отдела относительно просты: добавление новых пользователей, устранение простых отказов, установка новых узлов и новых версий программного обеспечения.

Сети кампусов получили название от слова *campus* – студенческий городок. Главными особенностями сетей кампусов является то, что они объединяют множество сетей различных отделов одного предприятия в пределах отдельного здания или в пределах одной территории, покрывающей площадь в несколько квадратных километров. Службы такой сети включают взаимодействие между сетями отделов, доступ к общим базам данных предприятия, доступ к общим высокоскоростным принтерам. Основное назначение этих сетей – обеспечить взаимодействие между сетями отделов и рабочих групп и создать доступ к корпоративным базам данных независимо от того, на каких типах компьютеров они располагаются и другим дорогостоящим сетевым ресурсам. Именно на уровне сети кампуса возникают проблемы интеграции неоднородного аппаратного и программного обеспечения. Типы компьютеров, сетевых операционных систем, сетевого аппаратного обеспечения могут отличаться в каждом отделе. Отсюда вытекают сложности управления сетями кампусов. Администраторы должны быть в этом случае более квалифицированными, а средства оперативного управления сетью – более совершенными.

Корпоративные сети – сети масштаба всего предприятия, корпорации. Они могут охватывать большие территории, вплоть до работы на нескольких континентах. Ввиду высокой стоимости индивидуальных выделенных коммуникаций и плохой защищенности от несанкционированного доступа коммутируемых каналов связи они чаще всего используют коммуникационные возможности Интернета, и поэтому территориальное размещение для таких сетей роли не играет. Число пользователей и компьютеров может измеряться тысячами, а число серверов – сотнями, расстояния между сетями отдельных территорий могут оказаться такими, что использование глобальных связей становится необходимым. Для соединения удаленных локальных сетей и отдельных компьютеров в корпоративной сети применяются разнообразные телекоммуникационные средства, в том числе телефонные каналы, радиоканалы, спутниковая связь. Непременным атрибутом такой сложной и крупномасштабной сети является высокая степень неоднородности (гетерогенности) – нельзя удовлетворить потребности тысяч пользователей с помощью однотипных программных и аппаратных средств. В корпоративной сети обязательно ис-

пользуются различные типы компьютеров – от мэйнфреймов до персоналок, несколько типов операционных систем и множество различных приложений.

В качестве иллюстрации примеров сетей можно привести схему корпоративной сети Самарского государственного университета. На рис. 4.8. изображена сеть управления бухгалтерского учета и финансового контроля (УБУиФК), которая является по приведенной выше классификации сетью отдела и имеет сети рабочих групп. Все рабочие станции сотрудников УБУиФК подключены через этажный концентратор и имею выход к главному файл-серверу, серверу баз данных, серверу приложений, а также к почтовому серверу и WWW-серверу. Компьютеры финансового, расчетного и материального отдела объединены в рабочие группы и имеют общие принтеры, к которым имеется доступ с разных рабочих станций. Расчетный отдел имеет, кроме того, общие дисковые накопители.

Рис. 4.8. Пример сети отдела

На рис. 4.9. представлена схема корпоративной сети университета и сети кампуса (группы зданий на ул. Потапова и ул. Ака-

демика Павлова). Между корпусами (зданиями) университета проложены оптоволоконные линии связи, а также один (резервный) радиоканал. Университет также имеет свой оптоволоконный канал связи до междугородней телефонной станции для подключения к глобальным сетям. Удаленный корпус на ул. Некрасова, филиал университета в г. Тольятти и представительства в городах Сызрань и Похвистнево имеют доступ к корпоративной информации университета по сети Интернет.

На рисунке 4.10. представлена принципиальная схема центрального коммуникационного узла университета, расположенного в одном из зданий на ул. Академика Павлова. В этот узел сосредоточены все коммуникации, средства управления сетью и основные корпоративные сервера. На рисунке 4.11 в качестве примера представлена принципиальная схема одного из зданий кампуса (корпус на ул. Потапова).

4.7. Требования к компьютерным сетям

Главным требованием, предъявляемым к сетям, является выполнение сетью того набора услуг, для оказания которых она предназначена. Все остальные требования – производительность, надежность, совместимость, управляемость, защищенность, расширяемость и масштабируемость – связаны с качеством выполнения этой основной задачи.

К основным характеристикам производительности сети относятся: *время реакции, пропускная способность* и *задержка передачи*. Время реакции определяется как время между возникновением запроса к какому-либо сетевому сервису и получением ответа на него. Пропускная способность отражает объем данных, переданных сетью в единицу времени. Задержка передачи равна интервалу между моментом поступления пакета на вход какого-либо сетевого устройства и моментом его появления на выходе этого устройства.

Для оценки надежности сетей используются различные характеристики, в том числе: *коэффициент готовности*, означающий долю времени, в течение которого система может быть использована; *безопасность*, то есть способность системы защитить данные от несанкционированного доступа; *отказоустойчивость* –

способность системы работать в условиях отказа некоторых ее элементов.

Совместимость означает, что сеть способна включать в себя самое разнообразное программное и аппаратное обеспечение.

Управляемость сети подразумевает возможность централизованно контролировать состояние основных элементов сети, выявлять и разрешать проблемы, возникающие при работе сети, выполнять анализ производительности и планировать развитие сети.

Расширяемость означает возможность сравнительно легкого добавления и наращивания длины сегментов сети и замены существующей аппаратуры более мощной.

Масштабируемость означает, что сеть позволяет наращивать количество узлов и протяженность связей в очень широких пределах, при этом производительность сети не ухудшается.

Прозрачность – свойство сети скрывать от пользователя детали своего внутреннего устройства, упрощая тем самым его работу в сети.

Качество обслуживания определяет количественные оценки вероятности того, что сеть будет передавать определенный поток данных между двумя определенными узлами в соответствии с потребностями приложения или пользователя.

Контрольные вопросы к главе 4

1. Какие аппаратные средства обеспечивают связь компьютера с периферийным устройством?
2. Какие программные средства участвуют в обмене информации компьютера с периферийным оборудованием?
3. Назовите основные топологии физических связей в сети.
4. Назовите недостатки и преимущества топологий «общая шина» и «дерево».
5. Перечислите основные топологические элементы сети.
6. Назовите основные типы адресации узлов сети.
7. Изобразите в виде графа принцип организации доменной символьной адресации.
8. Каковы цели маршрутизации в сети?
9. Назовите основные способы маршрутизации.
10. Назовите основные виды коммутации потоков в сети. В чем заключаются их преимущества и недостатки?

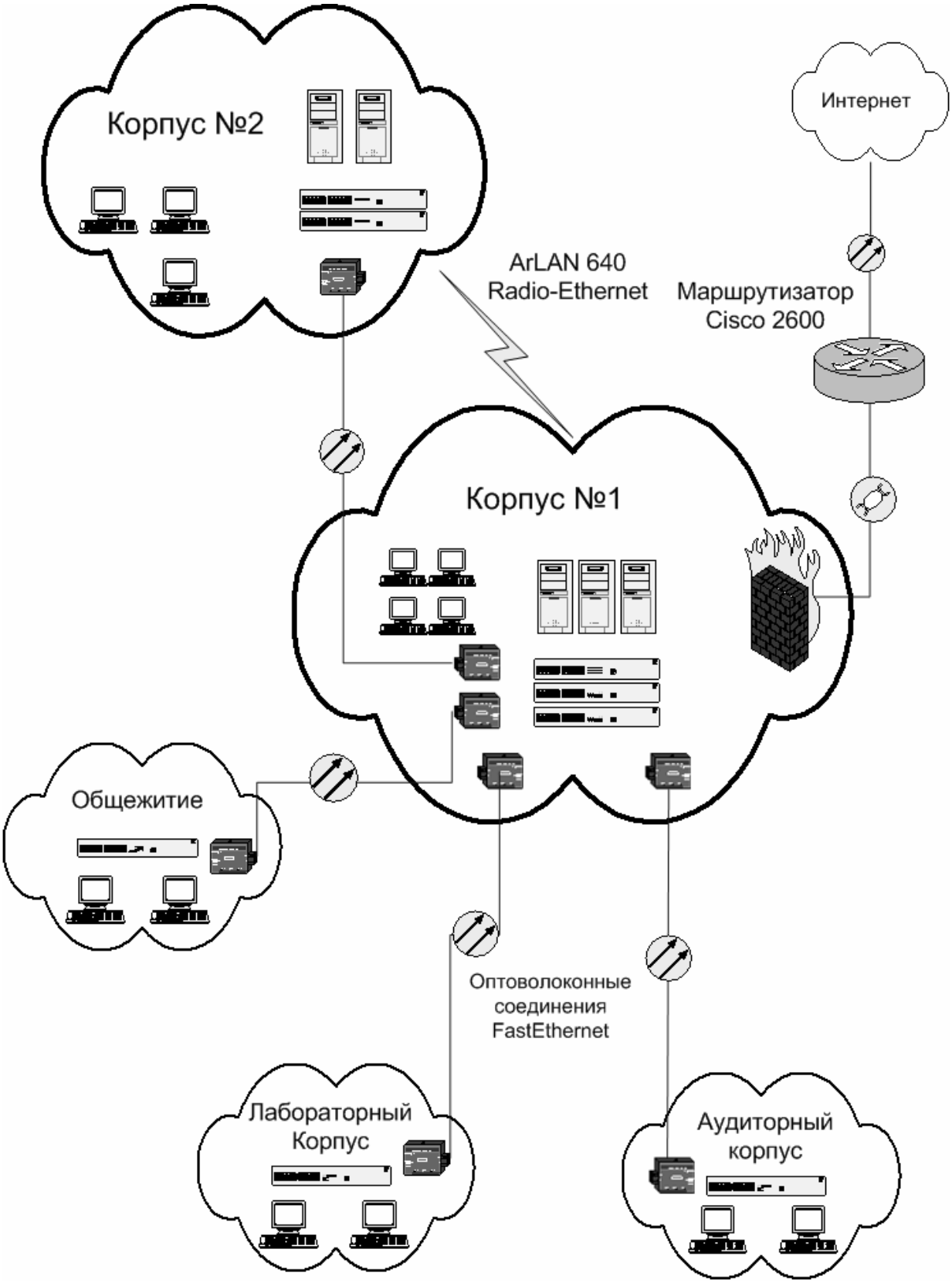


Рис. 4.9. Схема сети кампуса

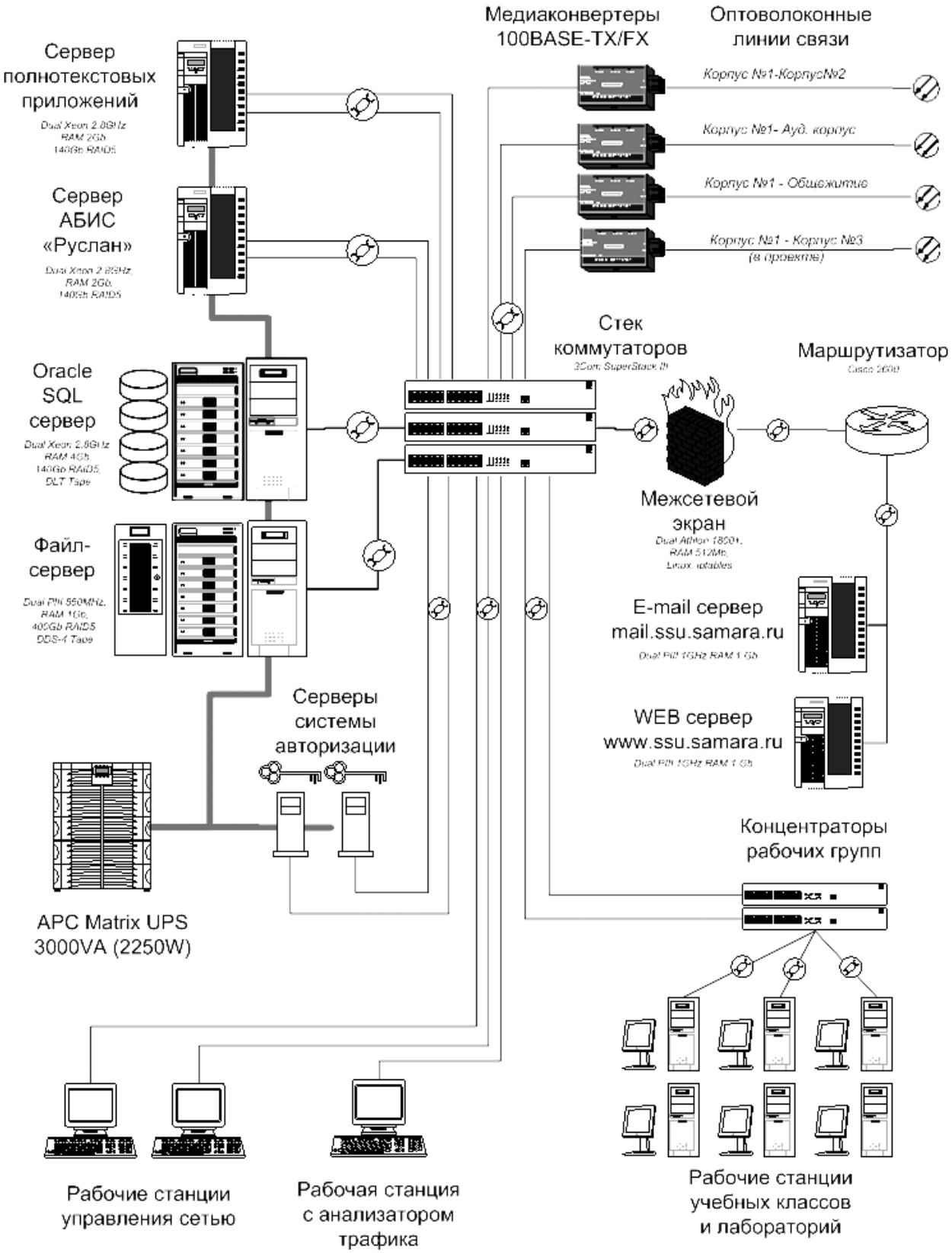
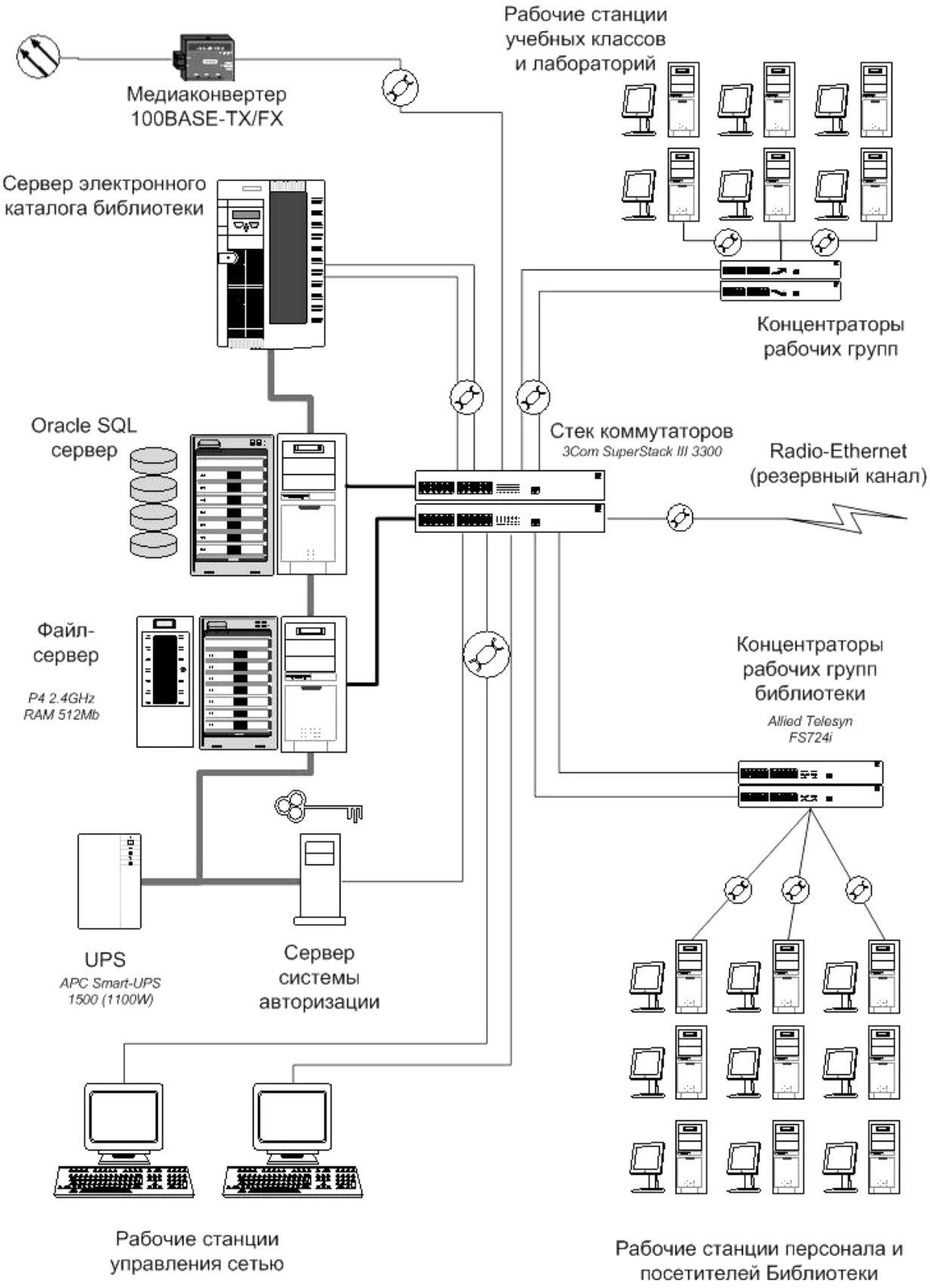

Медиаконвертеры
100BASE-TX/FX
Оптоволоконные
линии связи
Сервер
полнотекстовых
приложений
Dual Xeon 2.8GHz
RAM 2Gb
140Gb RAID5
Сервер
АБИС
«Руслан»
Dual Xeon 2.8GHz
RAM 2Gb
140Gb RAID5
Корпус №1-Корпус№2
Корпус №1- Ауд. корпус
Корпус №1 - Общежитие
Корпус №1 - Корпус №3
(в проекте)
Стек
коммутаторов
3Com SuperStack II
Маршрутизатор
Cisco 2600
Oracle
SQL
сервер
Dual Xeon 2.8GHz
RAM 4Gb
140Gb RAID5
DLT Tape
Межсетевой
экран
Dual Athlon 1850+
RAM 512Mb
Linux iptables
Файл-
сервер
Dual PIII 550MHz
RAM 1Gb
405Gb RAID5
DDS-4 Tape
E-mail сервер
mail.ssu.samara.ru
Dual PIII 1GHz RAM 1 Gb
WEB сервер
www.ssu.samara.ru
Dual PIII 1GHz RAM 1 Gb
Серверы
системы
авторизации
Концентраторы
рабочих групп
APC Matrix UPS
3000VA (2250W)
Рабочие станции
управления сетью
Рабочая станция
с анализатором
трафика
Рабочие станции
учебных классов
и лабораторий
Центральный телекоммуникационный узел в корпусе №1(ул.ак.Павлова)

Рис. 4.10.



Локальный телекоммуникационный узел в корпусе №2 (ул.Потапова)

Рис. 4.11.

ГЛАВА 5

ТЕХНОЛОГИИ ПЕРЕДАЧИ ДАННЫХ

5.1. Многоуровневые протоколы

Процесс передачи информации по каналам связи представляет собой достаточно сложную задачу. В конечном счете, отправитель и получатель должны оперировать понятными приложениям данными, например, текстовый файл. На самом деле информация передается по физическим каналам связи в виде электрических или оптических сигналов (для медного кабеля и оптоволоконных линий соответственно), либо радиоволн (например, спутниковые каналы связи). Указанные процессы преобразования должны пройти несколько стадий. На каждой стадии должны быть установлены определенные стандарты, позволяющие унифицировать применение различных аппаратно-программных средств.

В компьютерных сетях идеологической основой стандартизации является многоуровневый подход к разработке средств сетевого взаимодействия. Именно на основе этого подхода была разработана стандартная семиуровневая модель взаимодействия открытых систем, ставшая своего рода универсальным языком сетевых специалистов.

Такой подход заключается в следующем. Все множество модулей, решающих частные задачи организации сетевого взаимодействия, разбивают на группы и упорядочивают по *уровням*, образующим иерархию. В соответствии с принципом иерархии для каждого промежуточного уровня можно указать непосредственно примыкающие к нему соседние вышележащий и нижележащий уровни. Группа модулей, составляющих каждый уровень, должна быть сформирована таким образом, чтобы все модули этой группы для выполнения своих задач обращались с запросами только к модулям соседнего нижележащего уровня. С другой стороны, результаты работы всех модулей, отнесенных к некото-

рому уровню, могут быть переданы только модулям соседнего вышележащего уровня. Такая иерархическая декомпозиция задачи предполагает четкое определение функции каждого уровня и интерфейсов между уровнями. Интерфейс определяет набор функций, которые нижележащий уровень предоставляет вышележащему. В результате иерархической декомпозиции достигается относительная независимость уровней, а значит, возможность их автономной разработки и модификации. Количество уровней, их названия, содержание и назначение разнятся от сети к сети. Однако во всех сетях целью каждого уровня является предоставление неких служб для более верхних уровней, скрывая, таким образом, от верхних уровней детали реализации предоставляемого сервиса.

Уровень *n* одной машины поддерживает связь с уровнем *n* другой машины. Правила и соглашения, используемые в данном общении, называются п р о т о к о л о м уровня *n*. По сути, протокол является договоренностью общающихся сторон о том, как должно происходить общение. Объекты, включающие в себя соответствующие уровни на различных машинах, называются о д н о р а н г о в ы м и или равноправными узлами. Именно они общаются при помощи протокола. В действительности, данные не пересылаются с уровня *n* одной машины на уровень *n* другой машины. Вместо этого каждый уровень передает данные и управление уровню, лежащему ниже, пока не достигается самый нижний уровень. Ниже первого уровня располагается *физический носитель*, по которому и производится обмен информацией. Между каждой парой смежных уровней находится *интерфейс*, определяющий набор примитивных операций, предоставляемых нижним уровнем верхнему. В сущности, протокол и интерфейс выражают одно и то же понятие, но традиционно в сетях за ними закрепили разные области действия: протоколы определяют правила взаимодействия модулей одного уровня в разных узлах, а интерфейсы – правила взаимодействия модулей соседних уровней в одном узле.

На рис. 5.1 представлена принципиальная схема взаимодействия двух узлов, причем виртуальное общение показано пунктиром, а физическое – сплошными линиями.

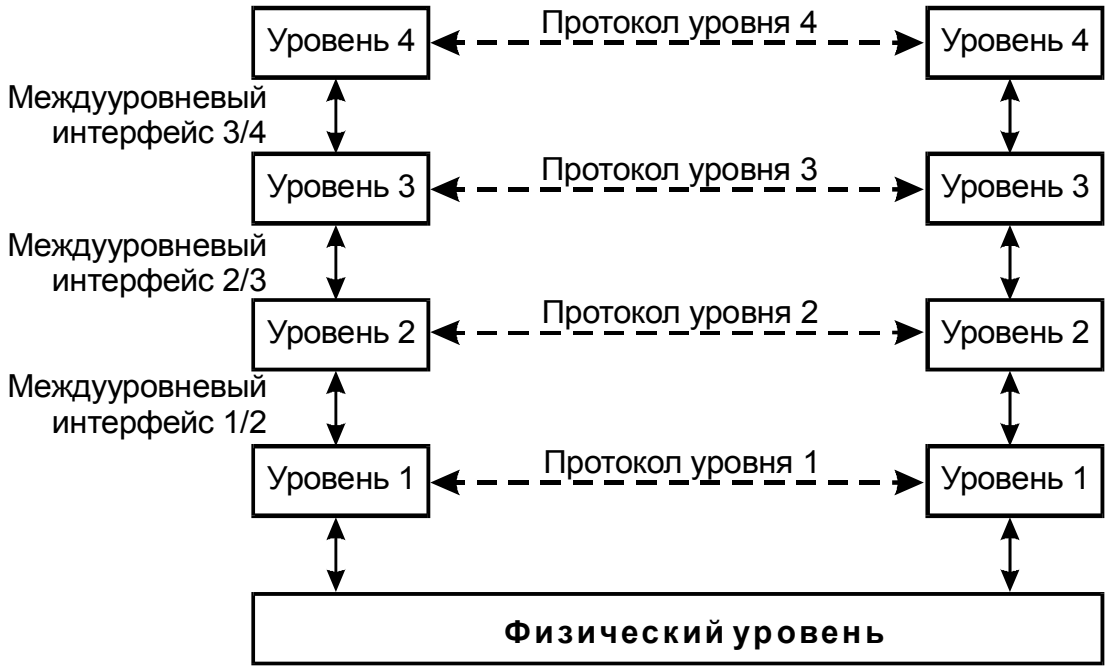


Рис.5.1. Схема взаимодействия двух узлов

Набор уровней и протоколов называется архитектурой сети. Спецификация архитектуры должна содержать достаточно информации для написания программного обеспечения или создания аппаратуры для каждого уровня, так чтобы они корректно выполняли требования протокола. Ни детали реализации, ни спецификации интерфейсов не являются частями архитектуры, так как они спрятаны внутри машины и не видны снаружи. При этом даже не требуется, чтобы интерфейсы на всех машинах сети были одинаковыми, лишь бы каждая машина правильно применяла все протоколы. Иерархически организованный набор протоколов, достаточный для организации взаимодействия узлов в сети, называется стеком коммуникационных протоколов.

Коммуникационные протоколы могут быть реализованы как программно, так и аппаратно. Протоколы нижних уровней часто реализуются комбинацией программных и аппаратных средств, а протоколы верхних уровней – как правило, чисто программными средствами. Программный модуль, реализующий некоторый протокол, часто для краткости также называют «*протоколом*». Понятно, что один и тот же алгоритм может быть запрограммирован с разной степенью эффективности. Точно так же и протокол может иметь несколько программных реализаций. Именно поэтому при сравнении протоколов следует учитывать не только логику

их работы, но и качество программных решений. Более того, на эффективность взаимодействия устройств в сети влияет качество всей совокупности протоколов, составляющих стек, в частности, насколько рационально распределены функции между протоколами разных уровней и насколько хорошо определены интерфейсы между ними.

Протоколы реализуются не только компьютерами, но и другими сетевыми устройствами – концентраторами, мостами, коммутаторами, маршрутизаторами и т. д. В зависимости от типа устройства в нем должны быть встроенные средства, реализующие тот или иной набор протоколов.

Чтобы было проще понять идею многоуровневого общения, можно воспользоваться следующей аналогией, представленной на рис. 5.2.

Руководители фирм из России (руководитель 1) и Японии (руководитель 2) договорились установить деловые отношения. По договоренности (протоколу между руководителями) руководитель 1 должен представить свои предложения руководителю 2. Для этого руководитель 1 подготовил текст документа и передал его своему переводчику, используя какой-то принятый интерфейс общения с ним (например, передача текста в бумажном или электронном виде) с указанием доставить руководителю 2 на японском языке.

Руководителя 1 после этого не интересует, каким образом переводчик доставит сообщение дальше. Он уверен лишь в том, что его поручение будет выполнено до конца. Однако переводчик 1 не знает японского языка, а переводчик 2 не знает русского, но оба знают французский. По договоренности (протоколу между переводчиками) переводчик 1 переводит документ на французский язык и передает текст секретарю 1, используя свой интерфейс общения с ним.

Наконец секретарь 1 передает текст секретарю 2 при помощи протокола общения между переводчиками (электронная почта, факс, почтовое отправление и т.п.). Причем секретарю 1 не важно содержание текста. Ему важно доставить конкретный текст именно секретарю 2, а не кому-либо другому. Далее текст аналогичным образом поднимается с уровня секретаря 2 через переводчика 2 к руководителю 2.

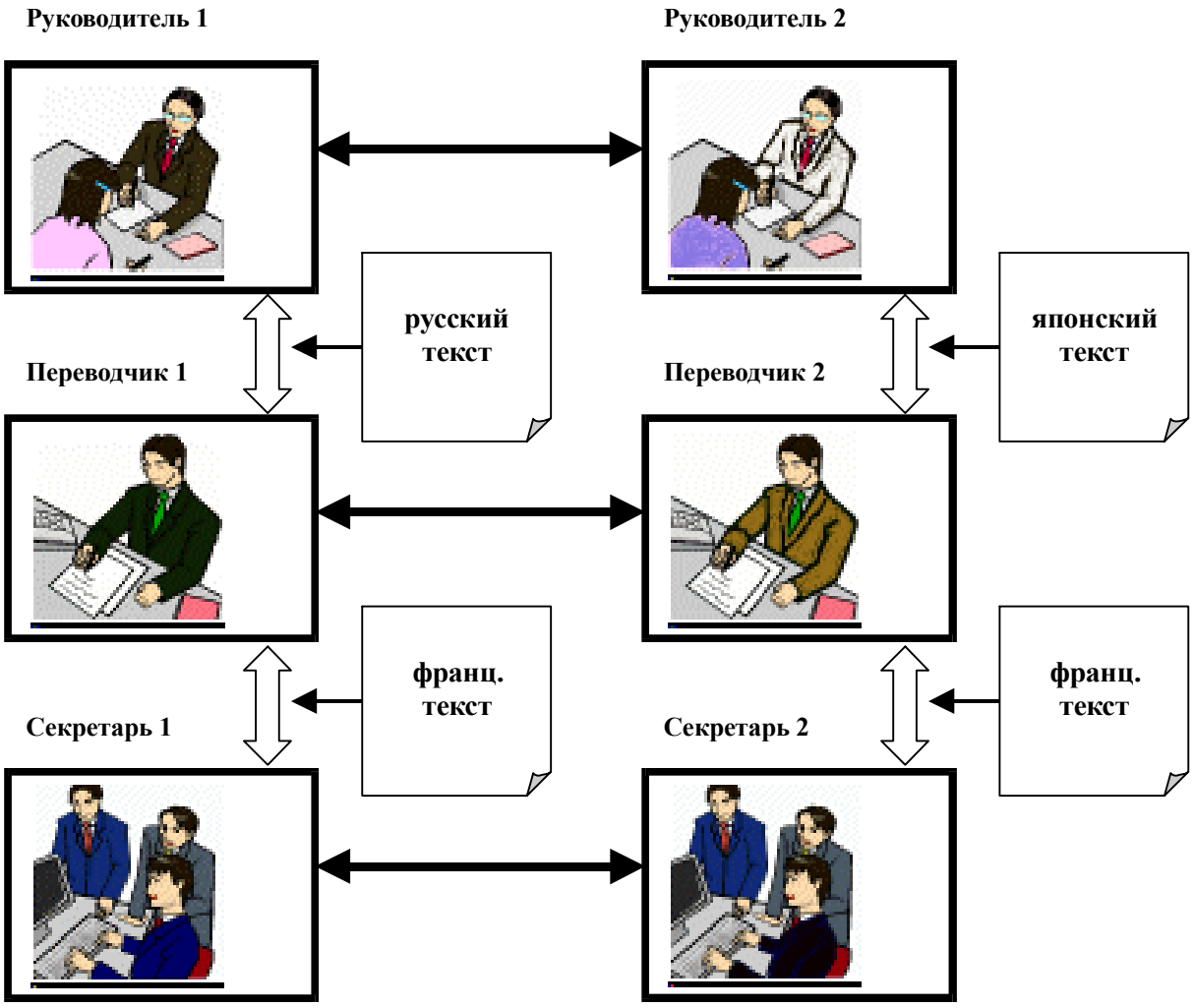


Рис.5.2. Пример многоуровнего общения

Описанная декомпозиция сложной задачи передачи информации на уровни позволяет достаточно широко варьировать в выборе аппаратных и программных компонентов. Например, замена переводчика 1 другим человеком (аналог аппаратной части) не повлияет на процесс передачи сообщения, потому что другой переводчик будет реализовывать сложившийся протокол с переводчиком 2, а также интерфейсы с руководителем 1 и секретарем 1. Аналогично замена способа передачи текста между переводчиком 1 и секретарем 1 (интерфейса) не повлияет на решение всей задачи передачи сообщений между руководителями.

5.2. Разработка уровней

При создании компьютерных сетей на некоторых уровнях возникает ряд ключевых проблем, которые должны решать соот-

ветствующие протоколы. В качестве примера приведем некоторые из них.

Каждый уровень нуждается в механизме идентификации отправителей и получателей. Поскольку в сети обычно довольно много компьютеров, на которых часто одновременно могут выполняться несколько процессов, то процессу необходимо указать, с кем он хочет «поговорить».

Также необходимо выработать правила для переноса данных. В некоторых системах данные могут перемещаться только в одном направлении. Этот метод называется симплексной связью. В других системах данные могут перемещаться в любом направлении, но не одновременно. Такая связь называется полудуплексной. И, наконец, существуют сети, в которых данные могут перемещаться одновременно в любом направлении, что называется дуплексной связью.

Важным аспектом является контроль ошибок, поскольку физические каналы связи несовершенны. Известно множество кодов, опознающих и исправляющих ошибки, однако обе стороны соединения должны договориться между собой о том, какой именно код будет выбран. Кроме того, получатель должен иметь возможность сообщить отправителю, какие из сообщений были получены правильно, а какие нет.

Не все каналы связи сохраняют последовательность посылаемых по ним сообщений. Чтобы исправить возможную потерю порядка последовательности сообщений, протокол должен явно снабжать получателя номерами пакетов, так, чтобы получаемые фрагменты сообщений могли бы быть собраны в правильном порядке.

Кроме того, на каждом уровне возникает вопрос, как организовать пересылку данных так, чтобы быстрая передающая сторона не завалила пакетами медленную принимающую сторону. Для разрешения данной проблемы существуют различные решения. Некоторые из них предполагают прямые или косвенные ответы получателя посылающей стороне, информирующие о текущем состоянии получателя. Другим решением может быть ограничение скорости передачи до некоторого договорного уровня.

Еще одна проблема, которую необходимо разрешать на различных уровнях, – это невозможность всех процессов принимать

сколь угодно длинные сообщения. С этой проблемой может быть связан вопрос, что делать, если процесс настаивает на передаче данных столь малыми порциями, что передача становится неэффективной. Для решения подобной проблемы можно объединять посылаемые сообщения в один большой пакет, а после пересылки снова разбивать его на отдельные сообщения.

5.3. Модель OSI

Для организации обмена информацией должен быть разработан комплекс программных и аппаратных средств, распределенных по разным устройствам сети. Поначалу разработчики и поставщики сетевых средств пытались идти каждый по своему пути, решая весь комплекс задач *с* помощью собственного набора протоколов, программ и аппаратуры. Однако решения различных поставщиков оказывались несовместимыми друг с другом, что вызывало массу неудобств для пользователей, которых по разным причинам не удовлетворял набор возможностей, предоставляемых только одним из поставщиков. Управление таким сложным, использующим многочисленную и разнообразную аппаратуру процессом, как передача и обработка данных в разветвленной сети, требует формализации и стандартизации процедур:

– выделения и освобождения ресурсов компьютеров, линий связи и коммуникационного оборудования;

– установления и разъединения соединений;

– маршрутизации, согласования, преобразования и передачи данных между узлами сети;

– контроля правильности передачи;

– исправления ошибок и т.д.

Необходимость стандартизации протоколов важна и для понимания сетями друг друга при их взаимодействии. Указанные задачи решаются с помощью системы стандартов, регламентирующих нормализованные процедуры взаимодействия элементов сети при установлении связи и передаче данных.

В начале 80-х годов международной организацией по стандартизации (*ISO* – International Organisation for Standardization) разработана система стандартных протоколов, получившая на-

звание модели взаимодействия открытых систем (Open System Interconnection – *OSI*), часто называемая также *эталонной семиуровневой логической моделью взаимодействия открытых систем*. Открытая система – система, доступная для взаимодействия с другими системами в соответствии с принятыми стандартами.

Модель OSI представляет собой самые общие рекомендации для построения стандартов совместимых сетевых программных продуктов, она же служит базой для производителей при разработке совместимого сетевого оборудования. Данные рекомендации должны быть реализованы как в аппаратуре, так и в программном обеспечении информационных сетей. Модель регламентирует общие функции, а не специальные решения, поэтому реальные сети могут частично отступать от модели.

Функции любого узла сети разбиваются на *уровни*. Внутри каждого узла взаимодействие между уровнями идет по вертикали. Взаимодействие между двумя узлами логически происходит по горизонтали – между соответствующими уровнями. Реально же из-за отсутствия непосредственных горизонтальных связей производится спуск до нижнего уровня в источнике, связь через физическую среду и подъем до соответствующего уровня в приемнике информации. Каждый уровень обеспечивает свой набор сервисных функций (сервисов), «прикладная ценность» которых возрастает с повышением уровня.

Уровень, с которого посылается запрос, и симметричный ему уровень в отвечающей системе формируют свои блоки данных. Данные снабжаются служебной информацией (заголовком) данного уровня и спускаются на уровень ниже, пользуясь сервисами соответствующего уровня. На этом уровне к полученной информации также присоединяется служебная информация, и так происходит спуск до самого нижнего уровня, сопровождаемый «обрастанием» заголовками.

Наконец, по нижнему уровню вся эта конструкция достигает получателя, где по мере подъема вверх освобождается от служебной информации соответствующего уровня. В итоге сообщение, посланное источником, в «чистом виде» достигает соответствующего уровня системы-получателя, независимо от тех «приключений», которые с ним происходили во время путешествия по

сети. Служебная информация управляет процессом передачи и служит для контроля его успешности и достоверности. В случае возникновения проблем может быть сделана попытка их уладить на том уровне, где они обнаружены. Если уровень не может решить проблему, он сообщает о ней на вызвавший его вышестоящий уровень.

Сервисы по передаче данных могут быть *гарантированными* и *негарантированными*. Гарантированный сервис на вызов ответит сообщением об успешности (по уведомлению от получателя) или неуспешности операции. Негарантированный сервис сообщит только о выполнении операции (он освободился), а дошли ли данные до получателя, при этом неизвестно. Контроль достоверности и обработка ошибок может выполняться на разных уровнях и инициировать повтор передачи блока. Как правило, чем ниже уровень, на котором контролируются ошибки, тем быстрее они обрабатываются.

В модели OSI средства взаимодействия делятся на семь уровней (рис. 5.3.): прикладной, представительный, сеансовый, транспортный, сетевой, канальный и физический. Канальный уровень называют еще уровнем передачи данных.

Для обозначения единиц обмена данными, с которыми имеют дело протоколы разных уровней, используется общее название протокольный блок данных (Protocol Data Unit, *PDU*). Для обозначения блоков данных определенных уровней часто используются специальные названия: кадр, пакет, дейтаграмма, сегмент.

На основании запроса приложения программное обеспечение прикладного уровня формирует сообщение стандартного формата. Обычное сообщение состоит из заголовка и поля данных. Заголовок содержит служебную информацию, которую необходимо передать через сеть прикладному уровню машины-адресата, чтобы сообщить ему, какую работу надо выполнить. Поле данных сообщения может быть пустым или содержать какие-либо данные, например те, которые необходимо записать в удаленный файл. После формирования сообщения прикладной уровень направляет его вниз по стеку представительному уровню.

Протокол представительного уровня на основании информации, полученной из заголовка прикладного уровня, выполняет

требуемые действия и добавляет к сообщению собственную служебную информацию – заголовок представительного уровня, в котором содержатся указания для протокола представительного уровня машины-адресата. Полученное в результате сообщение передается вниз сеансовому уровню, который, в свою очередь, добавляет свой заголовок, и т.д.

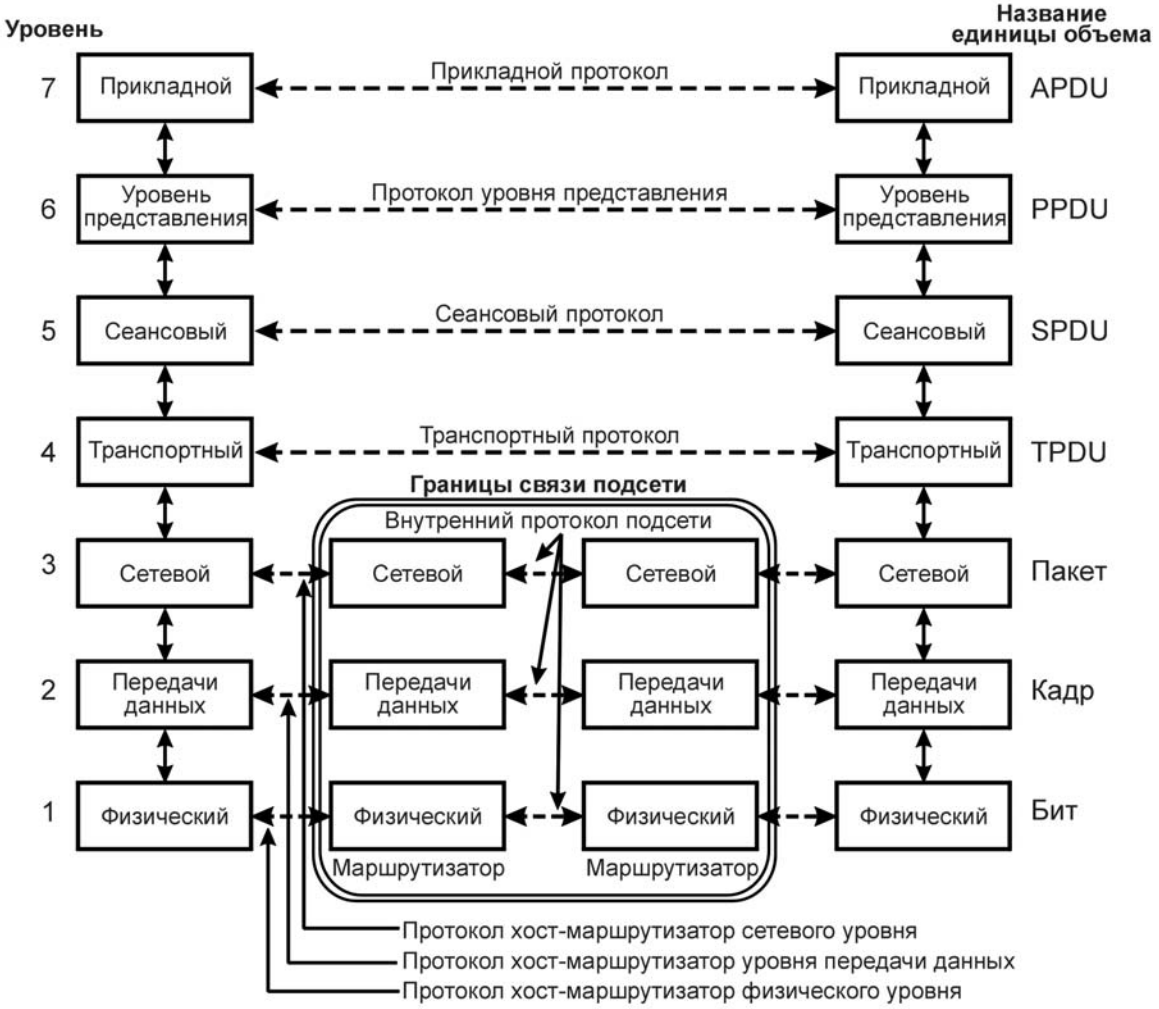


Рис. 5.3. Семиуровневая модель OSI

Некоторые реализации протоколов помещают служебную информацию не только в начале сообщения в виде заголовка, но и в конце, в виде так называемого «концевика». Наконец, сообщение достигает нижнего, физического уровня, который собственно и передает его по линиям связи машине-адресату.

Схема переноса данных в модели OSI представлена на рис. 5.4. Когда сообщение по сети поступает адресату, оно принимается его физическим уровнем и последовательно перемещается вверх с уровня на уровень. Каждый уровень анализирует и обра-

батывает заголовок своего уровня, выполняя соответствующие данному уровню функции, а затем удаляет этот заголовок и передает сообщение вышележащему уровню.

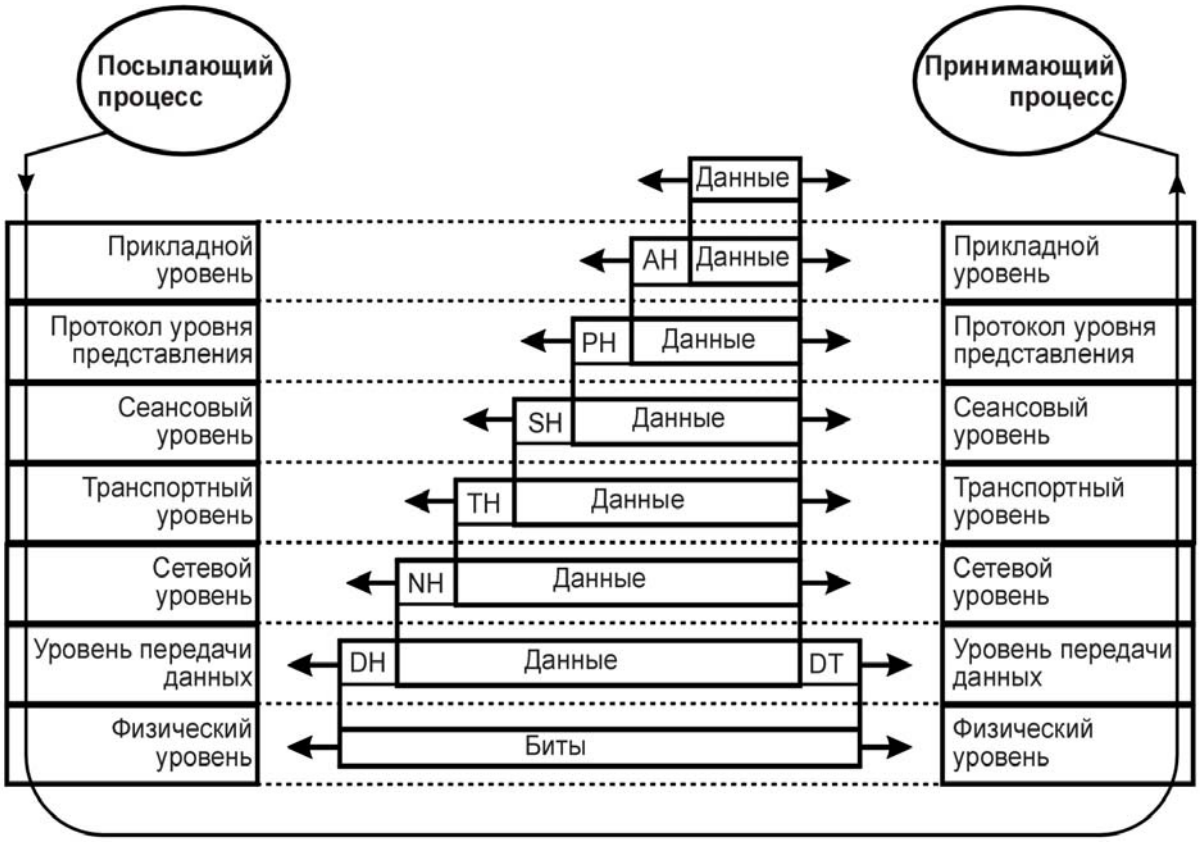


Рис. 5.4. Схема переноса данных в модели OSI

5.4. Функции уровней модели OSI

Физический уровень

Физический уровень имеет дело с передачей битов по физическим каналам связи, таким, например, как коаксиальный кабель, витая пара, оптоволоконный кабель. К этому уровню имеют отношение характеристики физических сред передачи данных, такие, как полоса пропускания, помехозащищенность, волновое сопротивление и др. На этом же уровне определяются характеристики электрических сигналов, передающих дискретную информацию, например, крутизна фронтов импульсов, уровни напряжения или тока передаваемого сигнала, тип кодирования, скорость передачи сигналов. Кроме этого, здесь стандартизуются

типы разъемов и назначение каждого контакта. Функции физического уровня реализуются во всех устройствах, подключенных к сети. Со стороны компьютера функции физического уровня выполняются сетевым адаптером или последовательным портом.

Примером протокола физического уровня может служить спецификация 10Base-T технологии Ethernet, которая определяет в качестве используемого кабеля неэкранированную витую пару, разъем RJ-45, максимальную длину физического сегмента 100 метров, а также некоторые другие характеристики среды и электрических сигналов.

Канальный уровень

На физическом уровне просто пересылаются биты. При этом не учитывается, что в некоторых сетях, в которых линии связи используются попеременно несколькими парами взаимодействующих компьютеров, физическая среда передачи может быть занята. Поэтому одной из задач канального уровня является проверка доступности среды передачи. Другой задачей канального уровня является реализация механизмов обнаружения и коррекции ошибок. Для этого на канальном уровне биты группируются в наборы, называемые *кадрами*, обычно размером от нескольких сот до нескольких тысяч байтов. Канальный уровень обеспечивает корректность передачи каждого кадра, помещая специальную последовательность битов в начало и конец каждого кадра для его выделения, а также вычисляет контрольную сумму, обрабатывая все байты кадра определенным способом и добавляя контрольную сумму к кадру. Когда кадр приходит по сети, получатель снова вычисляет контрольную сумму полученных данных и сравнивает результат с контрольной суммой из кадра. Если они совпадают, кадр считается правильным и принимается. Если же контрольные суммы не совпадают, то фиксируется ошибка. Канальный уровень может не только обнаруживать ошибки, но и исправлять их за счет повторной передачи поврежденных кадров.

Необходимо отметить, что функция исправления ошибок не является обязательной для канального уровня, поэтому в некоторых протоколах этого уровня она отсутствует, например в Ethernet. В протоколах канального уровня, используемых в ло-

кальных сетях, заложена определенная структура связей между компьютерами и способы их адресации. Хотя канальный уровень и обеспечивает доставку кадра между любыми двумя узлами локальной сети, он это делает только в сети с совершенно определенной топологией связей, именно той топологией, для которой он был разработан. К таким типовым топологиям, поддерживаемым протоколами канального уровня локальных сетей, относятся общая шина, кольцо и звезда, а также структуры, полученные из них с помощью мостов и коммутаторов.

Примерами протоколов канального уровня являются протоколы Ethernet, Token Ring, FDDI. В локальных сетях протоколы канального уровня используются компьютерами, мостами, коммутаторами и маршрутизаторами. В компьютерах функции канального уровня реализуются совместными усилиями сетевых адаптеров и их драйверов.

В глобальных сетях, которые редко обладают регулярной топологией, канальный уровень часто обеспечивает обмен сообщениями только между двумя соседними компьютерами, соединенными индивидуальной линией связи. Иногда в глобальных сетях функции канального уровня в чистом виде выделить трудно, так как в одном и том же протоколе они объединяются с функциями сетевого уровня.

В целом канальный уровень представляет собой весьма мощный и законченный набор функций по пересылке сообщений между узлами сети. В некоторых случаях протоколы канального уровня оказываются самодостаточными транспортными средствами и могут допускать работу поверх себя непосредственно протоколов прикладного уровня или приложений, без привлечения средств сетевого и транспортного уровней. Тем не менее, для обеспечения качественной транспортировки сообщений в сетях любых топологий и технологий функций канального уровня оказывается недостаточно, поэтому в модели OSI решение этой задачи возлагается на два следующих уровня – сетевой и транспортный.

Канальный уровень обеспечивает передачу пакетов данных, поступающих от протоколов верхних уровней, узлу назначения, адрес которого также указывает протокол верхнего уровня. Протоколы канального уровня оформляют переданные им пакеты в

кадры собственного формата, помещая указанный адрес назначения в одно из полей такого кадра, а также сопровождая кадр контрольной суммой. Протокол канального уровня имеет локальный смысл, он предназначен для доставки кадров данных, как правило, в пределах сетей с простой топологией связей и однотипной или близкой технологией, например в односегментных сетях Ethernet или же в многосегментных сетях Ethernet и Token Ring иерархической топологии, разделенных только мостами и коммутаторами. Во всех этих конфигурациях адрес назначения имеет локальный смысл для данной сети и не изменяется при прохождении кадра от узла-источника к узлу назначения. Возможность передавать данные между локальными сетями разных технологий связана с тем, что в этих технологиях используются адреса одинакового формата, к тому же производители сетевых адаптеров обеспечивают уникальность адресов независимо от технологии.

Другой областью действия протоколов канального уровня являются связи типа «точка-точка» глобальных сетей, когда протокол канального уровня ответственен за доставку кадра непосредственному соседу. Адрес в этом случае не имеет принципиального значения, а на первый план выходит способность протокола восстанавливать искаженные и утерянные кадры, так как плохое качество территориальных каналов, особенно коммутируемых телефонных, часто требует выполнения подобных действий. Если же перечисленные выше условия не соблюдаются, например связи между сегментами Ethernet имеют петлевидную структуру, либо объединяемые сети используют различные способы адресации, как это имеет место в сетях Ethernet, то протокол канального уровня не может в одиночку справиться с задачей передачи кадра между узлами и требует помощи протокола сетевого уровня.

Сетевой уровень

Сетевой уровень служит для образования единой транспортной системы, объединяющей несколько сетей. Он управляет логическим каналом передачи данных в сети (адресация и маршрутизация данных, коммутация: каналов, сообщений, пакетов). На этом уровне реализуется главная телекоммуникационная функция сетей – обеспечение связи ее пользователей. Каждый из

пользователей сети обязательно использует протоколы этого уровня и имеет свой уникальный адрес.

На сетевом уровне выполняется структуризация данных – разбивка их на пакеты и присвоение пакетам сетевых адресов. При организации доставки пакетов на сетевом уровне используется понятие «номер сети». В этом случае адрес получателя состоит из старшей части – номера сети и младшей – номера узла в этой сети. Все узлы одной сети должны иметь одну и ту же старшую часть адреса, поэтому термину «сеть» на сетевом уровне можно дать и другое, более формальное определение: сеть – это совокупность узлов, сетевой адрес которых содержит один и тот же номер сети.

Внутри сети доставка данных обеспечивается соответствующим канальным уровнем, а вот доставкой данных между сетями занимается сетевой уровень, который и поддерживает возможность правильного выбора маршрута передачи сообщения даже в том случае, когда характер структуры связей между составляющими сетями отличается от принятого в протоколах канального уровня. Сети соединяются между собой специальными устройствами, называемыми маршрутизаторами. С точки зрения сетевого уровня маршрутизатор – это устройство, которое собирает информацию о топологии межсетевых соединений и на ее основании пересылает пакеты сетевого уровня в сеть назначения. Чтобы передать сообщение от отправителя, находящегося в одной сети, получателю, находящемуся в другой сети, нужно совершить некоторое количество транзитных передач между сетями, каждый раз выбирая подходящий маршрут. Таким образом, маршрут представляет собой последовательность маршрутизаторов, через которые проходит пакет.

Проблема выбора наилучшего пути называется маршрутизацией, и ее решение является одной из главных задач сетевого уровня. Эта проблема осложняется тем, что самый короткий путь не всегда самый лучший. Часто критерием при выборе маршрута является время передачи данных по этому маршруту. Оно зависит от пропускной способности каналов связи и интенсивности трафика, которая может изменяться с течением времени. Некоторые алгоритмы маршрутизации пытаются приспособиться к изменению нагрузки, в то время как другие принимают решения на

основе средних показателей за длительное время. Выбор маршрута может осуществляться и по другим критериям, например, надежности передачи. Сетевой уровень решает также задачи согласования разных технологий, упрощения адресации в крупных сетях и создания надежных и гибких барьеров на пути нежелательного трафика между сетями.

На сетевом уровне определяются два вида протоколов. Первый вид – *сетевые протоколы*, которые реализуют продвижение пакетов через сеть. Именно эти протоколы обычно имеют в виду, когда говорят о протоколах сетевого уровня. Однако часто к сетевому уровню относят и другой вид протоколов, называемых протоколами обмена маршрутной информацией или просто *протоколами маршрутизации*. *С* помощью этих протоколов маршрутизаторы собирают информацию о топологии межсетевых соединений. Протоколы сетевого уровня реализуются программными модулями операционной системы, а также программными и аппаратными средствами маршрутизаторов.

Примерами протоколов сетевого уровня являются протокол межсетевого взаимодействия *IP* стека *TCP/IP* и протокол межсетевого обмена пакетами *IPX* стека Novell.

Транспортный уровень

Транспортный уровень управляет сегментированием данных (*сегмент* – блок данных транспортного уровня) и сквозной передачей (транспортировкой) данных от источника к потребителю (обмен управляющей информацией и установление между абонентами логического канала, обеспечение качества передачи данных).

На пути от отправителя к получателю пакеты могут быть искажены или утеряны. Хотя некоторые приложения имеют собственные средства обработки ошибок, существуют и такие, которые предпочитают сразу иметь дело с надежным соединением. Транспортный уровень обеспечивает приложениям или верхним уровням стека (прикладному и сеансовому) передачу данных с той степенью надежности, которая им требуется.

Модель OSI определяет пять классов сервиса, предоставляемых транспортным уровнем. Эти виды сервиса отличаются каче-

ством предоставляемых услуг: срочностью, возможностью восстановления прерванной связи, наличием средств мультиплексирования нескольких соединений между различными прикладными протоколами через общий транспортный протокол, а главное – способностью к обнаружению и исправлению ошибок передачи, таких, как искажение, потеря и дублирование пакетов. Если качество каналов передачи связи очень высокое и вероятность возникновения ошибок, не обнаруженных протоколами более низких уровней, невелика, то разумно воспользоваться одним из облегченных сервисов транспортного уровня, не обремененных многочисленными проверками, квотированием и другими приемами повышения надежности. Если же транспортные средства нижних уровней изначально очень ненадежны, то целесообразно обратиться к наиболее развитому сервису транспортного уровня, который работает, используя максимум средств для обнаружения и устранения ошибок.

Как правило, все протоколы, начиная с транспортного уровня и выше, реализуются программными средствами конечных узлов сети – компонентами их сетевых операционных систем. В качестве примера транспортных протоколов можно привести протоколы TCP и UDP стека TCP/IP и протокол SPX стека Novell. Протоколы нижних четырех уровней обобщенно называют сетевым транспортом или транспортной подсистемой, так как они полностью решают задачу транспортировки сообщений с заданным уровнем качества в составных сетях с произвольной топологией и различными технологиями. Оставшиеся три верхних уровня решают задачи предоставления прикладных сервисов на основании имеющейся транспортной подсистемы.

Сеансовый уровень

В функции сеансового уровня входит организация и проведение сеансов связи между прикладными процессами (инициализация и поддержание сеанса связи между абонентами сети, управление очередностью и режимами передачи: симплекс, полудуплекс, дуплекс).

Сеансовый уровень обеспечивает управление взаимодействием: фиксирует, какая из сторон является активной в настоящий

момент, предоставляет средства синхронизации. Последние позволяют вставлять контрольные точки в длинные передачи, чтобы в случае отказа можно было вернуться назад к последней контрольной точке, а не начинать все с начала. На практике немногие приложения используют сеансовый уровень, и он редко реализуется в виде отдельных протоколов, хотя функции этого уровня часто объединяют с функциями прикладного уровня и реализуют в одном протоколе.

Представительный уровень

Представительный уровень имеет дело с формой представления передаваемой по сети информации, не меняя при этом ее содержания. За счет уровня представления информация, передаваемая прикладным уровнем одной системы, всегда понятна прикладному уровню другой системы. С помощью средств данного уровня протоколы прикладных уровней могут преодолеть синтаксические различия в представлении данных или же различия в кодах символов. На этом уровне может выполняться шифрование и дешифрование данных, благодаря которым секретность обмена данными обеспечивается сразу для всех прикладных служб. Примером такого протокола является протокол Secure Socket Layer (*SSL*), который обеспечивает секретный обмен сообщениями для протоколов прикладного уровня стека TCP/IP.

Прикладной уровень

Задачей прикладного уровня является управление терминалами сети и прикладными процессами, которые являются источниками и потребителями информации, передаваемой в сети. Он ведает запуском программ пользователей, их выполнением, вводом-выводом данных, административным управлением.

Прикладной уровень – это в действительности просто набор разнообразных протоколов, с помощью которых пользователи сети получают доступ к разделяемым ресурсам, таким как файлы, принтеры или гипертекстовые web-страницы, а также организуют свою совместную работу. Единица данных, которой оперирует прикладной уровень, обычно называется сообщением. Существует очень большое разнообразие служб прикладного уровня. При-

ведем в качестве примера хотя бы несколько наиболее распространенных реализаций файловых служб: NCP в операционной системе Novell NetWare, SMB в Microsoft Windows NT, FTP и TFTP, входящие в стек TCP/IP.

5.5. Сетезависимые и сетенезависимые уровни

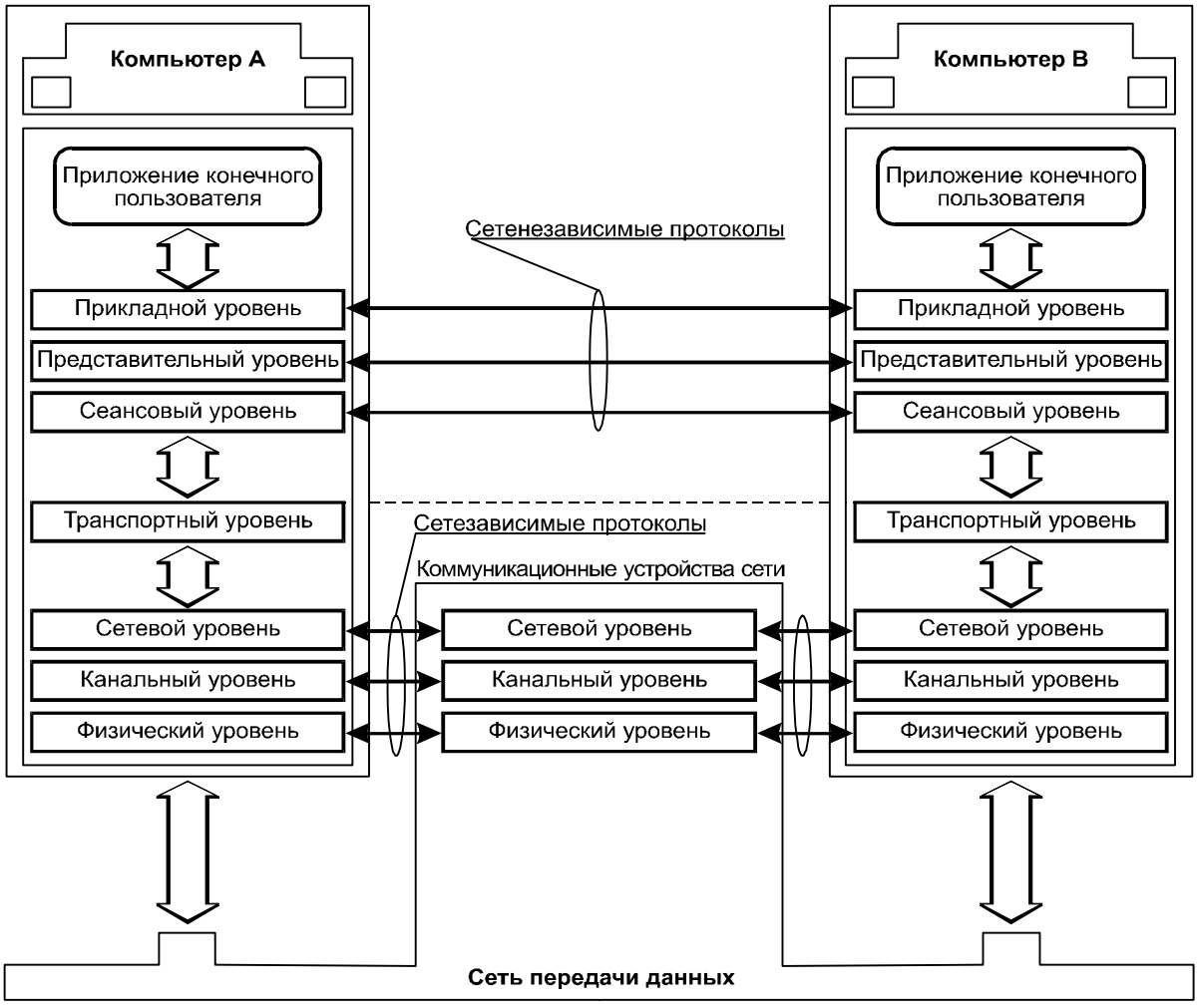


Рис. 5.5. Зависимость уровней модели OSI от сети

Функции всех уровней модели OSI могут быть отнесены к одной из двух групп: либо к функциям, зависящим от конкретной технической реализации сети, либо к функциям, ориентированным на работу с приложениями. Три нижних уровня – физический, канальный и сетевой – являются сетезависимыми, то есть протоколы этих уровней тесно связаны с технической реализаци-

ей сети и используемым коммуникационным оборудованием. Три верхних уровня – прикладной, представительный и сеансовый – ориентированы на приложения и мало зависят от технических особенностей построения сети. На протоколы этих уровней не влияют какие бы то ни было изменения в топологии сети, замена оборудования или переход на другую сетевую технологию.

Транспортный уровень является промежуточным. Он скрывает детали функционирования нижних уровней от верхних. Это позволяет разрабатывать приложения, не зависящие от технических средств непосредственной транспортировки сообщений. На рис. 5.5 показаны сетезависимые и сетенезависимые уровни модели OSI.

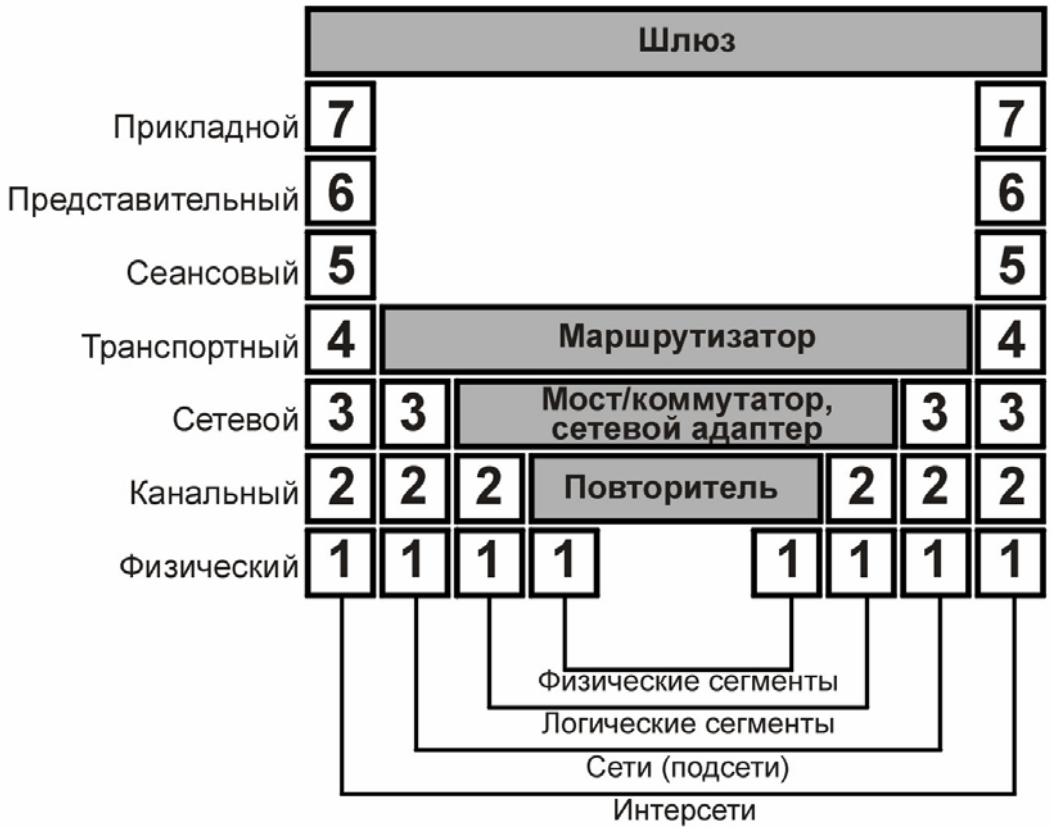


Рис.5.6. Распределение коммуникационных устройств по уровням

Компьютеры в сети взаимодействует друг с другом по протоколам всех семи уровней. Это взаимодействие компьютеры осуществляют через различные коммуникационные устройства: концентраторы, модемы, мосты, коммутаторы, маршрутизаторы, мультиплексоры. Соответствие функций различных устройств сети уровням модели OSI представлено на рис. 5.6. В зависимости от типа коммуникационное устройство может работать на

разных уровнях или на нескольких. На физическом уровне работает повторитель. Мост может работать на физическом и канальном уровнях, маршрутизатор на физическом, канальном и сетевом, иногда захватывая и транспортный уровень.

Модель OSI представляет хотя и очень важную, но только одну из многих моделей коммуникаций. Эти модели и связанные с ними стеки протоколов могут отличаться количеством уровней, их функциями, форматами сообщений, службами, поддерживаемыми на верхних уровнях, и прочими параметрами.

5.6. Стандартные стеки коммуникационных протоколов

Важнейшим направлением стандартизации в области вычислительных сетей является стандартизация коммуникационных протоколов. В настоящее время в сетях используется большое количество стеков коммуникационных протоколов. Наиболее популярными являются стеки: TCP/IP, IPX/SPX, NetBIOS/SMB, DECnet, OSI. Все эти стеки на нижних уровнях (физическом и канальном), используют одни и те же хорошо стандартизованные протоколы Ethernet, Token Ring, FDDI и некоторые другие, которые позволяют использовать во всех сетях одну и ту же аппаратуру. Зато на верхних уровнях все стеки работают по своим собственным протоколам. Эти протоколы часто не соответствуют рекомендуемому моделью OSI разбиению на уровни. В частности, функции сеансового и представительного уровня, как правило, объединены с прикладным уровнем. Такое несоответствие связано с тем, что модель OSI появилась как результат обобщения уже существующих и реально используемых стеков, а не наоборот.

5.6.1. Стек OSI

Следует четко различать модель OSI и стек OSI. В то время как модель OSI является концептуальной схемой взаимодействия открытых систем, стек OSI представляет собой набор вполне конкретных спецификаций протоколов. В отличие от других сте-

ков протоколов, стек OSI полностью соответствует модели OSI, он включает спецификации протоколов для всех семи уровней взаимодействия, определенных в этой модели. На нижних уровнях стек OSI поддерживает Ethernet, Token Ring, FDDI – то есть использует разработанные вне стека протоколы нижних уровней, как и все другие стеки. Протоколы сетевого, транспортного и сеансового уровней стека OSI специфицированы и реализованы различными производителями, но распространены пока мало. Протоколы стека OSI отличает большая сложность и неоднозначность спецификаций. Эти свойства явились результатом общей политики разработчиков стека, стремившихся учесть в своих протоколах все случаи жизни и все существующие и появляющиеся технологии. Из-за своей сложности протоколы OSI требуют больших затрат вычислительной мощности центрального процессора, что делает их более подходящими для мощных машин, а не для сетей персональных компьютеров.

Стек OSI – международный, независимый от производителей стандарт. Его поддерживает правительство США в своей программе GOSIP, в соответствии с которой все компьютерные сети, устанавливаемые в правительственных учреждениях США после 1990 года, должны либо непосредственно поддерживать стек OSI, либо обеспечить переход на этот стек в будущем. Тем не менее, стек OSI более популярен в Европе, чем в США, так как в Европе осталось меньше старых сетей, работающих по своим собственным протоколам. Большинство организаций пока только планируют переход к стеку OSI. Одним из крупнейших производителей, поддерживающих OSI, является компания AT&T, ее сеть Stargroup полностью базируется на этом стеке.

5.6.2. Стек IPX/SPX

Протокольный стек IPX/SPX разработан фирмой Novell для сетей NetWare, начиная с самых первых поколений. Этим стеком пользуются и сетевые ОС других фирм, включая Microsoft Windows 3:x/95/98/NT. Основу стека составляет протокол сетевого уровня (модели OSI) IPX (Internetwork Packet Exchange), отвечающий за адресацию и маршрутизацию пакетов и их негарантированную доставку между узлами различных IPX-сетей. Он под-

держивает только дейтаграммный (без установления соединений) способ обмена сообщениями. Поверх него работает транспортный протокол SPX (Sequenced Packet Protocol), обеспечивающий установление соединений и гарантированную доставку пакетов в правильном порядке. Протокол IPX может использовать технологии локальных сетей Ethernet, Token Ring, ARCnet, FDDI. Над протоколами IPX и SPX работают остальные протоколы стека, охватывающие верхние уровни модели. Прикладной уровень стека IPX/SPX составляют два протокола: NCP и SAP. Протокол NCP (NetWare Core Protocol) поддерживает все основные службы операционной системы Novell NetWare – файловую службу, службу печати и т. д. Протокол SAP (Service Advertising Protocol) выполняет вспомогательную роль. С помощью протокола SAP каждый компьютер, который готов предоставить какую-либо службу для клиентов сети, объявляет об этом широковещательно по сети, указывая в SAP-пакетах тип службы (например, файловая), а также свой сетевой адрес. Наличие протокола SAP позволяет резко уменьшить административные работы по конфигурированию клиентского программного обеспечения, так как всю необходимую информацию для работы клиенты узнают из объявлений SAP. В отличие от протокола IP, который изначально разрабатывался для глобальных сетей, протокол IPX создавался для применения в локальных сетях. Именно поэтому он является одним из самых экономичных протоколов в отношении требований к вычислительным ресурсам и хорошо работает в сравнительно небольших локальных сетях.

Формат пакета IPX приведен на рис. 5.7, длина полей указана в байтах.

CS	Len	TC	PT	DN	DH	DS	SN	SH	SS	Data
2	2	1	1	4	6	2	4	6	2	0-546

Рис. 5.7. Формат пакета IPX

CS (CheckSum) – контрольная сумма, обычно не используется, поскольку располагающийся ниже уровень передачи данных также предоставляет контрольную сумму;

Len (Length) – длина пакета, включая заголовок. Самый короткий пакет в 30 байт включает только заголовок, а рекомендуемый максимально большой – 576 байт;

TC (Transport Control) – управление транспортировкой. В этом поле учитывается количество сетей, которые пересек пакет (время жизни). Когда это количество превышает некий установленный максимум, пакет удаляется. Максимальное значение составляет 15;

PT (Packet Type) – тип пакета;

DN (Destination Network), **DH** (Destination Host), **DS** (Destination Socket)– адрес назначения;

SN (Source Network), **SH** (Source Host), **SS** (Source Socket) – адрес источника;

Data – поле данных. Поле данных нулевой длины может использоваться в служебных пакетах, например, для подтверждения получения предыдущего пакета.

Полный *IPX-адрес* имеет разрядность 12 байт и состоит из следующих частей:

– номера внешней сети (IPX external network number), 4 байта;

– номера узла (node address), 6 байт;

– локальный адрес на самой машине (socket number), 2 байта.

Номер сети в отличие от протокола IP имеет всегда фиксированную длину в 4 байта. В принципе, для корпоративных сетей эта длина является избыточной, так как вряд ли у предприятия возникнет потребность разделить свою сеть на 4 миллиарда подсетей. В период доминирования сетей IPX/SPX компания Novell рассматривала возможность создания единого всемирного центра по распределению IPX-адресов, аналогичного центру InterNIC сети Интернет. Однако стремительный рост популярности Интернета лишил это начинание смысла. Хотя протоколы IPX/SPX попрежнему работают в огромном количестве корпоративных сетей, заменить IP во всемирной сети они уже не смогут.

Под номером узла в протоколе IPX понимается аппаратный адрес узла. В сетях Ethernet адресом узла является MAC-адрес сетевого адаптера и задавать его специально не требуется (за исключением особых случаев). Номер сети требуется указывать только при конфигурировании серверов и маршрутизаторов. Номер сети для узлов, не занимающихся маршрутизацией (рабочих

станций), не указывается. В роли маршрутизатора, как правило, выступает внутренний маршрутизатор, входящий в ОС NetWare.

Номер сокета (socket) идентифицирует приложение, которое передает свои сообщения протоколу IPX.

Примерно раз в минуту каждый сервер рассылает всем пакет (при помощи широковещания), в котором сообщает всем свой адрес и список предоставляемых им служб. Рассылаемые пакеты собираются специальными процессами-агентами, работающими на машинах-маршрутизаторах, которые создают базы данных о предоставляемых услугах. Когда загружается машина-клиент, она тоже, используя широковещание, рассылает запрос, интересуясь расположением ближайшего сервера. Агент на локальной машине-маршрутизаторе видит этот запрос, просматривает базу данных серверов и подыскивает лучший сервер для данного запроса. Затем ответ отсылается клиенту, на основе которого тот может установить соединение с сервером. С этого момента клиент может использовать это соединение для получения доступа к файловой системе и другим службам.

Из анализа формата пакета можно сделать некоторые выводы об ограничениях протокола IPX.

1. *Отсутствует возможность динамической фрагментации на сетевом уровне*. В IPX-пакете нет полей, с помощью которых маршрутизатор может разбить слишком большой пакет на части. При передаче пакета в сеть с меньшим значением длины пакета IPX-маршрутизатор отбрасывает пакет. Протокол верхнего уровня, например NCP**,** должен последовательно уменьшать размер пакета до тех пор, пока не получит на него положительную квитанцию.

2. *Большие накладные расходы на служебную информацию*. Сравнительно небольшая максимальная длина поля данных IPX-пакета (546 байт при длине заголовка 30 байт) приводит к тому, что как минимум 5% данных являются служебными.

3. *Время жизни пакета ограничено числом 15*, что может оказаться недостаточным для большой сети (для сравнения, в IP-сетях пакет может пройти до 255 промежуточных маршрутизаторов).

4. *Отсутствует поле качества сервиса*, что не позволяет маршрутизаторам автоматически подстраиваться к требованиям приложения к качеству передачи трафика.

Кроме того, некоторые недостатки сетей Novell связаны не с протоколом IPX, а со свойствами других протоколов стека IPX/SPX. Недостатком IPX-адресации является ограничение длины адреса узла в 6 байт. Если какая-либо составная сеть использует аппаратные адреса большего размера, то протокол IPX не сможет доставить пакет узлу такой сети. Многие недостатки проявляются при работе стека IPX/SPX на медленных глобальных линиях связи, и это закономерно, так как ОС NetWare оптимизировалась для работы в локальной сети.

5.6.3. Стек TCP/IP

Рассмотрим теперь эталонную модель, использовавшуюся в компьютерной сети ARPANET. Эта сеть была исследовательской и финансировалась Министерством обороны США. В конце концов она объединила сотни университетов и правительственных зданий при помощи выделенных телефонных линий. Когда впоследствии появились спутниковые и радиосети, возникли большие проблемы при объединении с ними других сетей с помощью имеющихся протоколов. В результате понадобилась новая эталонная архитектура. Таким образом, возможность объединять различные сети в единое целое составляла одну из главных целей с самого начала. Позднее эта архитектура получила название **эталонной модели TCP/IP**, по своим двум основным протоколам.

Поскольку Министерство обороны беспокоилось, что ценные хосты, маршрутизаторы и межсетевые шлюзы могли быть мгновенно уничтожены, то важная задача состояла в том, чтобы добиться способности сети сохранять работоспособность при возможных потерях подсетевого оборудования, так чтобы при этом связь не прерывалась. Другими словами, требовалось, чтобы соединение не прерывалось, пока функционируют приемная и передающая машины, даже если некоторые промежуточные машины или линии связи внезапно выходили из строя. Кроме того, от архитектуры требовалась определенная гибкость, поскольку предполагалось использовать приложения с различными требованиями, от переноса файлов до передачи речи в реальном времени.

Сегодня стек TCP/IP используется для связи компьютеров всемирной информационной сети Интернет, а также в огромном

числе корпоративных сетей. Комплект протоколов Интернета состоит из набора общедоступных (по сети) документов, созданных коллективными усилиями мирового сетевого сообщества. Передача данных в Интернете основана на принципе коммутации пакетов, в соответствии с которым поток данных, передаваемых от одного узла к другому, разбивается на пакеты, передающиеся в общем случае через систему коммуникаций и маршрутизаторов независимо друг от друга и вновь собирающиеся на приемной стороне. Конечные узлы – отправители и получатели информации, называются хостами (host), промежуточные устройства, оперирующие IP-пакетами (анализирующие и модифицирующие информацию IP-заголовков), называют шлюзами (gateway). Весь комплект протоколов базируется на IP-протоколе негарантированной доставки пакетов (дейтаграмм) без установления соединения.

Стек TCP/IP на нижнем уровне поддерживает все популярные стандарты физического и канального уровней для локальных сетей – это Ethernet, Token Ring, FDDI. Основными протоколами стека, давшими ему название, являются протоколы IP и TCP. Эти протоколы в терминологии модели OSI относятся к сетевому и транспортному уровням соответственно. IP обеспечивает продвижение пакета по составной сети, а TCP гарантирует надежность его доставки.

Сегодня стек TCP/IP представляет собой самый распространенный стек транспортных протоколов вычислительных сетей. Стремительный рост популярности Интернета привел и к изменениям в расстановке сил в мире коммуникационных протоколов – протоколы TCP/IP, на которых построен Интернет, стали быстро теснить бесспорного лидера прошлых лет – стек IPX/SPX компании Novell. Сегодня в мире общее количество компьютеров, на которых установлен стек TCP/IP, намного превышает количество компьютеров, на которых работает стек IPX/SPX.

Поскольку стек TCP/IP изначально создавался для глобальной сети Интернет, он имеет много особенностей, дающих ему преимущество перед другими протоколами, когда речь заходит о построении сетей, включающих глобальные связи. Существует большое количество локальных, корпоративных и территориаль-

ных сетей, непосредственно не являющихся частями Интернета, в которых также используют протоколы TCP/IP.

В частности, очень полезным свойством, делающим возможным применение этого протокола в больших сетях, является его способность фрагментировать пакеты. Действительно, большая составная сеть часто состоит из сетей, построенных на совершенно разных принципах. В каждой из этих сетей может быть установлена собственная величина максимальной длины единицы передаваемых данных (кадра). В таком случае при переходе из одной сети, имеющей большую максимальную длину, в сеть с меньшей максимальной длиной может возникнуть необходимость деления передаваемого кадра на несколько частей. Протокол IP стека TCP/IP эффективно решает эту задачу.

Другой особенностью технологии TCP/IP является гибкая система адресации, позволяющая проще, чем другие протоколы аналогичного назначения включать в интерсеть сети разных технологий. Это свойство также способствует применению стека TCP/IP для построения больших гетерогенных сетей.

Однако, как и всегда, за получаемые преимущества надо платить, и платой здесь оказываются высокие требования к ресурсам и сложность администрирования IP-сетей. Мощные функциональные возможности протоколов стека TCP/IP требуют для своей реализации больших вычислительных затрат. На сегодняшний день факт остается фактом – сегодня это самый популярный стек протоколов, широко используемый как в глобальных, так и локальных сетях.

В стеке TCP/IP определены 4 уровня (рис. 5.8), которые решают задачу организации надежной и производительной работы составной сети, отдельные части которой могут быть построены на основе разных сетевых технологий.

Все изначальные требования к сети ARPANET обусловили выбор модели сети с коммутацией пакетов, в основе которой лежал не имеющий соединений межсетевой уровень. Этот уровень, называемый *интернет-уровнем* или *межсетевым уровнем*, является основой всей архитектуры. Его задача заключается в обеспечении возможности каждого хоста посылать пакеты в любую сеть и независимо двигаться к пункту назначения (например, в другой сети). Они могут прибывать не в том порядке, в котором были

отправлены. Если требуется соблюдение порядка отправления, эту задачу выполняют более верхние уровни. Здесь можно усмотреть аналогию с почтовой системой. Человек может бросить несколько международных писем в почтовый ящик в одной стране, и они будут доставлены по правильным адресам в других странах. Вероятно, письма по дороге пройдут через несколько международных почтовых шлюзов, однако это останется прозрачным для корреспондентов. В каждой стране (то есть каждой сети) могут быть свои марки, свои предпочитаемые размеры конвертов и правила доставки, незаметные для пользователей почтовой службы.

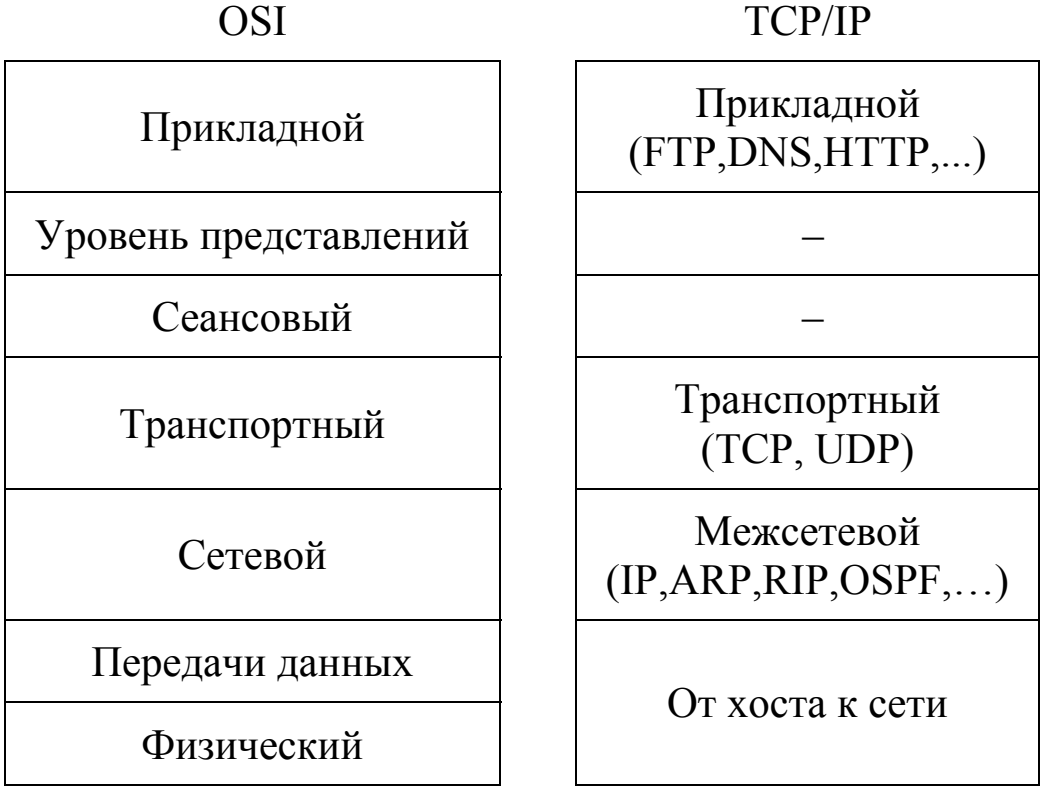


Рис. 5.8. Стек протоколов TCP/IP

Межсетевой уровень является стержнем всей архитектуры TCP/IP и обеспечивает перемещение пакетов в пределах всей составной сети. Поэтому можно утверждать, что межсетевой уровень модели TCP/IP функционально близок сетевому уровню модели OSI. Он определяет официальный формат пакета и протокол, называемый IP (Internet Protocol). Задачей межсетевого протокола является продвижение IP-пакетов между подсетями от одного пограничного маршрутизатора к другому, до тех пор, пока

пакет не попадет в сеть назначения. Протокол устанавливается на хостах и всех шлюзах. Протокол работает по принципу «по возможности», в соответствии с которым он не берет на себя ответственность за доставку пакета до узла назначения. Если пакет по каким-либо причинам теряется, то он не пытается повторить его передачу, а только посылает уведомление узлу-отправителю. Протокол изначально проектировался как средство передачи в составных сетях, состоящих из большого количества сетей, объединенных как локальными, так и глобальными связями. В связи с тем, что между двумя узлами таких сетей может быть проложено несколько возможных путей, то задача перемещения данных включает в себя задачу выбора маршрута пакета и недопущение закупорки транспортных артерий.

К уровню межсетевого взаимодействия также относятся протоколы сбора маршрутной информации RIP (Routing Internet Protocol) и OSPF (Open Shortest Path First). Для обмена информацией об ошибках между маршрутизаторами сети и узлом-источником пакета существует протокол межсетевых управляющих и динамических сообщений ICMP (Internet Control Message Protocol). Для преобразования адресов (из физических MAC-адресов в IP-адреса и наоборот) служат протоколы ARP (Address Resolution Protocol) и RARP (Reverse Address Resolution Protocol).

Уровень, расположенный над межсетевым уровнем модели TCP/IP, как правило, называют т р а н с п о р т н ы м . Он создан для того, чтобы одноранговые сущности на приемных и передающих хостах могли поддерживать связь, подобно транспортному уровню модели OSI. Протокол TCP (Transmission Control Protocol – протокол управления передачей), является надежным протоколом на основе соединений, позволяющим без ошибок доставлять байтовый поток с одной машины на любую другую машину объединенной сети. Протокол обеспечивает гарантированный поток данных между клиентами, установившими виртуальное соединение. Он разбивает входной поток байт на отдельные сообщения и передает их межсетевому уровню. На пункте назначения получающий TCP-процесс восстанавливает из полученных сообщений выходной поток. Кроме того, TCP осуществляет управление потоком, чтобы быстрый отправитель не завалил информацией медленного получателя.

Протокол позволяет нумеровать пакеты, подтверждать их прием, организовывать повторные передачи в случае потери, доставлять пакеты прикладному уровню в том порядке, в котором они были отправлены.

На транспортном уровне имеется другой протокол UDP (User Datagram Protocol) – простейший протокол пользовательских дейтаграмм, реализующий доставку «по возможности». Он используется в случае, если задача надежного обмена не ставится, либо реализуется средствами более высокого уровня (системными службами или пользовательскими приложениями).

От прикладного уровня транспортный уровень принимает задачу на передачу по сети данных, а после ее выполнения сообщает ему об этом. К межсетевому уровню транспортный уровень обращается как к инструменту, способному перемещать пакет по составной сети. Протоколы транспортного уровня устанавливаются на хостах.

В модели TCP/IP нет сеансового уровня и уровня представления. В этих уровнях не было необходимости, поэтому они не были включены в модель. Опыт работы с моделью OSI доказал правоту этой точки зрения: большинство приложений в них мало нуждаются.

Над транспортным уровнем располагается прикладной уровень. За долгие годы, использования в сетях различных стран и организаций стек TCP/IP вобрал в себя большое количество протоколов прикладного уровня. К ним относятся такие популярные протоколы, как протокол виртуального терминала *TELNET*, протокол переноса файлов *FTP* (File Transfer Protocol), простой протокол передачи электронной почты *SMTP* (Simple Mail Transfer Protocol). Протокол виртуального терминала позволяет пользователю регистрироваться на удаленном сервере и работать на нем. Протокол переноса файлов предоставляет эффективный способ перемещения информации с машины на машину. Электронная почта изначально представляла собой разновидность переноса файлов, однако позднее для нее был разработан специальный протокол. С годами было добавлено много других протоколов: *DNS* (Domain Name Service) – служба имен доменов, позволяющий преобразовывать имена хостов в сетевые адреса, *NNTP* (Network News Transfer Protocol)– сетевой протокол передачи но-

востей, *HTTP* (Hypertext Transfer Protocol) – протокол передачи гипертекстовой информации, используемый для создания страниц на World Wide Web, и многие другие. Протоколы прикладного уровня устанавливаются на хостах. Прикладной уровень реализуется программными системами, построенными в архитектуре клиент-сервер.

В эталонной модели TCP/IP не описывается подробно, что располагается ниже межсетевого уровня (Хост-сетевой уровень). Сообщается только, что хост соединяется с сетью при помощи какого-нибудь протокола, позволяющего ему посылать по сети IP-пакеты. Этот протокол никак не определяется и может меняться от хоста к хосту и от сети к сети.

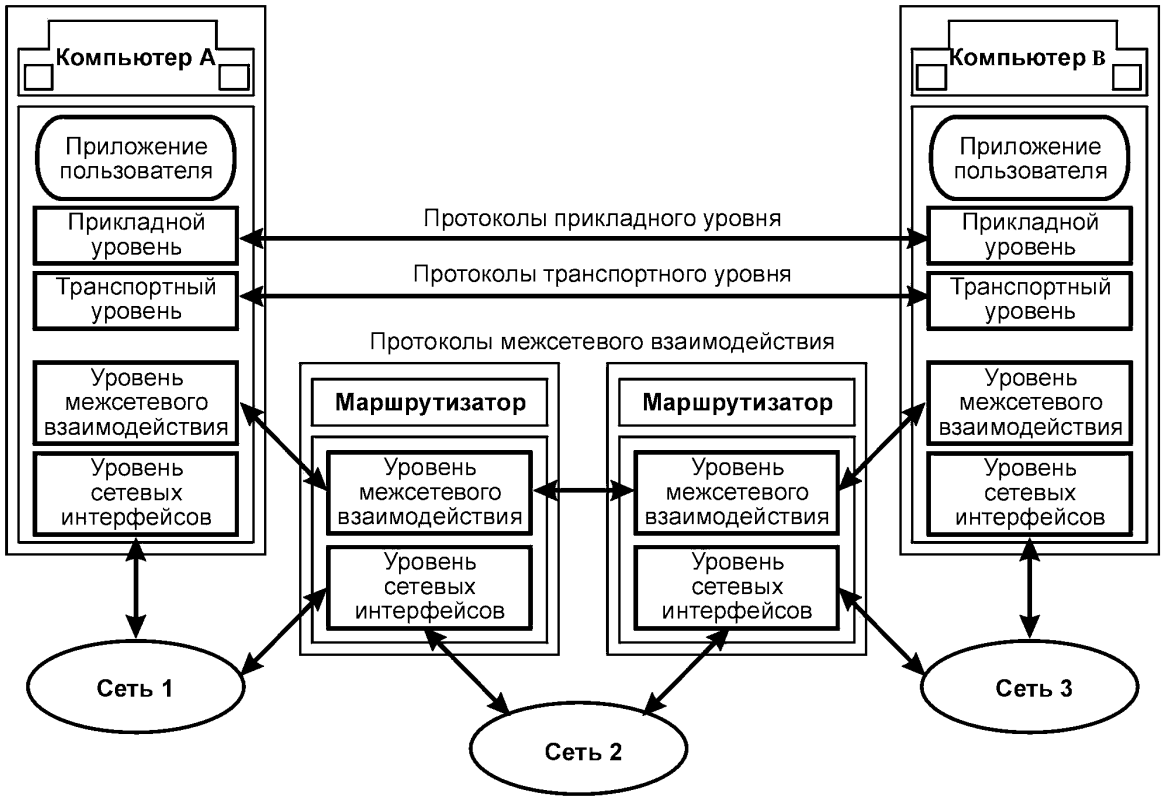


Рис. 5.9. Зависимость уровней стека TCP/IP от сети

Перемещение IP-пакета можно рассматривать как последовательность прыжков от шлюза к шлюзу, на каждом из которых определяется сетевой адрес следующего по маршруту шлюза. Чтобы добраться до следующего шлюза, необходимо пересечь некую подсеть. Для этого протоколы TCP/IP должны обратиться к транспортным средствам пересекаемой подсети с учетом ее технологии. В задачу интерфейса в этом случае входит упаковка IP-

пакета в единицу информации подсети и преобразование адреса шлюза назначения с учетом принятой для этой сети системы адресации.

Рассматривая многоуровневую архитектуру TCP/IP, можно выделить в ней, подобно архитектуре OSI, уровни, функции которых зависят от конкретной технической реализации сети, и уровни, функции которых ориентированы на работу с приложениями (рис. 5.9).

Протоколы прикладного уровня стека TCP/IP работают на компьютерах, выполняющих приложения пользователей. Даже полная смена сетевого оборудования в общем случае не должна влиять на работу приложений, если они получают доступ к сетевым возможностям через протоколы прикладного уровня.

Протоколы транспортного уровня зависят от сети уже в большей степени, так как они реализуют интерфейс к уровням, непосредственно организующим передачу данных по сети. Однако подобно протоколам прикладного уровня, протоколы транспортного уровня устанавливаются только на конечных узлах.

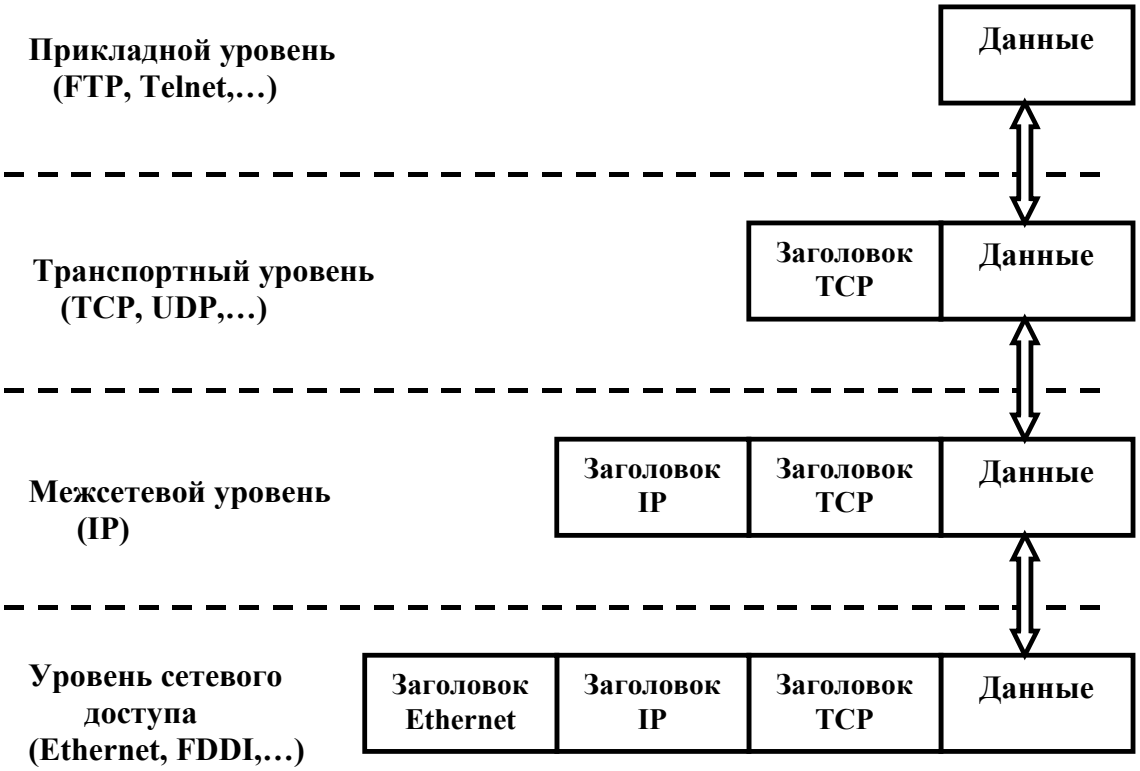


Рис. 5.10. Структура блоков данных стека TCP/IP

Протоколы двух нижних уровней являются сетезависимыми, программные модули протоколов межсетевого уровня и уровня сетевых интерфейсов устанавливаются на всех хостах и шлюзах.

При передаче данных между уровнями стека TCP/IP формируются соответствующие протокольные блоки данных. При передаче информации от прикладного процесса на каждом уровне добавляются соответствующие заголовки. После приема информации на узле назначения происходит отбрасывание заголовков уровней и в конечном итоге принимающий прикладной процесс получает данные. На нижнем уровне к IP-пакету добавляется заголовок, соответствующий технологии локальной сети (например, Ethernet). Структура блоков данных на каждом уровне стека TCP/IP представлена на рисунке 5.10.

5.6.4. Структура IP-пакета (IPv4)

Информация в TCP/IP передается пакетами со стандартизованной структурой, называемыми IP-дейтаграммами (IP Datagram), имеющими поле заголовка (IP Datagram Header) и поле данных (IP Datagram Data). Формат заголовка приведен на рис. 5.11, где он показан в виде шести 32-битных слов.

Поля имеют следующее назначение:

– Version, 4 бита – номер версии протокола, определяющий формат заголовка.

– IHL (Internet Header Length), 4 бита – длина заголовка в 32-битных словах. Обычно заголовок имеет длину в 20 байт (пять 32-битных слов), но иногда он может быть увеличен до 60 байт.

– Type of Service, 8 бит – абстрактное описание качества сервиса: биты 0 – 2 – Precedence (старшинство, преимущество) – параметр, определяющий приоритет трафика (большему значению соответствует больший приоритет). Маршрутизаторы и компьютеры могут принимать во внимание приоритет пакета и обрабатывать более важные в первую очередь.

Следующие три бита определяют критерии выбора маршрута. Реально выбор осуществляется между тремя альтернативами: малой задержкой, высокой пропускной способностью и высокой надежностью (достоверностью). Во многих случаях улучшение одного из параметров ведет к ухудшению других, кроме того, об-

работка каждого из параметров требует дополнительных вычислительных затрат.

бит 3 – Delay (задержка): 0 – нормальная, 1 – малая;

бит 4 – Throughput (пропускная способность): 0 – нормальная, 1 – высокая;

бит 5 – Reliability (надежность): 0 – нормальная, 1 – высокая;

биты 6-7 – резерв (нулевые значения).

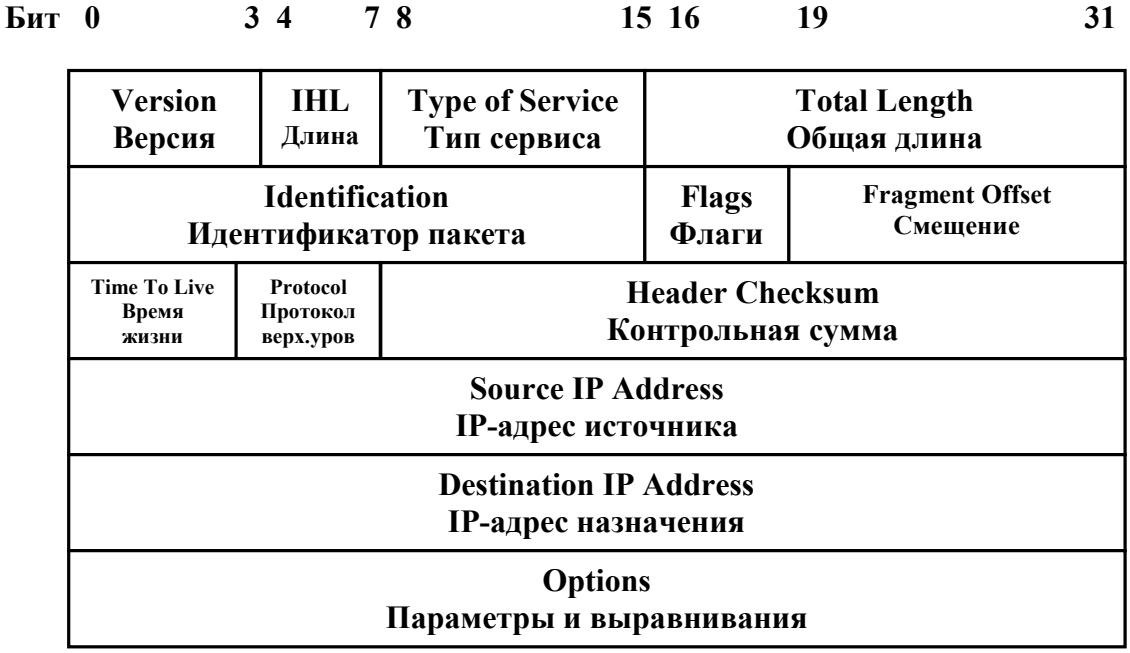


Рис. 5.11. Структура заголовка пакета IPv4

– Total Length, 16 бит – общая длина дейтаграммы (заголовок и данные) в байтах. Допускается длина до 65535 байт (ограничение в связи с длиной поля), но все хосты безусловно допускают прием пакетов длиной только до 576 байт. Пакеты большей длины рекомендуется посылать только по предварительной договоренности с принимающим хостом.

– Identification, 16 бит – идентификатор, назначаемый посылающим узлом для сборки фрагментов дейтаграмм. Все фрагменты должны иметь одинаковые значения этого поля.

– Flags, 3 бита – управляющие флаги, связанные с фрагментацией:

бит 0 – резерв, должен быть нулевым;

бит 1 – DF (Don' t Fragment – запрет фрагментирования): 0 – дейтаграмму можно фрагментировать, 1 – нельзя;

бит 2 – MF (More Fragments – будут еще фрагменты): 0 – последний фрагмент, 1 – не последний.

– Fragment Offset, 13 бит (смещение фрагмента)– местоположение фрагмента в дейтаграмме (смещение в 8-байтных блоках). Задает смещение поля данных пакета от начала общего поля данных исходного пакета, подвергшегося фрагментации. Первый фрагмент имеет нулевое смещение. Используется при сборке/разборке фрагментов пакетов при передачах их между сетями с разной длиной поля данных.

– Time to Live (TTL), 8 бит – время жизни пакета в сети в секундах. Начальное значение задается отправителем. В узлах сети, в которые попадает пакет, по истечении каждой секунды время жизни убавляется на одну секунду. Нулевое значение поля приводит к необходимости удаления дейтаграммы, не зависимо от того достигла ли она получателя. Поскольку современное оборудование редко задерживает пакет более чем на секунду, это поле может использоваться для подсчета промежуточных узлов. Заданием TTL можно управлять дальностью распространения пакетов: при TTL=1 пакет не может выйти за пределы подсети отправителя.

– Protocol, 8.бит – идентификатор протокола более высокого уровня, использующего поле данных пакета.

– Header Checksum, 16 бит – контрольная сумма заголовка. Сумма по модулю 2 всех 16-битных слов заголовка (вместе с контрольной суммой) должна быть нулевой. Контрольная сумма должна проверяться и пересчитываться в каждом шлюзе в связи с модификацией некоторых полей (TTL). Если контрольная сумма не верна, то пакет будет отброшен.

– Source Address, 32 бита – IP-адрес отправителя.

– Destination Address, 32 бита – IP-адрес получателя.

– Options – опции пакета, длина произвольна, но кратна 4 байтам (опции могут и отсутствовать).

На сегодняшний день определены пять разновидностей поля *Options*, однако не все маршрутизаторы поддерживают их всех: безопасность, строгая маршрутизация от источника, свободная маршрутизация от источника, запомнить маршрут, временной штамп.

Параметр «*Безопасность»* указывает уровень секретности дейтаграммы. Теоретически военный маршрутизатор может ис-

пользовать это поле, чтобы запретить маршрутизацию дейтаграммы через определенные государства. На практике все современные маршрутизаторы игнорируют этот параметр.

Параметр «*Строгая маршрутизация от источника»* задает полный путь следования дейтаграммы от отправителя до получателя в виде последовательности IP- адресов. Дейтаграмма обязана следовать именно по этому маршруту. Наибольшая польза этого параметра заключается в возможности системному менеджеру послать экстренные пакеты, когда таблицы маршрутизатора повреждены или для тестирования сети.

Параметр «*Свободная маршрутизация от источника»* требует, чтобы пакет прошел через указанный список маршрутизаторов в указанном порядке, но при этом по пути он может проходить через любые другие маршрутизаторы. Этот параметр наиболее всего полезен, когда по политическим или экономическим соображениям следует избегать прохождения пакетов через определенные государства.

Параметр «*Запомнить маршрут»* требует от всех маршрутизаторов, встречающихся по пути следования пакета, добавлять свой IP-адрес к полю Options. Этот параметр позволяет системным менеджерам вылавливать ошибки в алгоритмах маршрутизации

Наконец, параметр «*Временной штамп»* действует полностью аналогично параметру *«Запомнить маршрут»*, но кроме 32-разрядного IP-адреса каждый маршрутизатор также записывает 32-разрядную запись о текущем времени. Этот параметр также применяется в основном для отладки алгоритмов маршрутизации.

В дейтаграмму длиной 576 байт умещается 512-байтный блок данных и 64-байтный заголовок. Длина дейтаграммы определяется сетевым ПО так, чтобы она умещалась в поле данных сетевого кадра, осуществляющего ее транспортировку. Поскольку по пути следования к адресату могут встречаться сети с меньшим размером поля данных кадра, IP специфицирует единый для всех маршрутизаторов метод сегментации – разбивки дейтаграммы на фрагменты (тоже IP-дейтаграммы) и реассемблирования – обратной ее сборки приемником. Фрагментированная дейтаграмма собирается только ее окончательным приемником, поскольку отдельные фрагменты могут добираться до него различными путя-

ми. Порядок сборки определяется смещением фрагмента, перекрытие фрагментов и даже выход фрагмента за заявленный размер собираемого пакета, как правило, не контролируются. На основе этих свойств алгоритма сборки «умельцы» осуществляют взлом сетевых ОС. Возможна также конкатенация – соединение нескольких дейтаграмм в одну и сепарация – действие, обратное конкатенации.

5.6.5. Протокол (IPv6)

Всем понятно, что дни протокола IP в его теперешнем виде (IPv4) сочтены. В связи с лавинообразным ростом интереса к Интернету, начавшимся в середине 90-х годов, в третьем тысячелетии, скорее всего, им будет пользоваться гораздо большее количество пользователей, и особенно пользователей с принципиально иными требованиями. При неминуемой конвергенции компьютерной промышленности, средств связи и индустрии развлечений, возможно, очень скоро каждый телевизор планеты станет узлом Интернета, что в результате приведет к появлению миллиардов машин. В таких обстоятельствах становится очевидным, что протокол IP должен эволюционировать и стать более гибким. Предвидя появление этих проблем, проблемная группа проектирования Интернета IETF начала в 1990 г. работу над новой версией протокола IP, в которой никогда не должна возникнуть проблема нехватки адресов, а также будут решены многие другие проблемы. Кроме того, новая версия протокола должна была быть более гибкой и эффективной. Были сформулированы следующие основные цели.

1. Поддержка миллиардов хостов, даже при неэффективном использовании адресного пространства.
2. Уменьшение размера таблиц маршрутизации.
3. Упрощение протокола для ускорения обработки пакетов маршрутизаторами.
4. Лучшее обеспечение безопасности (аутентификации и конфиденциальности).
5. Уделение большего внимания типу сервиса, в частности, при передаче данных реального времени.

6. Добавление многоадресной рассылки с помощью указания области рассылки.

7. Возможность изменения положения хоста без необходимости изменять свой адрес.

8. Возможность дальнейшего развития протокола в будущем.

9. Возможность сосуществования старого и нового протоколов в течение нескольких лет.

Чтобы найти протокол, удовлетворяющий всем этим требованиям, IETF издал в RFC 1550 приглашение к дискуссиям и предложениям. После долгих обсуждений была выбрана версия, называемая в настоящий момент протоколом **SIPP** (Simple Internet Protocol Plus – простой Интернет-протокол плюс). Новому протоколу было дано обозначение **IPv6** (протокол IPv5 уже использовался в качестве экспериментального протокола потоков реального времени). Протокол IPv6 прекрасно справляется с поставленными задачами. Он обладает достоинствами протокола IP и лишен некоторых его недостатков (либо обладает ими в меньшей степени), к тому же наделен некоторыми новыми способностями. В общем случае протокол IPv6 не совместим с протоколом IPv4, но зато совместим со всеми другими протоколами Интернета.

Прежде всего, у протокола IPv6 поля адресов длиннее, чем у IPv4. Они имеют длину 16 байт, что решает основную проблему, поставленную при разработке протокола: обеспечить практически неограниченный запас Интернет-адресов.

Второе главное улучшение протокола IPv6 состоит в более простом заголовке пакета. Он состоит всего из 7 полей (вместо 13 у протокола IPv4). Таким образом, маршрутизаторы могут быстрее обрабатывать пакеты, что повышает производительность.

Третье основное усовершенствование заключается в лучшей поддержке необязательных параметров. Подобное изменение было существенным, так как в новом заголовке требуемые прежде поля стали необязательными. Кроме того, изменился способ представления необязательных параметров, что упростило для маршрутизаторов пропуск не относящихся к ним параметров и ускорило обработку пакетов.

В-четвертых, протокол IPv6 демонстрирует большой шаг вперед в области безопасности. Аутентификация и конфиденциальность являются ключевыми чертами нового IP-протокола.

Наконец, в новом протоколе было уделено больше внимания типу предоставляемых услуг. Для этой цели в заголовке пакета IPv4 было отведено 8-разрядное поле (на практике не используемое), но при ожидаемом росте мультимедийного трафика в будущем требовалось значительно больше разрядов.

Переход с протокола IPv4 на IPv6 не может произойти одновременно на всей сети Интернет. Первоначально появятся «островки» IPv6, которые будут общаться между собой. Со временем эти островки будут расширяться пока все они объединятся и Интернет будет полностью трансформирован. Учитывая огромные средства, вложенные в используемые в настоящее время IPv4-маршрутизаторы, процесс полного перехода на IPv6 по прогнозам займет около 10 лет.

Контрольные вопросы к главе 5

1. В чем заключается многоуровневый подход к разработке средств сетевого взаимодействия?
2. В чем заключается различие между понятиями «интерфейс» и «протокол» в многоуровневой модели взаимодействия узлов сети?
3. Перечислите основные уровни эталонной модели OSI.
4. Назовите основные функции каждого уровня в модели OSI.
5. Какие аппаратные коммуникационные средства соответствуют уровням OSI?
6. Назовите стандартные стеки коммуникационных протоколов и сферы их применения.
7. В чем заключается особенность стека протоколов OSI?
8. Каковы недостатки протокола IPX/SPX?
9. Перечислите основные уровни стека протоколов TCP/IP.
10. Назовите основные протоколы, работающие на каждом уровне стека TCP/IP.
11. Какие уровни протокола TCP/IP зависят от технической реализации сети?
12. Опишите структуру блоков данных на каждом уровне стека TCP/IP.
13. Какова структура заголовка IP-пакета (IPv4)?
14. В чем причина перехода на протокол IPv6?
15. Каковы основные отличия протокола IPv6 от IPv4?

ГЛАВА 6

СОСТАВНЫЕ СЕТИ

6.1. Архитектура составной сети

Сеть в общем случае рассматривается как совокупность нескольких сетей и называется составной сетью, или интерсетью (internetwork, или internet). Сети, входящие в составную сеть, называются подсетями (subnet), *составляющими сетями* или просто *сетями* (рис. 6.1).

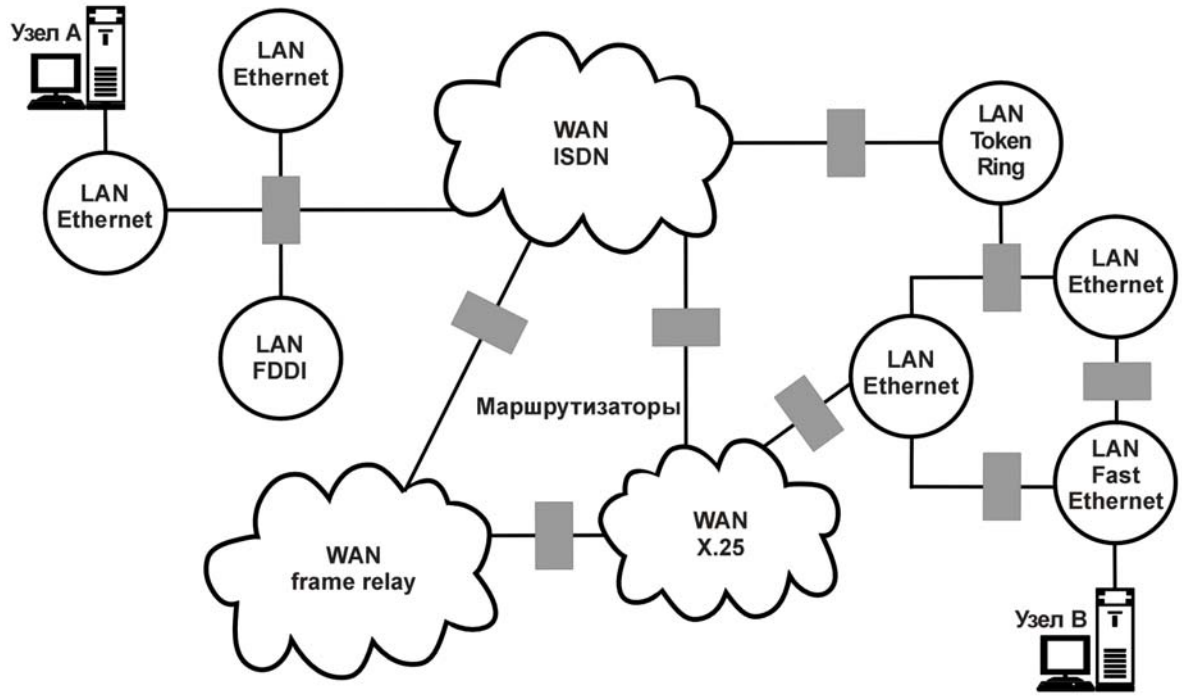


Рис. 6.1. Структура составной сети

Подсети соединяются между собой маршрутизаторами. Маршрутизатор (router) представляет собой устройство, имеющее один или несколько интерфейсов (портов) для подключения локальных сетей или удаленных соединений. На маршрутизаторы возлагаются и задачи фильтрации – пропускания пакетов, удов-

летворяющих определенным критериям, или наоборот, непропускания определенных пакетов. Компонентами составной сети могут являться как локальные, так и глобальные сети. Сети (подсети) составной сети могут отличаться различными параметрами, например системой адресации узлов, размерами передаваемых пакетов, параметрами безопасности, протоколами обмена и другими. Наличие различных сетей неизбежно приводит к существованию различных протоколов в каждой из них. Внутренняя структура каждой сети на рисунке не показана, так как она не имеет значения при рассмотрении сетевого протокола общей сети. Все узлы в пределах одной подсети взаимодействуют, используя единую для них технологию. Так, в составную сеть, показанную на рисунке, входит несколько сетей разных технологий: локальные сети Ethernet, Fast Ethernet, Token Ring, FDDI и глобальные сети frame relay, X.25, ISDN. Каждая из этих технологий способна обеспечить взаимодействие всех узлов в своей подсети, но не способна построить информационную связь между произвольно выбранными узлами, принадлежащими разным подсетям, например между узлом A и узлом B на рис. 6.1. Следовательно, для организации взаимодействия между любой произвольной парой узлов этой «большой» составной сети требуются дополнительные средства. Такие средства предоставляет сетевой уровень. Сетевой уровень выступает в качестве координатора, организующего работу всех подсетей, лежащих на пути продвижения пакета по составной сети. Для перемещения данных в пределах подсетей сетевой уровень обращается к используемым в этих подсетях технологиям. Хотя многие технологии локальных сетей (Ethernet, Token Ring, FDDI, Fast Ethernet и др.) используют одну и ту же систему адресации узлов, существует немало технологий, в которых применяются другие схемы адресации. Адреса, присвоенные узлам в соответствии с локальными технологиями подсетей, называют локальными. Чтобы сетевой уровень мог выполнить свою задачу, ему необходима собственная глобальная система адресации, не зависящая от способов адресации узлов в отдельных подсетях, которая позволила бы на сетевом уровне универсальным и однозначным способом идентифицировать любой узел составной сети. Естественным способом формирования сетевого адреса является уникальная нумерация всех подсетей со-

ставной сети и нумерация всех узлов в пределах каждой подсети. Таким образом, сетевой адрес представляет собой пару: номер сети (подсети) и номер узла.

В качестве номера узла может выступать либо локальный адрес этого узла (такая схема принята в стеке IPX/SPX), либо некоторое число, никак не связанное с локальной технологией, которое однозначно идентифицирует узел в пределах данной подсети. В первом случае сетевой адрес становится зависимым от локальных технологий, что ограничивает его применение. Например, сетевые адреса IPX/SPX рассчитаны на работу в составных сетях, объединяющих сети, в которых используются только MAC-адреса или адреса аналогичного формата. Второй подход более универсален, он характерен для стека TCP/IP. В том и другом случае каждый узел составной сети имеет наряду со своим локальным адресом еще один – универсальный сетевой адрес.

Данные, которые поступают на сетевой уровень и которые необходимо передать через составную сеть, снабжаются заголовком сетевого уровня. Данные вместе с заголовком образуют пакет. Заголовок пакета сетевого уровня имеет унифицированный формат, не зависящий от форматов кадров канального уровня тех сетей, которые могут входить в составную сеть, и несет, наряду с другой служебной информацией, данные о номере сети назначения этого пакета. Сетевой уровень определяет маршрут и перемещает пакет между подсетями. Каждый раз, когда пакет сетевого уровня передается из одной сети в другую, он извлекается из кадра первой подсети (освобождается от канального заголовка этой сети) и упаковывается в кадр (снабжается новым заголовком) канального уровня следующей подсети. Информацию, на основе которой делается эта замена, предоставляют служебные поля пакета сетевого уровня. В поле адреса назначения нового кадра указывается локальный адрес следующего маршрутизатора.

Если проводить аналогию между взаимодействием разнородных сетей и перепиской людей из разных стран, то сетевая информация – это общепринятый индекс страны, добавленный к адресу письма, написанному на одном из сотни языков земного шара, например на санскрите. И даже если это письмо должно пройти через множество стран, почтовые работники которых не знают санскрита, понятный им индекс страны-адресата подска-

жет, через какие промежуточные страны лучше передать письмо, чтобы оно кратчайшим путем попало в Индию. А уже там работники местных почтовых отделений смогут прочитать точный адрес, идентифицирующий город, улицу, дом и индивидуума, и доставить письмо адресату, так как адрес написан на языке и в форме, принятой в данной стране.

Основным полем заголовка сетевого уровня является номер сети-адресата. В протоколах локальных сетей такого поля в кадрах не предусмотрено, так как предполагалось, что все узлы принадлежат одной сети. Явная нумерация сетей позволяет протоколам сетевого уровня составлять точную карту межсетевых связей и выбирать рациональные маршруты при любой их топологии, в том числе альтернативные маршруты, если они имеются, что не умеют делать мосты и коммутаторы. Кроме номера сети заголовок сетевого уровня должен содержать и другую информацию, необходимую для успешного перехода пакета из сети одного типа в сеть другого типа. К такой информации может относиться, например:

– номер фрагмента пакета, необходимый для успешного проведения операций сборки-разборки фрагментов при соединении сетей с разными максимальными размерами пакетов;

– время жизни пакета, указывающее, как долго он путешествует по интерсети, это время может использоваться для уничтожения «заблудившихся» пакетов;

– качество услуги – критерий выбора маршрута при межсетевых передачах – например, узел-отправитель может потребовать передать пакет с максимальной надежностью, возможно, в ущерб времени доставки.

Когда две или более сети организуют совместную транспортную службу, то такой режим взаимодействия обычно называют межсетевым взаимодействием (internetworking). В результате наличия разнообразных сетей легко представить следующий сценарий взаимодействия компьютеров:

1. ЛС–ЛС (локальная сеть–локальная сеть).
2. ЛС–ГС (локальная сеть–глобальная сеть).
3. ГС–ГС (глобальная сеть–глобальная сеть).
4. ЛС–ГС–ЛС (локальная сеть–глобальная сеть–локальная сеть).

Эти четыре типа соединений показаны на рис. 6.2 в виде пунктирных линий.

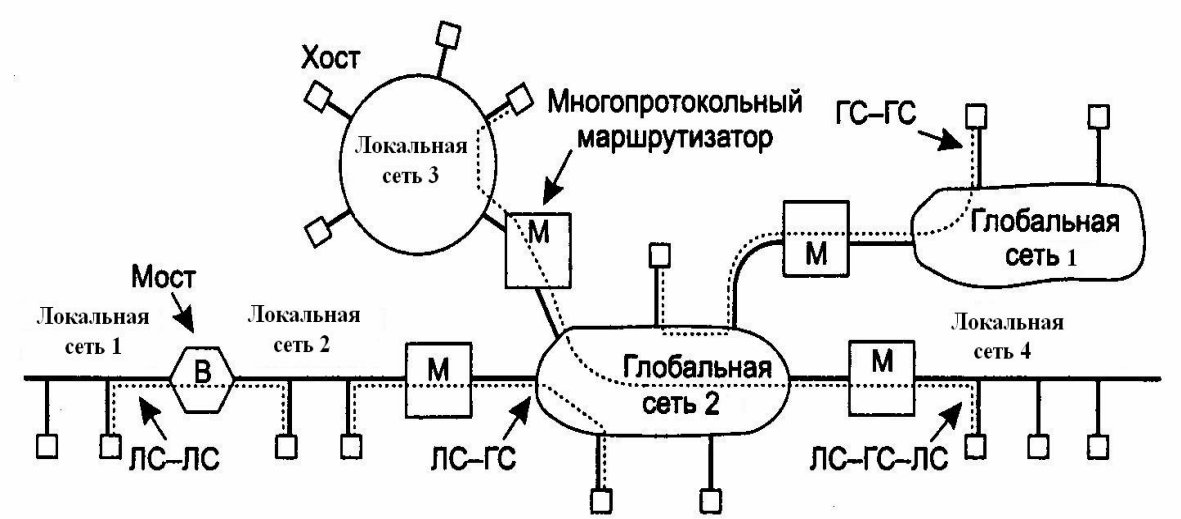


Рис. 6.2. Типы межсетевого взаимодействия

В каждом случае в месте соединения двух различных сетей для преобразования пакетов, передаваемых из одной сети в другую, необходимо установить «черный ящик». Название черного ящика, соединяющего две сети, зависит от сетевого уровня, на котором он выполняет свою работу. Некоторые общеупотребительные названия приведены ниже (хотя по терминологии в данной области единого мнения нет).

Уровень 1. Повторители копируют отдельные биты из одного сегмента кабеля в другой.

Уровень 2. Мосты хранят и посылают дальше кадры уровня передачи данных между локальными сетями.

Уровень 3. Многопротокольные маршрутизаторы передают пакеты между разнородными сетями.

Уровень 4. Транспортные шлюзы соединяют байтовые потоки на транспортном уровне.

Выше 4. Прикладные шлюзы позволяют объединять сети на уровне выше 4.

Повторители являются низкоуровневыми устройствами, которые просто усиливают или восстанавливают слабые сигналы. Они требуются для передачи данных по длинным кабелям.

В отличие от повторителей, копирующих биты из одного кабеля в другой, **мосты** являются устройствами с промежуточным

хранением. Мост принимает кадр целиком и передает его уровню передачи данных, где проверяется его контрольная сумма. Затем кадр посылается вниз на физический уровень для пересылки в другую сеть. Перед отправкой кадра в другую сеть мосты могут производить некоторые изменения кадра, например, добавлять или удалять некоторые поля из заголовка кадра. Поскольку мосты представляют собой устройства уровня передачи данных, они не занимаются заголовками сетевого и более высоких уровней, а также не могут принимать решения или производить изменения, зависящие от вышестоящих уровней.

Многопротокольные маршрутизаторы концептуально близки к мостам, с той разницей, что они применяются на сетевом уровне. Они просто принимают пакеты по одной линии и передают их по другой, как и обычные маршрутизаторы, но линии могут принадлежать различным сетям и использовать различные протоколы. Как и все маршрутизаторы, многопротокольные маршрутизаторы работают на сетевом уровне.

Транспортные шлюзы соединяют две сети на транспортном уровне. Наконец, **шлюзы прикладного уровня** соединяют две части приложения на прикладном уровне.

6.2. Модели передачи данных в составной сети

Наиболее распространенными являются два стиля объединения сетей: ориентированный на сцепление виртуальных каналов и дейтаграммный Интернет-стиль.

В сцепленной модели виртуальных каналов, показанной на рис. 6.3, соединение с хостом в удаленной сети устанавливается способом, близким к тому, как устанавливаются обычные соединения. Подсеть видит, что адресат является удаленным, и строит виртуальный канал к ближайшему маршрутизатору из сети адресата. Затем она создает виртуальный канал от этого маршрутизатора к внешнему «шлюзу» (многопротокольному маршрутизатору). Этот шлюз запоминает существование созданного виртуального канала в своих таблицах и продолжает строить другой виртуальный канал к маршрутизатору в соседней

подсети. Процесс продолжается до тех пор, пока не будет достигнут хост-получатель.

Когда по проложенному пути начинают идти пакеты данных, каждый шлюз переправляет их дальше, преобразуя формат пакетов. Очевидно, что все информационные пакеты будут передаваться по одному и тому же пути и, таким образом, прибудут к пункту назначения с сохранением порядка отправления. Таким образом, может быть построен сквозной виртуальный канал, пролегающий по нескольким сетям с различными протоколами.

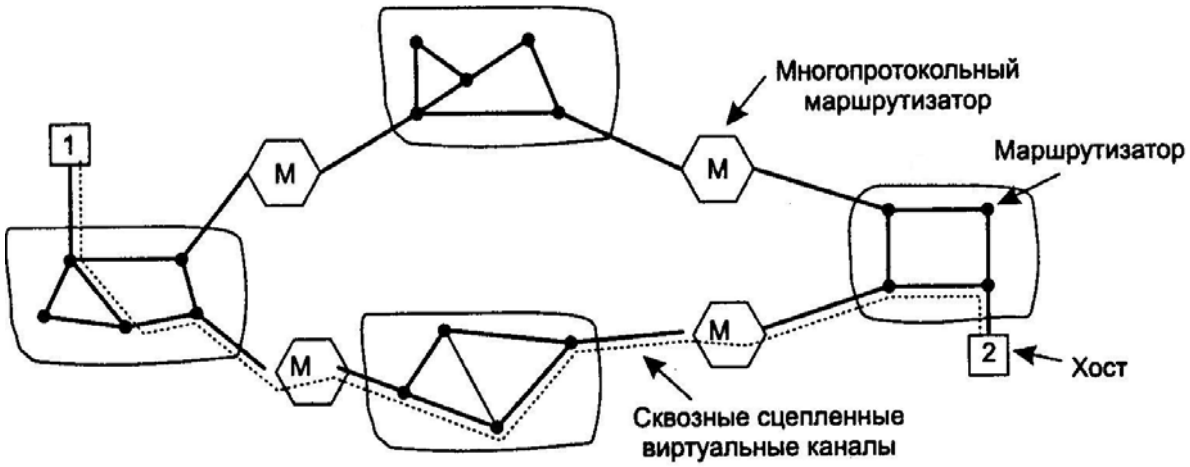


Рис. 6.3. Модель виртуальных каналов

Существенной особенностью данного подхода является то, что последовательность виртуальных пакетов устанавливается от источника через один или более шлюзов к приемнику. Каждый шлюз хранит таблицы, содержащие информацию о проходящих через них виртуальных каналах. Такая схема лучше всего работает, когда все сети обладают примерно одинаковыми свойствами. Например, если все они гарантируют надежную доставку пакетов сетевого уровня, то весь путь от источника до приемника также будет надежным. Аналогично, если ни одна из них не гарантирует надежной доставки, то и соединение виртуальных каналов также не будет надежным, С другой стороны, если машина-источник находится в сети, гарантирующей надежную доставку, а одна из промежуточных сетей может терять пакеты, то соединение виртуальных каналов фундаментально изменит сущность службы.

Альтернативной моделью объединения сетей является дейтаграммная модель, показанная на рис. 6.4. В данной модели единственная служба, которую сетевой уровень предоставляет транспортному уровню, состоит в возможности посылать в сеть дейтаграммы и надеяться на лучшее.

На сетевом уровне нет никакого упоминания о виртуальных каналах, не говоря уже об их сцеплении. В этой модели нет требования следования всех пакетов по одному и тому же маршруту, если они принадлежат к одному соединению. Дейтаграммы от хоста 1 к хосту 2 могут выбирать различные маршруты по объединенной сети. Выбор маршрута производится независимо для каждого пакета, возможно, в зависимости от текущего состояния трафика в сети. Такая стратегия может использовать различные маршруты и, таким образом, достигать большей пропускной способности, чем модель сцепленных виртуальных каналов. С другой стороны, не дается никакой гарантии того, что пакеты прибудут к получателю в нужном порядке, если они вообще прибудут. В этом случае необходим универсальный межсетевой пакет, который распознавался бы всеми маршрутизаторами. Именно эта идея была взята за основу при разработке IP-пакетов, то есть пакетов, созданных для передачи по разным сетям.

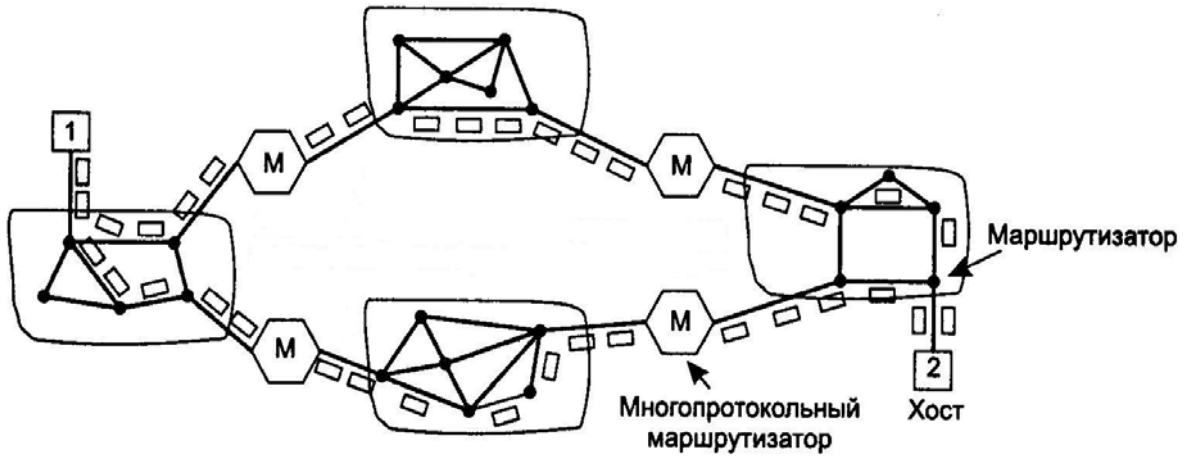


Рис. 6.4. Дейтаграммная модель

Подведем краткие итоги обсуждения способов объединения сетей. Модель сцепленных виртуальных каналов обладает рядом недостатков: маршрутизаторы должны хранить таблицы с записями для каждого открытого соединения, при возникновении за-

тора обходные пути не используются, выход маршрутизатора из строя прерывает все проходящие через него виртуальные каналы. Кроме того, очень сложно, может даже невозможно, реализовать систему виртуальных каналов, если в состав объединенной сети входит хотя бы одна ненадежная дейтаграммная сеть.

В случае дейтаграммного подхода к объединению сетей достигается более высокая надежность в случае отказов маршрутизаторов, однако требуются более длинные заголовки пакетов. В объединенной сети, как и в единой дейтаграммной сети, возможно применение различных адаптивных алгоритмов выбора маршрута. Главное преимущество дейтаграммного подхода к объединению сетей заключается в том, что для него не требуется, чтобы объединяемые сети были дейтаграммными или сетями виртуальных каналов. К дейтаграммным сетям относятся многие локальные сети, мобильные сети и даже некоторые глобальные сети. При включении одной из этих сетей в объединенную сеть стратегия объединения сетей на основе виртуальных каналов встречает серьезные трудности.

Объединение сетей в общем случае является исключительно сложной задачей. Однако есть частный случай, реализация которого вполне осуществима. Это случай, при котором хосты источник и приемник находятся в сетях одного типа, но между ними находится сеть другого типа. Например, представьте себе международный банк, у которого имеется две TCP/IP сети на основе Ethernet в разных городах (для примера в Лондоне и Париже), и эти сети соединены глобальной сетью, как показано на рис. 6.5.

Метод решения данной проблемы называется *туннелированием*. Чтобы послать IP-пакет хосту 2, хост 1 формирует пакет, содержащий IP-адрес хоста 2, помещает его в кадр Ethernet, адресованный парижскому многопротокольному маршрутизатору, и пересылает его по сети Ethernet. Получив кадр, многопротокольный маршрутизатор извлекает IP-пакет, помещает его в поле полезной нагрузки пакета сетевого уровня глобальной сети и пересылает его лондонскому многопротокольному маршрутизатору. Когда пакет попадает туда, лондонский многопротокольный маршрутизатор извлекает IP-пакет и посылает его хосту 2 внутри кадра Ethernet.

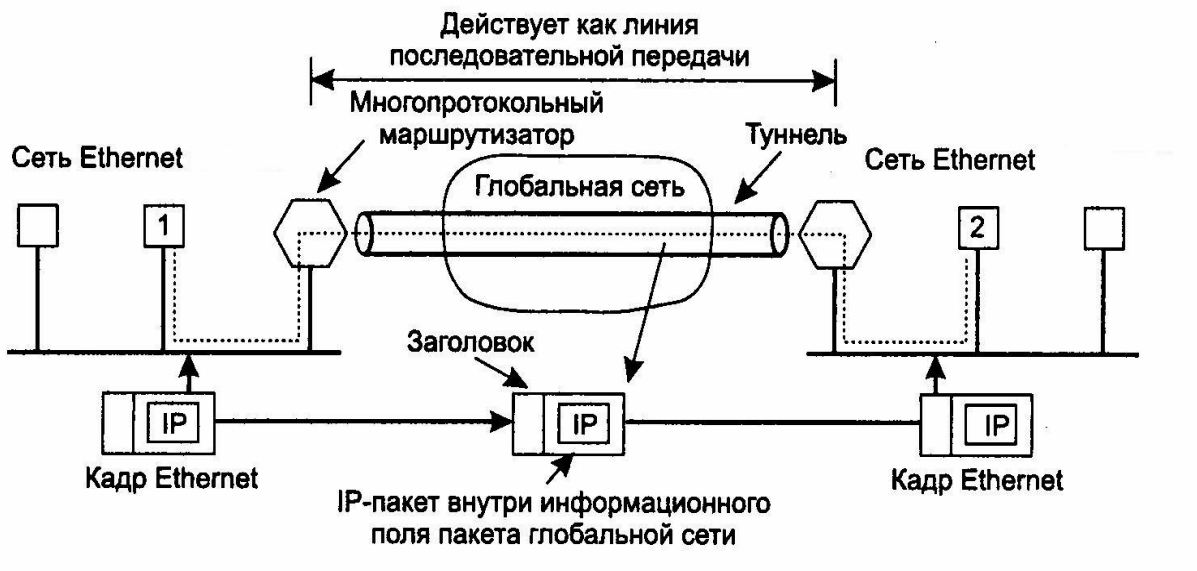


Рис.6.5. Модель туннелирования

Глобальную сеть при этом можно рассматривать как большой туннель, простирающийся от одного многопротокольного маршрутизатора до другого. IP-пакет просто перемещается от одного конца туннеля к другому, помещенный в удобную упаковку. Ему не нужно беспокоиться о взаимодействии с глобальной сетью. Это также не касается ни хостов, ни сети Ethernet. Переупаковкой пакета и переадресацией занимаются многопротокольные маршрутизаторы, для чего им нужно уметь разбираться в IP-адресах и обладать информацией о формате пакетов глобальной сети. В результате весь путь от середины одного многопротокольного маршрутизатора до середины другого действует как линия последовательной передачи.

6.3. Интернет как составная сеть

На сетевом уровне Интернет можно рассматривать как набор подсетей или *автономных систем*, соединенных друг с другом. Структуры как таковой у Интернета нет, но есть несколько магистралей. Они собраны из высокопропускных линий и быстрых маршрутизаторов. К магистралям присоединены региональные (среднего уровня) сети, с которыми соединяются локальные сети многочисленных организаций и поставщиков Интернет-услуг. Схема этой квазииерархической организации показана на рис. 6.6.

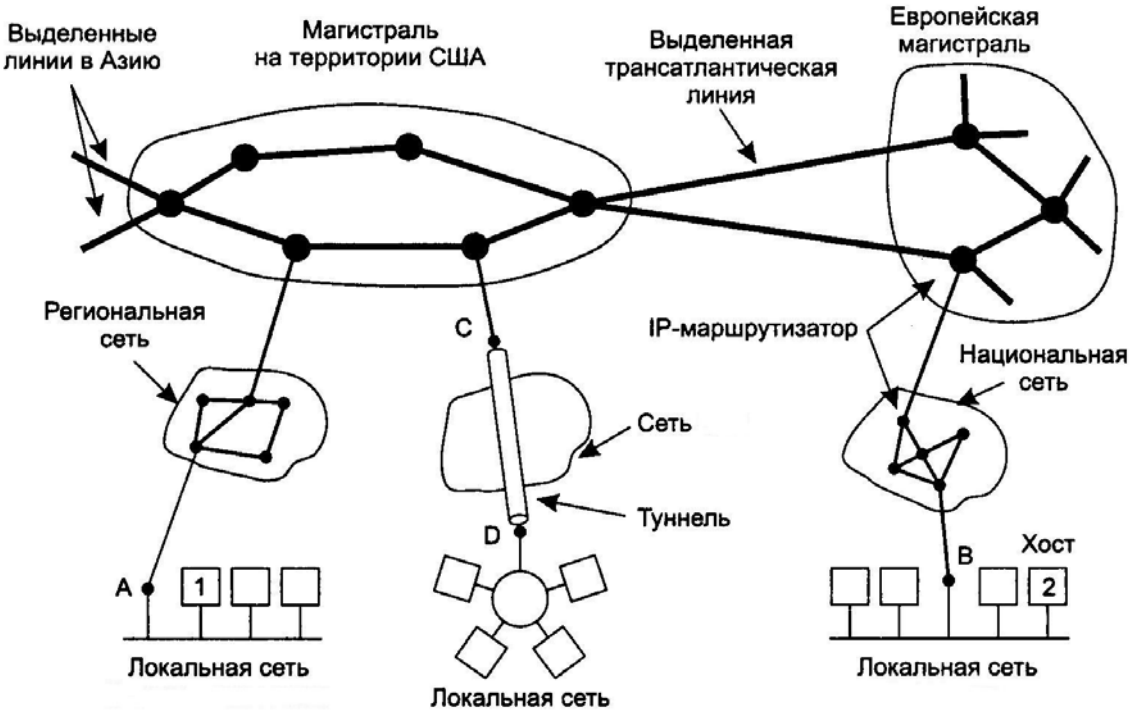


Рис. 6.6. Структура глобальной сети (Интернет)

Вся эта конструкция удерживается вместе протоколом сетевого уровня сети Интернет (IP). В отличие от большинства протоколов сетевого уровня, Интернет-протокол с самого начала разрабатывался как протокол межсетевого обмена. Его работа заключается в приложении максимума усилий по транспортировке дейтаграмм от отправителя к получателю, независимо от того, находятся ли эти машины в одной и той же сети или нет. Связь в Интернете работает следующим образом. Транспортный уровень берет поток данных и разбивает его на дейтаграммы. Теоретически размер дейтаграмм может достигать 64 Кбайт, однако на практике они обычно около 1500 байт. Каждая дейтаграмма пересылается по Интернету, возможно, разбиваясь при этом на более мелкие фрагменты, собираемые сетевым уровнем получателя в оригинальную дейтаграмму. Затем эта дейтаграмма передается транспортному уровню, вставляющему ее во входной поток получающего процесса.

6.4. Принципы маршрутизации

При передаче пакетов между двумя конечными узлами в составной сети одной из важнейших задач является определение

маршрута. Процесс выбора конкретного маршрута называется маршрутизацией. Рассмотрим принципы маршрутизации на примере составной сети, показанной на рисунке 6.7.

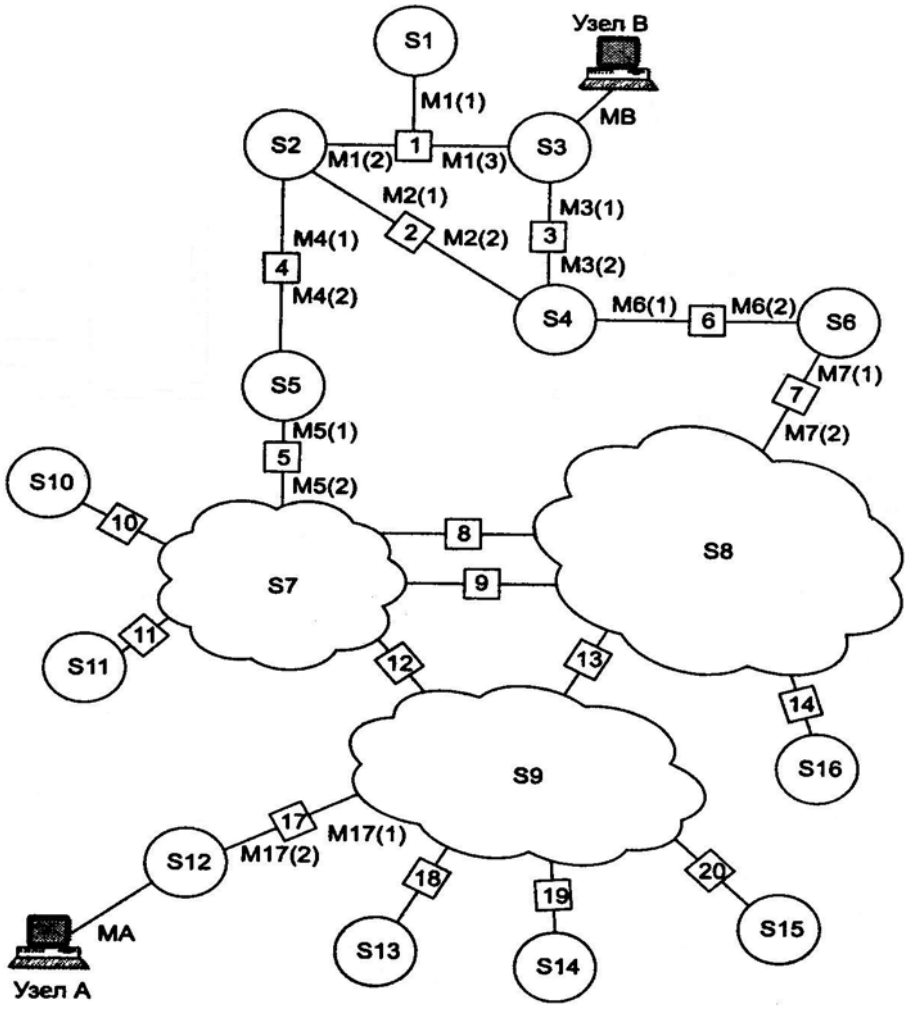


Рис. 6.7. Принципы маршрутизации в составной сети

В этой сети 20 маршрутизаторов (M1, M2,…, M20) объединяют 16 сетей (S1, S2,…, S16) в общую сеть. Маршрутизаторы имеют по несколько портов, к которым присоединяются сети. Каждый порт маршрутизатора можно рассматривать как отдельный узел сети: он имеет собственный сетевой адрес и собственный локальный адрес в той подсети, которая к нему подключена. Например, маршрутизатор под номером 1 имеет три порта, к которым подключены сети S1, S2, S3. На рисунке сетевые адреса этих портов обозначены как M1(1), M1(2) и M1(3). Порт M1(1) имеет локальный адрес в сети с номером S1, порт M1(2) – в сети S2, а порт M1(3) – в сети S3. Таким образом, маршрутизатор

можно рассматривать как совокупность нескольких узлов, каждый из которых входит в свою сеть. Как единое устройство маршрутизатор не имеет ни отдельного сетевого адреса, ни какого-либо локального адреса.

В сложных составных сетях почти всегда существует несколько альтернативных маршрутов для передачи пакетов между двумя конечными узлами. Маршрут – это последовательность маршрутизаторов, которые должен пройти пакет от отправителя до получателя. Так, пакет, отправленный из узла А в узел В, может пройти через маршрутизаторы 17, 12, 5, 4 и 1 или маршрутизаторы 17, 13, 7, 6 и 3. Нетрудно найти еще несколько маршрутов между узлами А и В. Задачу выбора маршрута из нескольких возможных решают маршрутизаторы, а также конечные узлы. Маршрут выбирается на основании имеющейся у этих устройств информации о текущей конфигурации сети, а также на основании указанного критерия выбора маршрута. Обычно в качестве критерия выступает задержка прохождения маршрута отдельным пакетом или средняя пропускная способность маршрута для последовательности пакетов. Часто также используется весьма простой критерий, учитывающий только количество пройденных в маршруте промежуточных маршрутизаторов (хопов).

Чтобы по адресу сети назначения можно было выбрать рациональный маршрут дальнейшего следования пакета, каждый конечный узел и маршрутизатор анализируют специальную информационную структуру, которая называется таблицей маршрутизации. Используя условные обозначения для сетевых адресов маршрутизаторов и номеров сетей в том виде, как они приведены на рис. 6.7, посмотрим, как могла бы выглядеть таблица маршрутизации, например, в маршрутизаторе 4 (табл. 6.1).

Примечание

Таблица 6.1 значительно упрощена по сравнению с реальными таблицами маршрутизации, например, отсутствуют столбцы с признаками состояния маршрута, временем, в течение которого действительны записи данной таблицы. Вместо номера сети назначения может быть указан полный сетевой адрес отдельного узла назначения.

Кроме того, как уже было сказано, здесь указаны адреса сетей условного формата, не соответствующие какому-либо определенному сетевому протоколу. Тем не менее, эта таблица содержит основные поля, имеющиеся в реальных таблицах при использовании конкретных сетевых протоколов, таких, как IP или IPX.

Таблица 6.1.

Номер сети назначения	**Сетевой адрес следующего порта маршрутизатора**	**Сетевой адрес выходного порта**	**Расстояние до сети назначения**
S1	M1(2)	M4(1)	1
S2	–	M4(1)	0
S3	M1(2)	M4(1)	1
S4	M2(1)	M4(1)	1
S5	–	M4(2)	0
S6	M2(1)	M4(1)	2
Default	M5(1)	M4(2)	–

В первом столбце приведенной выше таблицы перечисляются номера сетей, входящих в интерсеть. В каждой строке таблицы следом за номером сети указывается сетевой адрес следующего маршрутизатора (более точно, сетевой адрес соответствующего порта следующего маршрутизатора), на который надо направить пакет, чтобы тот передвигался по направлению к сети с данным номером по рациональному маршруту. Когда на маршрутизатор поступает новый пакет, номер сети назначения, извлеченный из поступившего кадра, последовательно сравнивается с номерами сетей из каждой строки таблицы. Строка с совпавшим номером сети указывает, на какой ближайший маршрутизатор следует направить пакет. Например, если на какой-либо порт маршрутизатора 4 поступает пакет, адресованный в сеть S6, то из таблицы маршрутизации следует, что адрес следующего маршрутизатора – M2(1), то есть очередным этапом движения данного пакета будет движение к порту 1 маршрутизатора 2.

Поскольку пакет может быть адресован в любую сеть составной сети, может показаться, что каждая таблица маршрутизации должна иметь записи обо всех сетях, входящих в составную сеть. Но при таком подходе в случае крупной сети объем таблиц маршрутизации может оказаться очень большим, что повлияет на время ее просмотра, потребует много места для хранения и т. п.

Поэтому на практике число записей в таблице маршрутизации стараются уменьшить за счет использования специальной записи – *маршрутизатор по умолчанию* (*default*).

Действительно, если принять во внимание топологию составной сети, то в таблицах маршрутизаторов, находящихся на периферии составной сети, достаточно записать номера сетей, непосредственно подсоединенных к данному маршрутизатору или расположенных поблизости, на тупиковых маршрутах. Обо всех же остальных сетях можно сделать в таблице единственную запись, указывающую на маршрутизатор, через который пролегает путь ко всем этим сетям. Такой маршрутизатор называется маршрутизатором по умолчанию, а вместо номера сети в соответствующей строке помещается особая запись, например Default. В нашем примере таким маршрутизатором по умолчанию для сети S5 является маршрутизатор 5, точнее его порт M5(1). Это означает, что путь из сети S5 почти ко всем сетям большой составной сети пролегает через этот порт маршрутизатора. Перед тем как передать пакет следующему маршрутизатору, текущий маршрутизатор должен определить, на какой из нескольких собственных портов он должен поместить данный пакет. Для этого служит третий столбец таблицы маршрутизации. Еще раз подчеркнем, что каждый порт идентифицируется собственным сетевым адресом.

Некоторые реализации сетевых протоколов допускают наличие в таблице маршрутизации сразу нескольких строк, соответствующих одному и тому же адресу сети назначения. В этом случае при выборе маршрута принимается во внимание столбец «Расстояние до сети назначения». При этом под расстоянием понимается любая метрика, используемая в соответствии с заданным в сетевом пакете критерием. Расстояние может измеряться *хопами*, временем прохождения пакета по линиям связи, какой-либо характеристикой надежности линий связи на данном маршруте или другой величиной, отражающей качество данного маршрута по отношению к заданному критерию. В табл. 6.1 расстояние между сетями измерялось хопами. Расстояние для сетей, непосредственно подключенных к портам маршрутизатора, здесь принимается равным 0.

Наличие нескольких маршрутов к одному узлу делают возможным передачу трафика к этому узлу параллельно по несколь-

ким каналам связи, что повышает пропускную способность и надежность сети.

Задачу маршрутизации решают не только промежуточные узлы-маршрутизаторы, но и конечные узлы – компьютеры. Средства сетевого уровня, установленные на конечном узле, при обработке пакета должны, прежде всего, определить, направляется ли он в другую сеть или адресован какому-нибудь узлу данной сети. Если номер сети назначения совпадает с номером данной сети, то пакету не требуется решать задачу маршрутизации. Если же номера сетей отправления и назначения не совпадают, то маршрутизация нужна.

Таблицы маршрутизации конечных узлов полностью аналогичны таблицам маршрутизации, хранящимся на маршрутизаторах. Однако, если маршрутизаторы обычно автоматически создают таблицы маршрутизации, обмениваясь служебной информацией, то для конечных узлов таблицы маршрутизации часто создаются вручную администраторами и хранятся в виде постоянных файлов на дисках.

6.5. Протоколы маршрутизации

Задача маршрутизации решается на основе анализа таблиц маршрутизации, размещенных во всех маршрутизаторах и конечных узлах сети. Основная работа по созданию таблиц маршрутизации выполняется автоматически, но и возможность вручную скорректировать или дополнить таблицу тоже, как правило, предусматривается. Для автоматического построения таблиц маршрутизации маршрутизаторы обмениваются информацией о топологии составной сети в соответствии со специальным служебным протоколом. Протоколы этого типа называются протоколами маршрутизации (или маршрутизирующими протоколами).

Протоколы маршрутизации (например, RIP, OSPF) следует отличать от собственно сетевых протоколов (например, IP, IPX). Те и другие выполняют функции сетевого уровня модели OSI – участвуют в доставке пакетов адресату через разнородную составную сеть. Но в то время как первые собирают и передают по сети чисто служебную информацию, вторые предназначены для

передачи пользовательских данных, как это делают протоколы канального уровня. Протоколы маршрутизации используют сетевые протоколы как транспортное средство. При обмене маршрутной информацией пакеты протокола маршрутизации помещаются в поле данных пакетов сетевого уровня или даже транспортного уровня, поэтому с точки зрения вложенности пакетов протоколы маршрутизации формально следовало бы отнести к более высокому уровню, чем сетевой.

В том, что маршрутизаторы для принятия решения о продвижении пакета обращаются к адресным таблицам, можно увидеть их некоторое сходство с мостами и коммутаторами. Однако природа используемых ими адресных таблиц значительно различается. Вместо MAC-адресов в таблицах маршрутизации указываются номера сетей, которые соединяются в интерсеть. Другим отличием таблиц маршрутизации от адресных таблиц мостов является способ их создания. В то время как мост строит таблицу, пассивно наблюдая за проходящими через него информационными кадрами, посылаемыми конечными узлами сети друг другу, маршрутизаторы по своей инициативе обмениваются специальными служебными пакетами, сообщая соседям об известных им сетях в интерсети, маршрутизаторах и о связях этих сетей с маршрутизаторами. Обычно учитывается не только топология связей, но и их пропускная способность и состояние. Это позволяет маршрутизаторам быстрее адаптироваться к изменениям конфигурации сети, а также правильно передавать пакеты в сетях с произвольной топологией.

С помощью протоколов маршрутизации маршрутизаторы составляют карту связей сети той или иной степени подробности. На основании этой информации для каждого номера сети принимается решение о том, какому следующему маршрутизатору надо передавать пакеты, направляемые в эту сеть, чтобы маршрут оказался рациональным. Результаты этих решений заносятся в таблицу маршрутизации. При изменении конфигурации сети некоторые записи в таблице становятся недействительными. В таких случаях пакеты, отправленные по ложным маршрутам, могут «зацикливаться» и теряться. От того, насколько быстро протокол маршрутизации приводит в соответствие содержимое таблицы реальному состоянию сети, зависит качество работы всей сети.

Выводы

Маршрут – это последовательность маршрутизаторов, которые должен пройти пакет от отправителя до получателя. Задачу выбора маршрута из нескольких возможных решают маршрутизаторы и конечные узлы на основе таблиц маршрутизации. Записи в таблицу могут вноситься вручную администратором и автоматически – протоколами маршрутизации.

Протоколы маршрутизации (например, RIP или OSPF) следует отличать от собственно сетевых протоколов (например, IP или IPX). В то время как первые собирают и передают по сети служебную информацию о возможных маршрутах, вторые предназначены для передачи пользовательских данных.

Сетевые протоколы и протоколы маршрутизации реализуются в виде программных модулей на конечных узлах-компьютерах и на промежуточных узлах-маршрутизаторах.

Маршрутизатор представляет собой сложное многофункциональное устройство, в задачи которого входит: построение таблицы маршрутизации, определение на ее основе маршрута, буферизация, фрагментация и фильтрация поступающих пакетов, поддержка сетевых интерфейсов. Функции маршрутизаторов могут выполнять как специализированные устройства, так и универсальные компьютеры с соответствующим программным обеспечением.

6.6. Фрагментация пакетов

Каждая сеть ограничивает размер своих пакетов. Эти пределы вызваны различными причинами, среди которых есть следующие:

1. Аппаратные.
2. Операционная система (например, все буферы имеют размер 512 байт).
3. Протоколы (например, количество битов в поле длины пакета).
4. Соответствие какому-либо международному или национальному стандарту.
5. Желание снизить количество пересылаемых повторно (из-за ошибок передачи) пакетов.

6. Желание предотвратить ситуацию, когда один пакет слишком долгое время занимает канал.

Результатом действия всех этих факторов является тот факт, что разработчики не могут выбирать максимальный размер пакета по своему желанию. Максимальный размер поля полезной нагрузки варьируется от 48 байт (ATM-ячейки) до 65 515 байт (IP-пакеты), хотя на более высоких уровнях размер поля полезной нагрузки часто бывает больше. Очевидная проблема возникает, когда большой пакет хочет пройти по сети, чей максимальный размер пакетов слишком мал. Одно из решений состоит в предотвращении возникновения самой проблемы. Другими словами, объединенная сеть должна использовать такой алгоритм маршрутизации, который не допускает пересылки пакетов по сетям, которые не могут их принять. Однако, если оригинальный пакет окажется слишком велик для сети адресата, то алгоритм маршрутизации окажется в данном случае бессилен. Следовательно, единственное решение проблемы заключается в разрешении шлюзам разбивать пакеты на *фрагменты* и посылать каждый фрагмент в виде отдельного межсетевого пакета.

Для восстановления оригинальных пакетов из фрагментов применяются две противоположные стратегии. Первая стратегия заключается в том, что пакет, входя через сеть небольшим допустимым размером пакетов, разбивается на входе шлюзом (*G1*) на фрагменты. Этот вариант показан на рис. 6.8, *а*. Каждый фрагмент адресуется одному и тому же выходному шлюзу (*G2*), восстанавливающему из этих фрагментов оригинальный пакет. Этот процесс повторяется при проходе через каждую сеть, максимальный размер пакетов в которой недостаточно велик.

Такой способ фрагментации прост, но, тем не менее, создает некоторые проблемы. Во-первых, выходной шлюз должен знать, когда он получил все части пакета, поэтому каждый фрагмент должен содержать либо поле счетчика, либо признак конца пакета. Во-вторых, все фрагменты должны выходить через один и тот же шлюз. Таким образом, налагается запрет на использование фрагментами различных путей к окончательному получателю, в результате может оказаться потерянной часть производительности. Наконец, повторяющиеся фрагментации и последующие

сборки пакета при прохождении каждой сети с малым размером пакетов приводят к дополнительным накладным расходам.

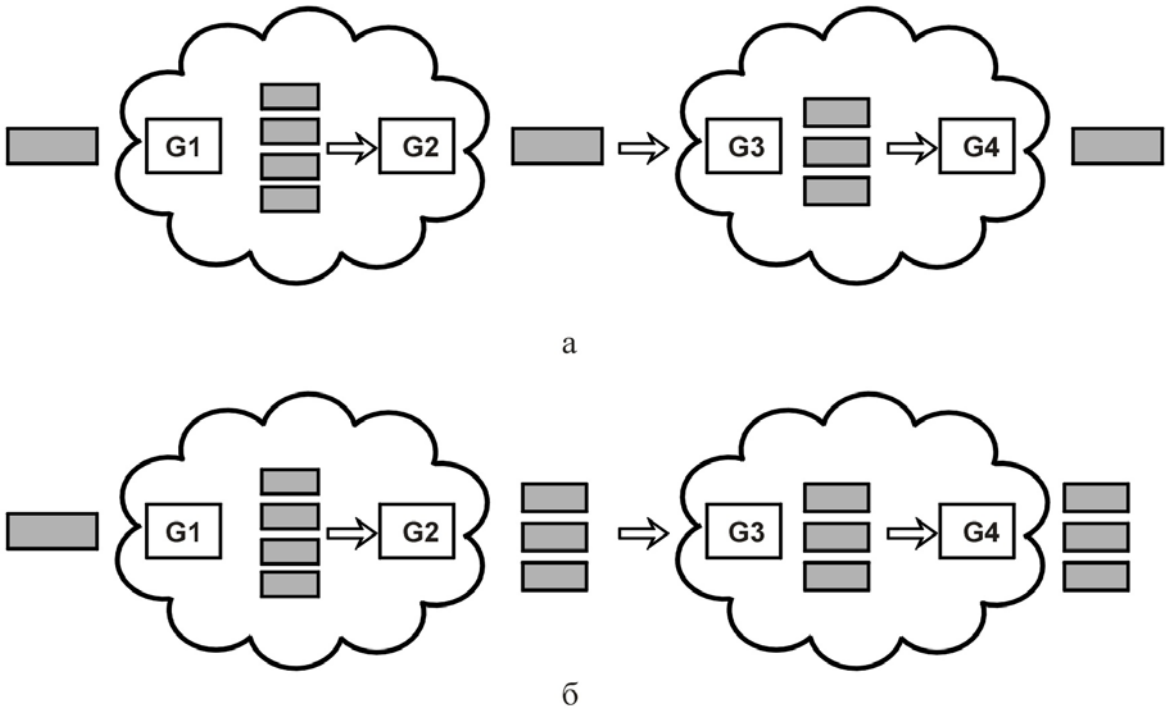


Рис. 6.8. Виды фрагментации пакетов

Другая стратегия фрагментации состоит в отказе от восстановления пакета из фрагментов на промежуточных маршрутизаторах. Как только пакет разбит на отдельные фрагменты, с каждым фрагментом обращаются как с отдельным пакетом. Задача восстановления оригинального пакета возложена на получающий хост (рис. 6.8, *б*).

Такой способ фрагментации также имеет свои проблемы. Например, он требует, чтобы каждый хост мог восстановить пакет из фрагментов. Кроме того, при фрагментации большого пакета возрастают суммарные накладные расходы, так как каждый фрагмент должен иметь заголовок.

В то время как в случае первого способа фрагментации лишние заголовки исчезали при выходе из сети с малым размером пакетов, в данном методе накладные расходы сохраняются на протяжении всего пути. Однако преимущество второй стратегии фрагментации состоит в возможности использовать для передачи фрагментов несколько различных маршрутов, что повышает производительность. Естественно, при использовании модели сцепленных виртуальных каналов это преимущество бесполезно.

Фрагменты пакета должны нумероваться таким образом, чтобы можно было восстановить исходный поток данных. Это гарантирует правильную сборку пакета получателем, независимо от порядка, в котором будут получены отдельные фрагменты.

Контрольные вопросы к главе 6

1. Что такое составная сеть?
2. Для чего необходима адресация узлов сети? Какова структура адреса в составной сети?
3. Что такое виртуальный канал?
4. В чем заключается дейтаграммная модель передачи данных, каковы ее преимущества и недостатки по сравнению с виртуальным каналом?
5. Опишите принцип организации туннеля при передаче данных.
6. Для чего необходима маршрутизация пакетов в составной сети?
7. С помощью каких аппаратных и программных средств реализуется задача маршрутизации?
8. Для чего необходима фрагментация пакетов?

ГЛАВА 7

АДРЕСАЦИЯ И МАРШРУТИЗАЦИЯ В IP-СЕТЯХ

7.1. Адресация в IP-сетях

При построении сетей одной из важнейших проблем является адресация узлов. Принятый в IP-сетях способ адресации узлов позволяет однозначно идентифицировать миллионы сетевых интерфейсов. В стеке TCP/IP используются три типа адресов:

– *локальные*, или *аппаратные*, адреса, используемые для адресации узлов в пределах подсети;

– *сетевые*, или *IP-адреса*, используемые для однозначной идентификации узлов в пределах всей составной сети;

– *доменные имена* – символьные идентификаторы узлов, к которым часто обращаются пользователи.

В общем случае сетевой интерфейс может иметь одновременно один или несколько локальных адресов и один или несколько сетевых адресов, а также одно или несколько доменных имен.

Аппаратный (локальный) адрес однозначно идентифицирует узел в пределах подсети. MAC-адрес обычно встраивается в аппаратуру компанией изготовителем, поэтому его стараются делать по возможности компактным. Если подсеть использует одну из базовых технологий LAN – Ethernet, FDDI, Token Ring, – то для доставки данных любому узлу такой подсети достаточно указать MAC-адрес.

IP-адреса представляют собой основной тип адресов, на основании которых сетевой уровень передает пакеты между сетями. Эти адреса имеют длину 4 байта. Они представляются в виде четырех чисел, представляющих значения каждого байта в десятичной форме, разделенных точками. IP-адрес состоит из двух

частей: номера сети (префиксная часть) и номера узла (хост часть).

Номер сети может быть выбран администратором произвольно либо назначен по рекомендации специального подразделения Интернета, если сеть должна работать как составная часть Интернета. В настоящее время с Интернетом соединены десятки тысяч сетей, и это число удваивается каждый год. Номера сетям во избежание конфликтов назначаются **сетевым информационным центром** (NIC, Network Information Center). Обычно поставщики услуг Интернета получают диапазоны адресов у подразделений InterNIC, а затем распределяют их между своими абонентами.

Номер узла в протоколе IP назначается независимо от локального адреса узла. Маршрутизатор по определению входит сразу в несколько сетей, поэтому каждый порт маршрутизатора имеет собственный IP-адрес. Конечный узел также может входить в несколько IP-сетей. В этом случае компьютер должен иметь несколько IP-адресов по числу сетевых связей. Таким образом, IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение.

Символьные имена в IP-сетях называются доменными и строятся по иерархическому признаку. Составляющие полного символьного имени в IP-сетях разделяются точкой и перечисляются в следующем порядке: сначала простое имя хоста, затем имя группы узлов (например, имя организации), затем имя более крупной группы (поддомена) и так до имени домена самого высокого уровня (например, домена, объединяющего организации по географическому принципу: RU – Россия, UK – Великобритания, SU – США). Между доменным именем и IP-адресом узла нет никакой функциональной зависимости, поэтому единственный способ установления соответствия – это таблица. В сетях TCP/IP используется специальная распределенная служба доменных имен (Domain Name System, *DNS*), которая устанавливает это соответствие на основании создаваемых администраторами сети таблиц соответствия. Поэтому доменные имена называют также DNS-именами.

Запись IP-адреса не предусматривает специального разграничительного знака между номером сети и номером узла. Каким образом маршрутизаторы, на которые поступают пакеты, выде-

ляют из адреса назначения номер сети, чтобы по нему определить дальнейший маршрут? Какая часть из 32 бит, отведенных под IP-адрес, относится к номеру сети, а какая – к номеру узла?

Рис. 7.1. Классификация IP адресов

Схема деления IP-адреса на номер сети и номер узла первоначально была основана на понятии класса, который определяется значениями нескольких первых битов адреса. Используемые для IP-адреса форматы классов показаны на рис. 7.1.

Количество допустимых адресов хостов в сети определяется по формуле:

$$N=2^{(32-P)}-2,$$

где P-длина префикса. Формат класса *A* позволяет задавать адреса до 126 сетей с 16777216 хостами в каждой, класса *B* – до 16 382 сетей с 65536 хостами, класса *C* – 2 млн сетей с 254 хостами в каждой. Формат класса *D* предназначен для многоадресной рассылки. Адреса, начинающиеся с 11110, зарезервированы для будущего применения.

Наименьший IP-адрес выглядит как 0.0.0.0, а наибольший – 255.255.255.255. Комбинации из всех нулей или единиц зарезервированы под служебные цели.

1. IP-адрес 0.0.0.0 используется хостом только при загрузке.

2. IP-адреса с нулевым номером сети обозначают текущую сеть. Эти адреса позволяют машинам обращаться к хостам собственной сети, не зная ее номера (но они должны знать ее класс и сколько нулей использовать).

3. Адрес, состоящий изо всех единиц, обеспечивает широковещание в пределах текущей (обычно локальной) сети.

4. Адреса, в которых указана сеть, но со всеми единицами в поле номера хоста, обеспечивают широковещание в пределах любой удаленной локальной сети, соединенной с Интернетом.

5. Наконец, все адреса вида 127. xx. yy. zz зарезервированы для тестирования сетевого программного обеспечения методом обратной передачи. Отправляемые по этому адресу пакеты не попадают на линию, а обрабатываются локально как входные пакеты.

К сожалению, протокол IP быстро становится жертвой собственной популярности: ему перестает хватать адресов. Это принимающее угрожающие размеры бедствие вызвало в Интернет-сообществе большое количество обсуждений и споров по поводу путей выхода из сложившейся ситуации. Еще в 1987 г. некоторые пророки предсказывали, что однажды Интернет может вырасти до 100 000 сетей. Большинство экспертов тогда не принимали всерьез эти предсказания, утверждая, что у Интернета в запасе имеются десятки лет, если ему вообще грозит что-либо подобное. 100 000-я сеть была подключена к Интернету в 1996 г.

Проблема заключается в том, что Интернету стало недостаточно IP- адресов. В принципе, адресов может существовать более 2 млрд, однако при использовании части поля адреса для разделения адресного пространства на классы (см. рис. 7.1) общее количество возможных адресов резко сокращается. В частности, главная проблема заключается в сетях класса *B*. Для большинства организаций сеть класса *A* с 16 млн. адресов слишком велика, а сеть класса *C* с 256 адресами слишком мала. Сеть класса *B* с 65 536 адресами подходит им лучше всего. Возможно, было бы лучше отвести на номер хоста в адресе класса *C* 10 бит, что позволило бы иметь до 1022 хостов в каждой сети. В таком случае, возможно, большинство организаций остановило бы свой выбор на сети класса *C*, которых можно было бы создать до полумиллиона (против 16 384 сетей класса *B*). Однако тогда еще быстрее возникла бы другая проблема: разрастание таблиц маршрутиза-

торов. С точки зрения маршрутизаторов, пространство IP-адресов представляет собой двухуровневую иерархию сетевых номеров и номеров хостов. Маршрутизаторы не должны знать обо всех хостах, но они должны знать обо всех сетях. Если бы применялись полмиллиона сетей класса С, каждому маршрутизатору в Интернете потребовалась бы таблица из полумиллиона записей.

Для ускорения работы маршрутизаторов весь мир разделен на четыре зоны, каждой из которых выделена часть адресного пространства сетей класса С. Разбиение было произведено следующим образом:

1. Адреса от 194.0.0.0 до 195.255.255.255 – для Европы;
2. Адреса от 198.0.0.0 до 199.255.255.255 – для Северной Америки;
3. Адреса от 200.0.0.0 до 201.255.255.255 – для Центральной и Южной Америки;
4. Адреса от 202.0.0.0 до 203.255.255.255 – для Азии и Тихоокеанского региона.

Подобным образом, каждому региону было предоставлено около 32 млн. адресов, плюс еще 320 млн. адресов класса *С* от 204.0.0.0 до 223.255.255.255 зарезервировано на будущее. Преимущество этого подхода состоит в том, что любой маршрутизатор за пределами Европы, получив пакет, адресованный 194. xx. yy. zz или 195. xxx. yyy. zzz, может просто переслать его стандартному европейскому шлюзу. В результате 32 млн. адресов уплотняются в одну строку таблицы маршрутизатора. То же самое происходит и с другими регионами. Однако по прибытии пакета в регион опять возникает проблема маршрутизации между сетями.

Одним из решений, реализуемым в настоящий момент, является алгоритм маршрутизации **CIDR** (Classless InterDomain Routing – бесклассовая междоменная маршрутизация). Идея метода состоит в использовании маски сети, которая позволяет максимально гибко устанавливать границу между номером сети и номером узла.

Маска – это число, которое используется в паре с IP-адресом. Двоичная запись маски содержит последовательность единиц в тех разрядах, которые должны в IP-адресе интерпретироваться как номер сети. Поскольку номер сети является цельной частью адреса, единицы в маске также должны представлять непрерыв-

ную последовательность. Граница между последовательностью единиц и последовательностью нулей в маске соответствует границе между номером сети и номером узла в IP-адресе. При таком подходе адресное пространство можно представить как совокупность множества сетей разного размера.

В десятичном представлении диапазоны адресов и маски сетей стандартных классов имеют следующие значения:

1. Класс A: 1.0.0.0 – 126.0.0.0, маска 255.0.0.0.
2. Класс B: 128.0.0.0 – 191.255.0.0, маска 255.255.0.0.
3. Класс C: 192.0.0.0 – 223.255.255.0, маска 255.255.255.0.
4. Класс D: 224.0.0.0–239.255.255.255, маска 255.255.255.255.
5. Класс E: 240.0.0.0 – 247.255.255.255, маска 255.255.255.255.

Образование байт маски поясняет таблица 7.1 возможных значений элементов маски.

Таблица 7.1.

Двоичное	Десятичное
11111111	255
11111110	254
11111100	252
11111000	248
11110000	240
11100000	224
11000000	192
10000000	128
00000000	0

Снабжая каждый IP-адрес маской, можно отказаться от понятий классов адресов и сделать систему адресации более гибкой. Например, если адрес 185.23.44.206 ассоциировать с маской 255.255.255.0, то номером сети будет 185.23.44.0, а не 185.23.0.0, как это определено системой классов. В масках количество еди-

ниц в последовательности, определяющей границу номера сети, не обязательно должно быть кратным 8, чтобы повторять деление адреса на байты.

Пусть, например, для IP-адреса 129.64.134.5 указана маска 255.255.128.0. В двоичном виде IP-адрес 129.64.134.5 выглядит так:

10000001. 01000000. 10000110. 00000101

Маска 255.255.128.0 в двоичном виде выглядит так:

11111111. 11111111.10000000. 00000000

Если игнорировать маску, то в соответствии с системой классов адрес 129.64.134.5 относится к классу *B*, а значит, номером сети являются первые два байта – 129.64.0.0, а номером узла – 0.0.134.5. Если же использовать для определения границы номера сети маску, то 17 последовательных двоичных единиц в маске 255.255.128.0, «наложенные» на IP-адрес, делят его на следующие две части:

номер сети 10000001. 01000000. 1 (129.64.128.0)

номер узла 0000110. 00000101 (0.0.6.5).

С появлением метода CIDR старые сети класса *A*, *B*, *C* для маршрутизации более не используются.

7.2. Подсети

Как было показано, у всех хостов сети должен быть один и тот же номер сети. Это свойство IP-адресации может вызвать проблемы при росте сети. Например, представьте компанию, начавшую подключение к Интернету с сети класса *C*. Со временем число компьютеров компании может превысить 254, и компании может понадобиться вторая сеть класса C. В качестве альтернативы компания может приобрести вторую сеть другого класса с отдельным IP-адресом для нее. В конце концов, компания получит несколько локальных сетей, каждая со своим маршрутизатором и со своим сетевым адресом класса *C*.

По мере увеличения количества отдельных локальных сетей их управление становится все сложнее. При установке каждой новой сети системный администратор должен связаться с сетевым информационным центром, чтобы получить новый сетевой

адрес. Затем этот адрес должен быть объявлен всему миру. Кроме того, перемещение машины из одной локальной сети в другую потребует изменения ее IP-адреса, что, в свою очередь, означает изменение файлов конфигурации машины, и также объявления всем нового IP-адреса машины. Если какая-либо новая машина получит освободившийся адрес, она будет получать электронную почту и другие данные, предназначенные другой машине, до тех пор, пока известие о смене адреса не распространится по всему миру.

Решение этих проблем состоит в разбиении сети на несколько частей для внутреннего использования, но так, чтобы для внешнего мира эта сеть продолжала действовать как единая сеть. В литературе, посвященной Интернету, эти части называются подсетями. Если бы наша растущая компания вместо класса *C* начала бы с сети класса *B*, она могла бы с появлением второй локальной сети разбить 16-разрядный номер хоста на 6-разрядный номер подсети и 10-разрядный номер хоста, как показано на рис. 7.2.

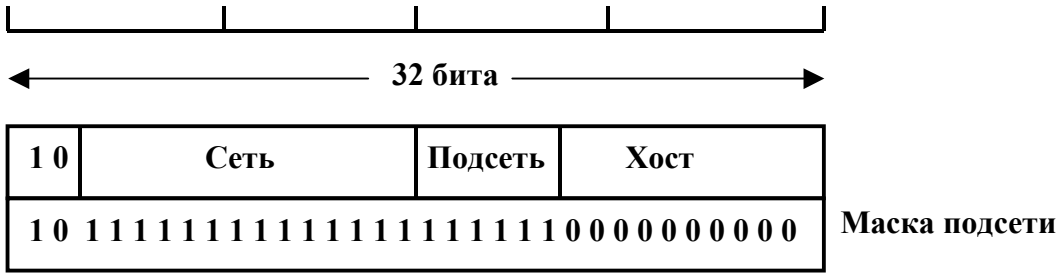


Рис. 7.2. Деление сети класса *B* на подсети

При подобном разбиении адреса компания могла бы иметь до 62 подсетей (0 и 1 зарезервированы) с количеством хостов в каждой до 1022. За пределами сети ее разбиение на подсети остается незаметным, поэтому появление новой подсети не требует контакта с Сетевым информационным центром или изменений внешних баз данных.

Чтобы понять, как функционируют подсети, следует рассмотреть процесс обработки IP-пакетов маршрутизатором. У каждого маршрутизатора есть таблица, содержащая IP-адреса сетей и IP-адреса хостов. Адреса сетей позволяют получать доступ к удаленным сетям, а адреса хостов – обращаться к локальным хостам. С каждой таблицей связан сетевой интерфейс, применяющийся

для получения доступа к пункту назначения, а также другая информация. Когда IP-пакет прибывает на маршрутизатор, адрес получателя, указанный в пакете, ищется в таблице маршрутизатора. Если пакет отправляется в удаленную сеть, он пересылается следующему маршрутизатору по интерфейсу, указанному в таблице. Если пакет предназначается локальному хосту (то есть в локальной сети маршрутизатора), он посылается напрямую адресату.

При разбиении сети на подсети таблицы маршрутизаторов изменяются. При этом к ним добавляются новые строки вида (эта сеть, подсеть, 0) и (эта сеть, эта подсеть, хост). Таким образом, маршрутизатор в каждой подсети знает, как получить доступ ко всем остальным подсетям и ко всем хостам своей подсети. Подробности о хостах других подсетей ему знать не нужно. Все, что нужно маршрутизатору, – это, определив класс сети, наложить маску подсети на IP-адрес пакета (см. рис. 7.2), чтобы, удалив номер хоста, получить номер подсети, который затем ищется в таблице. Разбиение сети на подсети уменьшает размер таблиц маршрутизаторов, создавая трехуровневую иерархию.

7.3. Порядок назначения IP-адресов

У каждой подсети в пределах составной сети должен быть собственный уникальный номер, следовательно, процедура распределения номеров должна быть централизованной. Аналогично, узлы должны быть однозначно пронумерованы в пределах каждой из подсетей, отсюда следует, что централизованный характер должна иметь и процедура распределения номеров узлов в пределах каждой подсети. Если сеть небольшая, то уникальность адресов может быть обеспечена вручную администратором.

В больших сетях, подобных Интернету, уникальность сетевых адресов гарантируется централизованной, иерархически организованной системой их распределения. Главным органом регистрации глобальных адресов в Интернете с 1998 года является *ICANN* (Internet Corporation for Assigned Names and Numbers) – неправительственная некоммерческая организация, управляемая советом директоров. Эта организация координирует работу ре-

гиональных отделов, деятельность которых охватывает большие географические площади: *ARIN* (Северная Америка), *LACNIC* (Южная Америка), *RIPE* (Европа), *APNIC* (Азия и Тихоокеанский регион), *AFRINIC* (Африка).

Региональные отделы выделяют блоки адресов сетей крупным поставщикам услуг, те, в свою очередь, присваивают их своим клиентам, среди которых могут быть и более мелкие поставщики услуг. Региональным сетевым информационным центром по России является компания RU-CENTER (сайт www.nic.ru).

Понятно, что в любой автономной сети могут быть использованы произвольные IP-адреса, лишь бы они были синтаксически правильными и уникальными в пределах этой сети. Совпадение адресов в не связанных между собой сетях не вызовет никаких отрицательных последствий. Однако во всех сетях, входящих в единую составную сеть (например, Интернет), должны использоваться глобально уникальные IP-адреса, однозначно определяющие сетевые интерфейсы в пределах всей составной сети.

IP-адреса и маски назначаются узлам при их конфигурировании вручную, или автоматически с использованием DHCP- или BootP-серверов. Ручное назначение адресов требует внимания – некорректное назначение адресов и масок приводит к невозможности связи по IP. При этом администратор должен помнить, какие адреса из имеющегося пула он уже использовал, а какие еще свободны. Однако с точки зрения надежности и безопасности (защиты от несанкционированного доступа) оно имеет свои преимущества.

Протокол *DHCP* (Dynamic Host Configuration Protocol) обеспечивает автоматическое динамическое назначение IP-адресов и масок подсетей для узлов-клиентов DHCP-сервера. Адреса вновь активированным узлам назначаются автоматически из области адресов, выделенных DHCP-серверу. По окончании работы узла его адрес возвращается в пул и в дальнейшем может назначаться для другого узла. Применение DHCP облегчает инсталляцию и диагностику для узлов, а также снимает проблему дефицита IP-адресов (реально отнюдь не все клиенты одновременно работают в сети).

Протокол *BootP* выполняет аналогичные функции, но использует статическое распределение ресурсов. При инициализации

узел посылает широковещательный запрос, на который BootP-сервер ответит пакетом с IP-адресом, маской, а также адресами шлюзов (gateways) и серверов службы имен (nameservers). Эти данные хранятся в списке, составленном по MAC-адресам клиентов BootP, хранящимся на сервере. Естественно, что по отключении узла его IP-адрес не может быть использован другими узлами.

7.4. Управляющие протоколы Интернета

7.4.1. Протокол ICMP

За работой Интернета следят маршрутизаторы. Когда случается что-либо неожиданное, о происшествии сообщается по протоколу ICMP (Internet Control Message Protocol – протокол управляющих сообщений Интернета), также используемому для тестирования Интернета. Протоколом ICMP определено около десятка типов сообщений. Каждое ICMP-сообщение вкладывается в IP-пакет.

Сообщение АДРЕСАТ НЕДОСТУПЕН используется, когда подсеть или маршрутизатор не могут обнаружить пункт назначения или когда пакет с битом DF (не фрагментировать) не может быть доставлен, так как путь преграждает сеть с маленьким размером пакетов.

Сообщение ВРЕМЯ ИСТЕКЛО посылается, когда пакет игнорируется, так как его счетчик уменьшился до нуля. Это событие является признаком того, что пакеты двигаются по замкнутым путям, что имеется большая перегрузка или установлено слишком низкое значение таймера.

Сообщение ПРОБЛЕМА С ПАРАМЕТРОМ указывает, что обнаружено неверное значение в поле заголовка, что является признаком наличия ошибки в программном обеспечении отправившего этот пакет хоста или промежуточного маршрутизатора.

Сообщение ПЕРЕАДРЕСОВАТЬ посылается хосту, отправившему пакет, когда маршрутизатор замечает, что пакет адресован неверно.

Сообщения ЗАПРОС ОТКЛИКА и ОТКЛИК посылаются, чтобы определить, достижим и жив ли конкретный адресат. По-

лучив сообщение ЗАПРОС ОТКЛИКА, хост должен отправить обратно сообщение ОТКЛИК.

Сообщения ЗАПРОС ВРЕМЕННОГО ШТАМПА и ОТКЛИК С ВРЕМЕННЫМ ШТАМПОМ имеют то же назначение, но при этом в ответе проставляется время получения сообщения и время отправления ответа. Это сообщение используется для измерения производительности сети.

7.4.2. Протоколы разрешения адресов

Одной из главных задач, которая ставилась при создании протокола IP, являлось обеспечение совместной согласованной работы в сети, состоящей из подсетей, в общем случае использующих разные сетевые технологии. Взаимодействие технологии TCP/IP с частными технологиями подсетей происходит многократно при перемещении пакета IP по составной сети. На каждом маршрутизаторе протокол IP определяет, в какую следующую подсеть и какому пограничному узлу в этой подсети надо направить пакет. Таким пограничным узлом является маршрутизатор, и протоколу IP известен его IP-адрес. Однако технологии подсетей могут не понимать IP-адресов, поэтому они не могут использоваться для отправки пакетов, так как аппаратура уровня передачи данных не понимает Интернет-адресов.

В настоящее время большинство хостов соединены с локальными сетями с помощью интерфейсных карт, понимающих только адреса данной локальной сети. Например, каждая когда-либо выпущенная сетевая карта Ethernet имеет 48-разрядный Ethernet-адрес. Производители сетевых карт Ethernet запрашивают у центра блок адресов, что гарантирует уникальность Ethernet-адресов. Сетевые карты отправляют и принимают кадры, основываясь на 48-разрядных Ethernet-адресах. О 32-разрядных IP-адресах им ничего не известно.

Таким образом, возникает вопрос: как устанавливается соответствие IP-адресов и адресов уровня передачи данных, таких как Ethernet-адреса? Чтобы понять, как это работает, рассмотрим показанный на рис. 7.3 пример.

На рисунке мы видим две сети Ethernet, одна с IP-адресом 192.31.65.0, а другая – с IP-адресом 192.31.63.0. Они соединены

кольцом FDDI с IP-адресом 192.31.60.0. У каждой машины сетей Ethernet есть уникальный Ethernet-адрес, обозначенный на рисунке от E1 до E6, а у каждой машины кольца FDDI есть FDDI-адрес, обозначенный от F1 до F3.

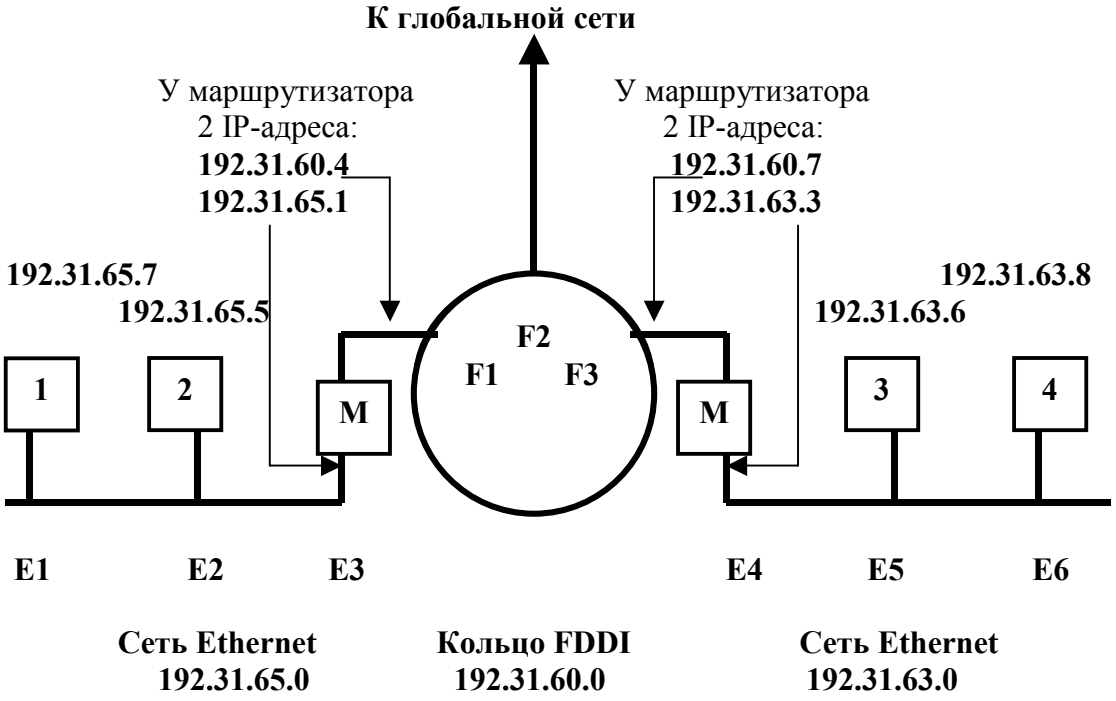


Рис.7.3. Соответствие IP адресов адресам локальных сетевых технологий

Прежде всего, рассмотрим, как пользователь с хоста 1 (IP-адрес 192.31.65.7) посылает пакет пользователю на хост 2 (IP-адрес 192.31.65.5). Программное обеспечение верхнего уровня хоста 1 создает пакет и передает его IP-программе для пересылки. Программное обеспечение протокола IP определяет, что адресат находится в его собственной сети, но ему нужно как-то определить Ethernet-адрес получателя. Одно из решений состоит в том, что в системе хранится файл конфигурации, в котором перечислены соответствия всех локальных IP-адресов Ethernet-адресам. Такое решение, конечно, возможно, но в организациях с тысячами машин поддержка этих файлов в обновленном состоянии потребует много времени и подвержена ошибкам.

Лучшее решение заключается в рассылке хостом 1 по сети Ethernet широковещательного пакета с вопросом «Кому принад-

лежит IP-адрес 192.31.65.5?». Этот пакет будет получен каждой машиной сети Ethernet 192.31.65.0, а хост 2 ответит на вопрос своим Ethernet-адресом E2. Таким образом, хост 1 узнает, что IP-адрес 192.31.65.5 принадлежит хосту с Ethernet-адресом E2. Протокол, который задает подобный вопрос и получает ответ на него, называется **ARP** (Address Resolution Protocol – протокол разрешения адресов). Он работает почти на каждой машине в Интернете.

Затем программное обеспечение протокола IP хоста 1 создает Ethernet-кадр, адресованный E2, помещает в его поле полезной нагрузки IP-пакет, адресованный 192.31.65.5, и посылает его по сети Ethernet. Сетевая карта Ethernet хоста 2 обнаруживает кадр, замечает, что он адресован ей, считывает его и вызывает прерывание. Ethernet-драйвер извлекает IP-пакет из поля полезной нагрузки и передает его IP-программе, которая, видя, что пакет адресован правильно, обрабатывает его.

Для повышения эффективности протокола ARP существуют различные методы оптимизации. Во-первых, машина, на которой работает протокол ARP, запоминает результат преобразования адреса, на случай, если ей придется снова связаться с той же машиной. В следующий раз она найдет нужный адрес в своем кэше, сэкономив, таким образом, на рассылке широковещательного пакета. В большинстве случаев хосту 2 понадобится отослать ответ на пакет, что также потребует от него обращения к ARP, чтобы определить адрес отправителя. Этого обращения можно избежать, если отправитель включит в ARP-пакет свои IP- и Ethernet-адреса. Когда широковещательный ARP-пакет прибудет на хост 2, пара (192.31.65.7, E1) будет сохранена хостом 2 в ARP-кэше для будущего использования. Более того, эту пару адресов могут сохранить все машины сети Ethernet. Кроме того, каждая машина может рассылать свою пару адресов во время загрузки. Обычно эта широковещательная рассылка производится в виде ARP-пакета, запрашивающего свой собственный IP-адрес. Ответа на этот запрос быть не должно, но все машины могут запомнить эту пару адресов. Если ответ все же придет, это будет означать, что двум машинам назначен один и тот же IP-адрес. При этом вторая машина должна проинформировать системного администратора и прекратить загрузку.

Посмотрим снова на рис. 7.3, только на этот раз хост 1 хочет послать пакет хосту 4 (192.31.63.8). Обращение к ARP не даст результата, так как хост 4 не увидит широковещательного пакета (маршрутизаторы не переправляют широковещательные пакеты Ethernet-уровня). Решение состоит в том, что хост 1 сразу видит, что адресат находится в удаленной сети, поэтому он посылает весь внешний трафик по Ethernet-адресу, обрабатывающему все пакеты для удаленных адресатов, то есть маршрутизатору E3. Хост 1 помещает IP-пакет в поле полезной нагрузки Ethernet-кадра, адресованного маршрутизатору E3. Получив Ethernet-кадр, маршрутизатор извлекает из поля полезной нагрузки IP-пакет и ищет его IP-адрес в своих таблицах. Он обнаруживает, что пакеты, адресованные сети 192.31.63.0, должны пересылаться маршрутизатору 192.31.60.7. Если ему еще не известен FDDI-адрес маршрутизатора 192.31.60.7, то он посылает по кольцу широковещательный ARP-пакет и узнает, что нужный ему адрес F3. Затем он помещает IP-пакет в поле полезной нагрузки FDDI-кадра, адресованного маршрутизатору F3, и отправляет его по кольцу. Когда кадр попадает на маршрутизатор F3, FDDI-драйвер извлекает из поля полезной нагрузки IP-пакет и передает его IP-программе, которая видит, что этот пакет следует переслать 192.31.63.8. Если этого IP-адреса еще нет в ARP-кэше, маршрутизатор посылает широковещательный ARP-запрос по сети Ethernet и узнает, что нужный ему адрес принадлежит хосту E6, поэтому он создает Ethernet-кадр, адресованный хосту E6, помещает IP-пакет в поле полезной нагрузки и передает его по сети Ethernet. Получив Ethernet-кадр, хост 4 извлекает из поля полезной нагрузки IP-пакет и передает его. IP-программе для обработки.

В некоторых случаях возникает обратная задача – нахождение IP-адреса по известному локальному адресу. Тогда в действие вступает *реверсивный протокол ARP* (Reverse Address Resolution Protocol, RARP). Этот протокол используется, например, при старте бездисковых станций, не знающих в начальный момент своего IP-адреса, но знающих MAC-адрес своего сетевого адаптера.

Недостаток протокола RARP заключается в том, что в нем для обращения к RARP-серверу используется адрес, состоящий из всех единиц (ограниченное широковещание). Однако эти широ-

ковещательные запросы не переправляются маршрутизаторами в другие сети, поэтому в каждой сети требуется свой RARP-сервер.

Для решения данной проблемы был разработан альтернативный загрузочный протокол **BOOTP**. В отличие от RARP он использует UDP- сообщения, пересылаемые маршрутизаторами в другие сети. Он также снабжает бездисковые рабочие станции дополнительной информацией, включающей IP-адрес файлового сервера, содержащего образ памяти, IP-адрес маршрутизатора по умолчанию, а также маску подсети.

7.4.3. Организация доменов и доменных имен

Для идентификации компьютеров аппаратное и программное обеспечение в сетях TCP/IP полагается на IP-адреса, поэтому для доступа к сетевому ресурсу в параметрах программы вполне достаточно указать IP-адрес, чтобы программа правильно поняла, к какому хосту ей нужно обратиться. Однако пользователи обычно предпочитают работать с символьными именами компьютеров, и операционные системы локальных сетей приучили их к этому удобному способу. Следовательно, в сетях TCP/IP должны существовать символьные имена хостов и механизм для установления соответствия между символьными именами и IP-адресами.

В операционных системах, которые первоначально разрабатывались для работы в локальных сетях, таких как Novell NetWare, Microsoft Windows или IBM OS/2, пользователи всегда работали с символьными именами компьютеров. Так как локальные сети состояли из небольшого числа компьютеров, то использовались так называемые плоские имена, состоящие из последовательности символов, не разделенных на части. Для установления соответствия между символьными именами и MAC- адресами в этих операционных системах применялся механизм широковещательных запросов, подобный механизму запросов протокола ARP. Так, широковещательный способ разрешения имен реализован в протоколе NetBIOS, на котором были построены многие локальные ОС. Так называемые NetBIOS-имена стали на долгие годы одним из основных типов плоских имен в локальных сетях.

Для стека TCP/IP, рассчитанного в общем случае на работу в больших территориально распределенных сетях, подобный под-

ход оказывается неэффективным по нескольким причинам. Плоские имена не дают возможности разработать единый алгоритм обеспечения уникальности имен в пределах большой сети. В небольших сетях уникальность имен компьютеров обеспечивает администратор сети, записывая несколько десятков имен в журнале или файле. При росте сети задачу решают уже несколько администраторов, согласовывая имена между собой неформальным способом. Однако если сеть расположена в разных городах или странах, то администраторам каждой части сети нужно придумать способ именования, который позволил бы им давать имена новым компьютерам независимо от других администраторов, обеспечивая в то же время уникальность имен во всей сети. Самым надежным способом решения этой задачи является отказ от плоских имен.

В сети ARPANET соответствие текстовых и двоичных адресов просто записывалось в файле *hosts. txt*, в котором перечислялись все хосты и их IP-адреса. Каждую ночь все хосты получали этот файл с сайта, на котором тот хранился. В сети, состоящей из нескольких сот больших машин, работающих под управлением системы с разделением времени, такой подход работал вполне неплохо. Однако когда к сети были подключены тысячи рабочих станций, всем стало ясно, что этот способ не сможет работать вечно. Во-первых, размер файла стал слишком большим. Однако, что еще важнее, если управление именами хостов не будет осуществляться централизованно, неизбежно возникновение конфликтов имен. В то же время представить себе централизованное управление именами всех хостов гигантской международной сети довольно сложно.

Управление большим и постоянно изменяющимся набором имен представляет собой нетривиальную проблему. В почтовой системе на письмах требуется указывать (явно или неявно) страну, область, город, улицу, номер дома, квартиру и фамилию получателя. Благодаря использованию такой иерархической схемы не возникает путаницы между Ивановым Иваном Ивановичем, живущим в Самаре и Ивановым Иваном Ивановичем, живущим в Москве.

Для разрешения проблем с адресацией в глобальной сети была разработана аналогичная служба имен доменов **DNS** (Domain

Name System). Суть системы DNS заключается в иерархической схеме имен, основанной на доменах, и распределенной базе данных, реализующей эту схему имен. В первую очередь эта система используется для преобразования имен хостов и пунктов назначения электронной почты в IP-адреса, но также может использоваться и в других целях. В настоящее время система DNS является одним из важнейших компонентов инфраструктуры Интернет.

Интернет концептуально разделен на 200 **доменов** верхнего уровня. Доменами называют в Интернете множество хостов, объединенное в логическую группу. Каждый домен верхнего уровня подразделяется на поддомены, которые, в свою очередь, также могут состоять из других доменов, и т.д. Все эти домены можно рассматривать в виде дерева. Каждый домен управляет доступом к доменам, расположенным под ним.

Домены верхнего уровня разделяются на две группы: родовые домены и домены государств. К родовым относятся домены: *com* (commercial – коммерческие организации), *edu* (educational – учебные заведения), *gov* (government – федеральное правительство США), *int* (international – определенные международные организации), *mil* (military – вооруженные силы, *net* (network – сетевые операторы связи) и *org* (некоммерческие организации). За каждым государством в соответствии с международным стандартом ISO 3166 закреплен один домен государства.

Решение о введении первых доменов верхнего уровня общего назначения COM, EDU, GOV, MIL, ORG, NET, INT было принято в 1983 году. Тогда же была разработана спецификация системы DNS и реализован первый сервер доменных имен. В 1985 году были зарегистрированы первые доменные имена (поддомены) в зоне COM.

В ноябре 2000 года было утверждено 4 новых родовых имени доменов верхнего уровня, а именно: *biz* (бизнес), *info* (информация), *name* (имена людей) и *pro* (специалисты, такие как доктора и адвокаты). Кроме того, по просьбе соответствующих отраслевых организаций были введены еще три специализированных имени доменов верхнего уровня: *aero* (аэрокосмическая промышленность), *coop* (кооперативы) и *museum* (музеи). К концу 2004 года в зоне COM было зарегистрировано около 33 млн доменных имен, а во всех доменах верхнего уровня около 63 млн имен.

В будущем появятся и другие домены верхнего уровня. Между прочим, по мере коммерциализации Интернета появляется все больше спорных вопросов. Взять хотя бы домен *pro*. Он предназначен для сертифицированных специалистов. Но кто является специалистом, а кто нет? Кем должны быть эти специалисты сертифицированы? Понятно, что доктора и адвокаты это профессионалы. А что делать со свободными художниками, учителями музыки, водопроводчиками, парикмахерами, мусорщиками? Имеют ли право квалифицированные представители всех этих и многих других профессий получать домены pro? Если да, то кто выдаст сертификат каждому из этих специалистов? В принципе, получить домен второго уровня типа *name-of-company. com* не сложно. Надо лишь проверить, не занято ли желаемое имя домена кем-то другим и не является ли оно чьей-нибудь торговой маркой. Для этого надо зайти на сайт регистрационного бюро верхнего уровня (в данном случае *com*). Если все в порядке, заказчик регистрируется и за небольшую ежегодную абонентскую плату получает домен второго уровня.

Имя каждого домена, подобно полному пути к файлу в файловой системе, состоит из пути от этого домена до вершины дерева. Компоненты пути разделяются точками. Имена доменов не чувствительны к изменению регистра символов. Так, например, edu и EDU означают одно и то же. Длина имен компонентов может достигать 63 символов, а длина полного пути не должна превосходить 255 символов. На практике, почти все организации в США помещаются под родовыми доменами, тогда как почти все организации за пределами Соединенных Штатов располагаются под доменами их государств.

Структура доменов отражает не физическое состояние сети, а логическое разделение между организациями и их подразделениями.

В общих чертах система DNS применяется следующим образом. Для преобразования имени в IP-адрес прикладная программа обращается к библиотечной процедуре, называющейся **распознавателем**, передавая ей имя в качестве параметра. Распознаватель посылает IP-пакет локальному DNS-серверу, который ищет имя в базе данных и возвращает соответствующий IP-адрес распознавателю, который, в свою очередь, передает его вызывавшей

его прикладной программе. Имея IP- адрес, программа может установить TCP-соединение с адресатом или послать ему UDP-пакеты.

Теоретически один сервер мог бы содержать всю базу данных DNS и отвечать на все запросы к ней. На практике этот сервер оказался бы настолько перегруженным, что был бы просто бесполезным. Более того, если бы его когда-либо выключили, то весь Интернет оказался бы неработоспособен. Чтобы избежать проблем, связанных с хранением всей информации в одном месте, пространство имен DNS разделено на непересекающиеся **зоны.** Каждая зона содержит часть общего дерева доменов, также в нее входят серверы имен, хранящие управляющую информацию об этой зоне. Обычно в каждой зоне находится один основной сервер зоны, получающий информацию из файла на своем диске, и несколько дополнительных серверов имен, которые получают информацию от основного сервера имен. Для большей надежности некоторые серверы, обслуживающие зону, могут находиться за пределами самой зоны. Где провести границы зон, целиком зависит от администратора зоны. Это решение основывается на том, сколько серверов имен требуется в той или иной зоне.

Распознаватель обращается с запросом разрешения имени домена к одному из локальных серверов имен. Если искомый домен относится к сфере ответственности данного сервера имен, тогда данный DNS-сервер сам отвечает распознавателю на его запрос. Однако если домен удаленный и информацию о запрашиваемом домене нельзя получить на месте, сервер имен посылает сообщение с запросом серверу домена верхнего уровня запрашиваемого домена.

Служба DNS использует текстовые файлы почти такого формата, как и файл *hosts*, и эти файлы администратор также подготавливает вручную. Однако служба DNS опирается на иерархию доменов, и каждый сервер службы DNS хранит только часть имен сети, а не все имена, как это происходит при использовании файлов *hosts*. При росте количества узлов в сети проблема масштабирования решается созданием новых доменов и поддоменов имен и добавлением в службу DNS новых серверов.

Для каждого домена имен создается свой DNS-сервер. Каждый DNS-сервер кроме таблицы отображений имен содержит

ссылки на DNS-серверы своих поддоменов. Эти ссылки связывают отдельные DNS-серверы в единую службу DNS. Ссылки представляют собой IP-адреса соответствующих серверов. Для обслуживания корневого домена выделено несколько дублирующих друг друга DNS-серверов, IP-адреса которых являются широко известными (их можно узнать, например, в InterNIC).

Процедура разрешения DNS-имени во многом аналогична процедуре поиска файловой системой адреса файла по его символьному имени. Действительно, в обоих случаях составное имя отражает иерархическую структуру организации соответствующих справочников – каталогов файлов или таблиц DNS. Здесь домен и доменный DNS-сервер являются аналогом каталога файловой системы. Для доменных имен, так же как и для символьных имен файлов, характерна независимость именования от физического местоположения. Процедура поиска адреса файла по символьному имени заключается в последовательном просмотре каталогов, начиная с корневого. Для определения IP-адреса по доменному имени также необходимо просмотреть все DNS-серверы, обслуживающие цепочку поддоменов, входящих в имя хоста, начиная с корневого домена. Существенным отличием является то, что файловая система расположена на одном компьютере, а служба DNS по своей природе является распределенной.

История российского сегмента доменных имен начинается с 1994 года, когда появился национальный домен RU. Управление национальным доменом было передано Российскому НИИ Общественных Сетей (РосНИИРОС). На конец 2004 года в домене RU 165822 компаниями и частными лицами было зарегистрировано 305339 доменов (http://www. nic. ru). Распределение доменов по территории России (федеральным округам) следующее: Центральный – 63.17%, Северо-Западный – 10.16%, Приволжский – 4.43%, Сибирский – 4.21%, Уральский – 3.56%, Южный – 3.06%, Дальневосточный – 1.31%. Более половины доменов (54.2%) зарегистрировано в Москве и Московской области, в Санкт-Петербурге – 8.7%, в Свердловской области – 2.3%, Новосибирской – 1.9%, Самарской – 1.3%. По итогам 2004года и начала 2005 года наблюдается тенденция снижения доли Центрального федерального округа и повышение доли остальных округов. В последние годы наблюдается увеличение чила регистраций рос-

сийских организаций в международных доменах COM, NET, ORG. К концу 2004 года число таких регистраций достигла 29% от общего количества регистраций в зоне RU.

7.4.4. Протокол внутреннего шлюза OSPF

Сеть Интернет состоит из большого количества автономных систем (подсетей). Каждая автономная система управляется своей организацией и может использовать внутри свой алгоритм маршрутизации. Алгоритм маршрутизации внутри автономной системы называется протоколом внутреннего шлюза. Алгоритм маршрутизации между автономными системами называется протоколом внешнего шлюза.

Алгоритм маршрутизации внутри автономной системы введен с 1990 года и называется *OSPF* (Open Shortest Path First – открытый алгоритм предпочтительного выбора кратчайшего маршрута). В ближайшем будущем он, скорее всего, станет главным протоколом внутреннего шлюза. При разработке протокола ставились ряд требований, которые необходимо было удовлетворить. Во-первых, этот алгоритм должен был быть напечатан в открытой литературе, откуда буква «О» (Open – открытый) в OSPF. Во-вторых, новый протокол должен был уметь учитывать широкий спектр различных параметров, включая физическое расстояние, задержку и т.д. В-третьих, этот алгоритм должен был быть динамическим, автоматически и быстро адаптирующимся к изменениям топологии. В-четвертых, он должен был поддерживать выбор маршрутов, основываясь на типе сервиса. Новый протокол должен был уметь по-разному выбирать маршрут для трафика реального времени и для других видов трафика. IP-пакет содержит поле «Тип службы», но ни один из имеющихся протоколов маршрутизации не использовал его. В-пятых, новый протокол должен был уметь распределять нагрузку на линии. Большинство предыдущих протоколов посылало все пакеты по одному лучшему маршруту. Следующий по оптимальности маршрут не использовался совсем. Во многих случаях распределение нагрузки по нескольким линиям дает лучшую производительность. В-шестых, необходима поддержка иерархических систем.

К 1988 г. Интернет вырос настолько, что ни один маршрутизатор не мог вместить сведения о его полной топологии.

Протокол OSPF поддерживает три следующих типа соединений и сетей:

1. Двухточечные линии, соединяющие два маршрутизатора.

2. Сети множественного доступа с широковещанием (то есть большинство локальных сетей).

3. Сети множественного доступа без широковещания (то есть большинство глобальных сетей с коммутацией пакетов).

Сеть *множественного доступа* – это сеть, у которой может быть несколько маршрутизаторов, способных общаться друг с другом напрямую. Этим свойством обладают все локальные и глобальные сети. В основе работы протокола OSPF лежит представление о множестве сетей, маршрутизаторов и линий в виде направленного графа, в котором каждой дуге поставлена в соответствие ее цена (расстояние, задержка и т.д.). Затем, основываясь на весе дуг, алгоритм вычисляет кратчайший путь. На рис. 7.4 показана автономная система, содержащая все три типа сетей и ее представление в виде ориентированного графа.

Многие автономные системы в Интернете сами также довольно велики, и управлять ими не просто. Протокол OSPF позволяет делить их на пронумерованные области, то есть на сети или множества смежных сетей. У каждой автономной системы есть *магистральная область*. Все области соединены с магистралью. Каждый маршрутизатор, соединенный с двумя и более областями, является частью магистрали. Работа маршрутизаторов заключается в расчете кратчайшего пути от себя до всех остальных маршрутизаторов этой области, включая маршрутизатор, соединенный с магистралью, который обязательно должен иметься в области, хотя бы один. Кратчайший путь для каждой области вычисляется отдельно.

Протокол OSPF различает четыре класса маршрутизаторов.

1. Внутренние маршрутизаторы, расположенные целиком внутри области.

2. Маршрутизаторы границы области, соединяющие две и более областей.

3. Магистральные маршрутизаторы, находящиеся на магистрали.

4. Маршрутизаторы границы автономной системы, общающиеся с маршрутизаторами других автономных систем.

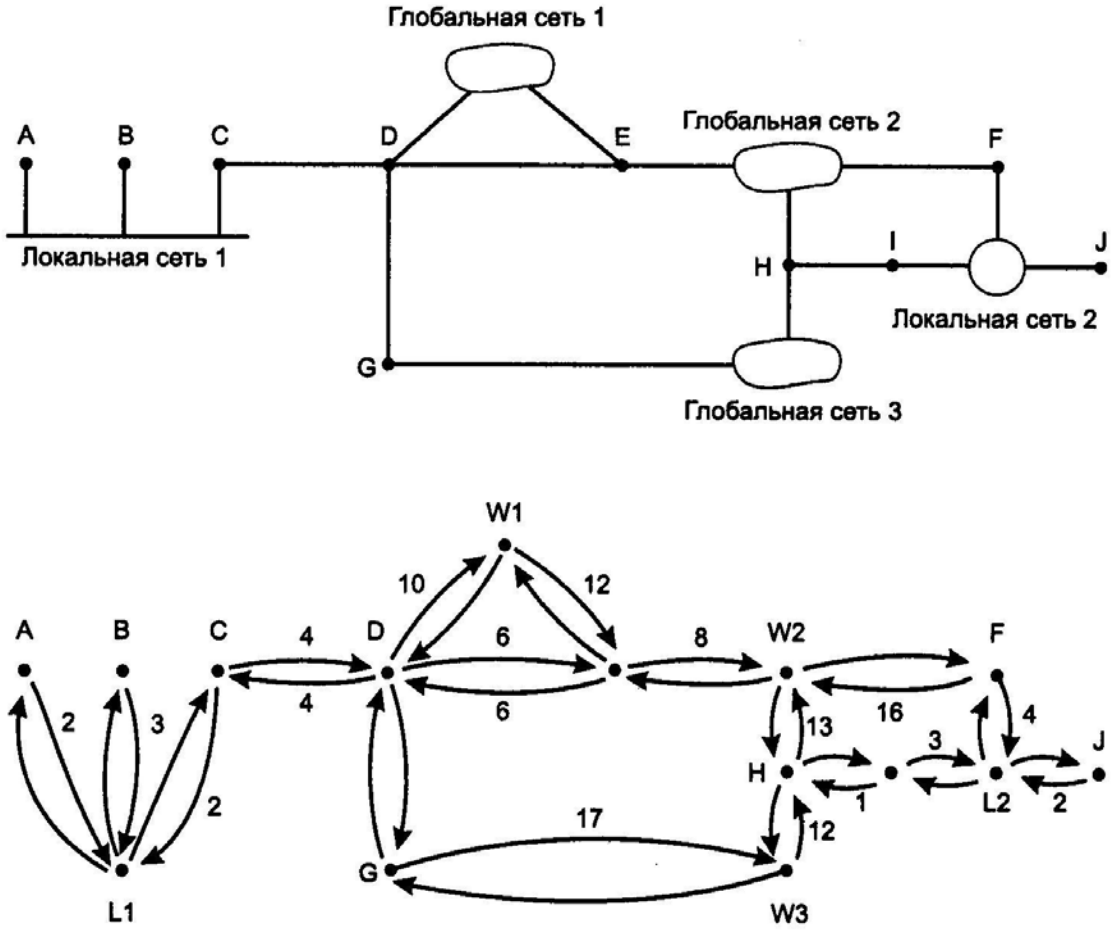


Рис. 7.4. Автономная система и её представление ориентированным графом

Эти классы могут перекрываться. Например, все пограничные маршрутизаторы автоматически являются магистральными.

В OSPF процесс построения таблицы маршрутизации разбивается на два крупных этапа. На первом этапе каждый маршрутизатор строит граф связей сети, в котором вершинами графа являются маршрутизаторы и IP-сети, а ребрами интерфейсы маршрутизаторов. Все маршрутизаторы для этого обмениваются со своими соседями той информацией о графе сети (топологии), которой они располагают к данному моменту времени. Подобные сообщения называются *router links advertisement – объявление о связях маршрутизатора*. Кроме того, при передаче топологической информации маршрутизаторы ее не модифицируют, как это

делают RIP-маршрутизаторы, а передают в неизменном виде. В результате распространения топологической информации все маршрутизаторы сети располагают идентичными сведениями о графе сети, которые хранятся в *топологической базе данных* каждого маршрутизатора.

Второй этап состоит в нахождении оптимальных маршрутов с помощью полученного графа. Каждый маршрутизатор считает себя центром сети и ищет оптимальный маршрут до каждой известной ему сети. В каждом найденном таким образом маршруте запоминается только один шаг – до следующего маршрутизатора, в соответствии с принципом одношаговой маршрутизации. Данные об этом шаге и попадают в таблицу маршрутизации. Задача нахождения оптимального пути на графе является достаточно сложной и трудоемкой.

После первоначального построения таблицы маршрутизации необходимо отслеживать изменения состояния сети и вносить коррективы в таблицу маршрутизации. Для контроля состояния связей и соседних маршрутизаторов OSPF-маршрутизаторы не используют обмен полной таблицей маршрутизации. Вместо этого они передают специальные короткие сообщения HELLO. Если состояние сети не меняется, то OSPF-маршрутизаторы корректировкой своих таблиц маршрутизации не занимаются и не посылают соседям объявления о связях. Если же состояние связи изменилось, то ближайшим соседям посылается новое объявление, касающееся только данной связи, что, конечно, экономит пропускную способность сети. Получив новое объявление об изменении состояния связи, маршрутизатор перестраивает граф сети, заново ищет оптимальные маршруты (не обязательно все, а только те, на которых отразилось данное изменение) и корректирует свою таблицу маршрутизации. Одновременно маршрутизатор ретранслирует объявление каждому из своих ближайших соседей (кроме того, от которого он получил это объявление). При появлении новой связи или нового соседа маршрутизатор узнает об этом из новых сообщений HELLO. В сообщениях HELLO указывается достаточно детальная информация о том маршрутизаторе, который послал это сообщение, а также о его ближайших соседях, чтобы данный маршрутизатор можно было однозначно идентифицировать. Сообщения HELLO отправляются через каж-

дые 10 с, чтобы повысить скорость адаптации маршрутизаторов к изменениям, происходящим в сети. Небольшой объем этих сообщений делает возможным такое частое тестирование состояния соседей и связей с ними. К недостаткам протокола OSPF следует отнести высокую вычислительную сложность, которая растет с увеличением размерности сети.

На рис. 7.5 показана часть Интернета с автономными системами и областями.

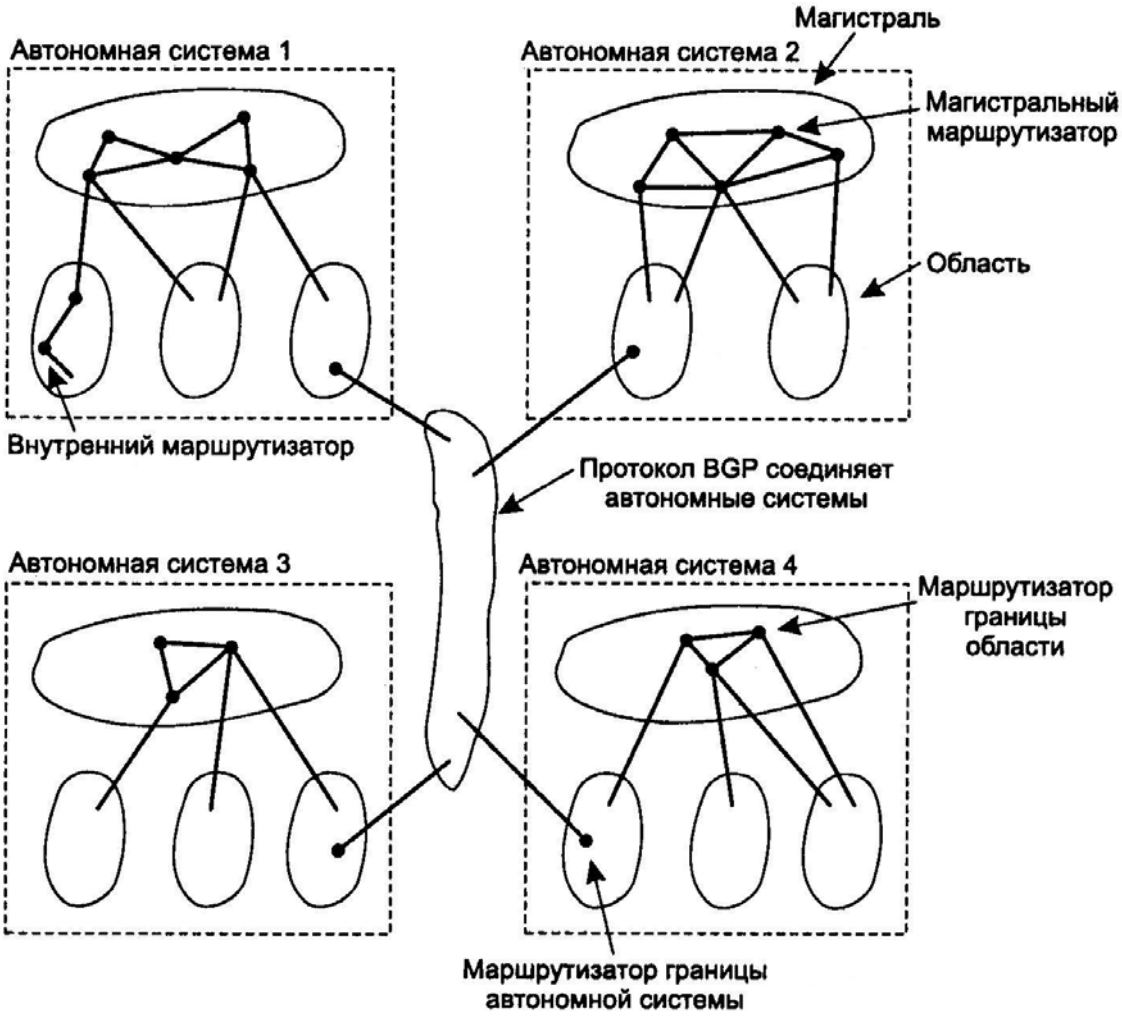


Рис. 7.5. Схема связи автономных систем

При выборе маршрута между различными автономными системами используется протокол **BGP** (Border Gateway Protocol–пограничный межсетевой протокол). Для выбора маршрута между различными автономными системами требуется другой протокол, так как цели протоколов внутреннего и внешнего шлюзов различны. Задача протокола внутреннего шлюза ограничивается

максимально эффективной передачей пакетов от отправителя к получателю. Политикой этот протокол не интересуется. Протокол внешнего шлюза вынужден помногу заниматься политикой. Например, корпоративной автономной системе может понадобиться возможность принимать и посылать пакеты на любой сайт Интернета. Однако прохождение через некую автономную систему пакета, отправитель и получатель которого находятся за пределами автономной системы, может быть нежелательно, даже если кратчайший путь между отправителем и получателем пролегает через эту автономную систему. С другой стороны, может оказаться желательным транзит трафика через другие автономные системы. Протоколы внешнего шлюза вообще и протокол BGP в частности разрабатывались для возможности учета различных стратегий при выборе маршрута между автономными системами.

Обычные стратегии выбора маршрутов включают в себя политические, экономические соображения, а также соображения безопасности. Политики настраиваются вручную на каждом BGP-маршрутизаторе. Они не являются частью протокола. С точки зрения BGP-маршрутизатора весь мир состоит из других BGP-маршрутизаторов и соединяющих их линий связи. Два BGP-маршрутизатора считаются соединенными, если у них есть общая сеть. Особая заинтересованность протокола BGP в транзитном трафике отразилась в разделении всех сетей на три категории. Первая категория представляет собой **тупиковые сети,** имеющие только одно соединение с BGP-графом. Они не могут использоваться для транзитного трафика. Вторую категорию представляют **многосвязные сети.** Они могут применяться для транзитного трафика, если только, конечно, согласятся на это. Наконец, имеются **транзитные сети,** такие как магистрали, для которых транзитный трафик является желательным, возможно с некоторыми ограничениями. Пары BGP-маршрутизаторов общаются друг с другом, устанавливая TCP-соединения. Таким образом, обеспечивается надежная связь и скрываются детали устройства сети, по которой проходит трафик.

7.5. Маршрутизация для мобильных хостов

Сегодня миллионы людей обладают переносными компьютерами и желают читать свою электронную почту, оставаясь в подключенном к сети состоянии, даже находясь в пути. К сожалению, адресная система протокола IP создает определенные трудности для работы в сети, когда клиент находится далеко от дома. Главным виновником проблемы является сама схема адресации. Каждый IP- адрес содержит три поля: класс, номер сети и номер хоста. Например, рассмотрим машину с IP-адресом 160.80.40.20. Маршрутизаторы, расположенные по всему миру, содержат таблицы, в которых сообщается, которую линию следует использовать, чтобы попасть в сеть 160.80. Когда приходит пакет с IP-адресом получателя вида 160.80. xxx. yyy, он отправляется по этой линии. Если вдруг машина с этим адресом отвозится в какое-либо удаленное место, адресованные ей пакеты будут продолжать направляться по ее домашнему адресу в ее локальную сеть (или ее маршрутизатору). Электронная почта перестанет доходить до владельца машины. Предоставление же машине нового адреса, соответствующего ее новому расположению, является нежелательным, так как об этом изменении придется информировать большое количество людей, программ и баз данных. Мобильные хосты привносят новое усложнение: чтобы направить пакет к мобильному хосту, его нужно сначала найти.

Когда потребность в мобильных хостах значительно возросла, проблемная группа проектирования Интернета (IETF, Internet Engineering Task Force) создала рабочую группу для поиска решения проблемы. Основными целями были признаны следующие.

1. Каждый мобильный хост должен иметь возможность использовать свой домашний IP-адрес где угодно.

2. Изменения программного обеспечения фиксированных хостов недопустимы.

3. Изменения программного обеспечения и таблиц маршрутизаторов недопустимы.

4. Большая часть пакетов, направляемых мобильным хостам, должны доставляться напрямую.

5. Не должно быть никаких дополнительных расходов, когда мобильный хост находится дома.

Модель мира, обычно используемая разработчиками сетей, представлена на рис. 7.6. Здесь мы видим глобальную сеть, состоящую из маршрутизаторов и хостов, с которой соединены локальные и региональные сети и беспроводные соты. Пользователи, которые никогда не перемещаются, называются стационарными. Они соединены с сетью медными проводами и оптическими кабелями. Мы будем различать два других типа пользователей: мигрирующих пользователей, являющихся в основном стационарными пользователями, перемещающимися время от времени с одного фиксированного места на другое, но пользующимися сетью, только когда физически соединены с нею. Блуждающие пользователи работают с переносными компьютерами и им требуется связь с сетью прямо на ходу. Для обозначения последних двух категорий пользователей мы будем использовать термин м о б и л ь н ы е п о л ь з о в а т е л и .

Предполагается, что у всех пользователей есть постоянное домашнее местоположение, которое никогда не меняется. У пользователей также есть постоянный домашний адрес, которым можно воспользоваться для определения домашнего местоположения. Целью маршрутизации в системах с мобильными пользователями является обеспечение возможности передачи пакетов мобильным пользователям, используя их домашние адреса. При этом пакеты должны эффективно достигать пользователей независимо от их расположения. Самое сложное здесь, конечно, – найти пользователя.

В модели, показанной на рис. 7.6, мир разделен (географически) на области, что обычно будет означать локальную сеть или беспроводную соту. Каждая область может содержать одного или более **внешних агентов,** следящих за всеми мобильными пользователями, посещающими область. Кроме того, в каждой области имеется **внутренний агент,** следящий за временно покинувшими свою область пользователями. Когда в области появляется новый пользователь, либо, подсоединившись к ней (то есть, соединив свой компьютер с сетью), либо просто переместившись в соту, его компьютер должен зарегистрироваться в данной области, связавшись с местным внешним агентом.

Процедура регистрации обычно выглядит следующим образом.

1. Периодически каждый внешний агент рассылает пакет, объявляя, таким образом, о своем существовании и местонахождении. Вновь прибывший мобильный хост может ждать подобного сообщения, но может и сам, не дождавшись его, передать пакет с запросом о наличии внешнего агента в данной области.

2. Мобильный хост регистрируется в данной области, сообщая внешнему агенту свой домашний адрес, текущий адрес уровня передачи данных, а также информацию, подтверждающую его подлинность.

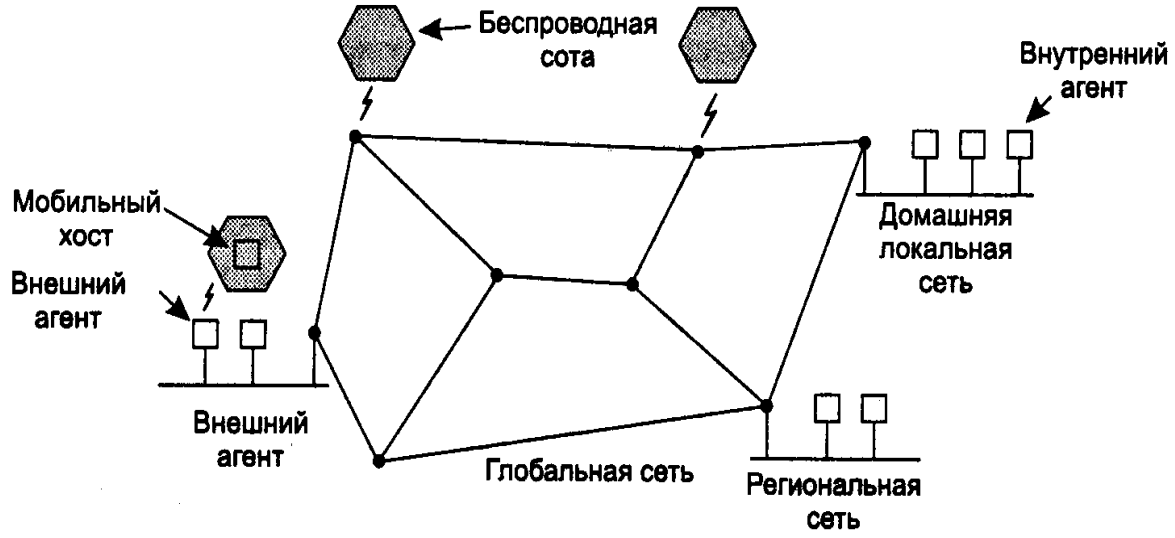


Рис. 7.6. Схема подключения мобильных хостов

3. Внешний агент связывается с внутренним агентом мобильного пользователя и сообщает ему: «Один из ваших хостов находится в нашей области». Это сообщение содержит адрес сети внешнего агента, а также информацию, подтверждающую подлинность мобильного хоста, чтобы убедить внутреннего агента, что мобильный хост действительно находится здесь.

4. Внутренний агент проверяет переданный ему идентификатор безопасности мобильного хоста, содержащий временной штамп, доказывающий, что идентификатор был создан всего несколько секунд назад. Если проверка подлинности хоста проходит успешно, внутренний агент разрешает внешнему агенту продолжать связь.

5. Получив подтверждение от внутреннего агента, внешний агент заносит сведения о мобильном хосте в свою таблицу и со-

общает ему, что он зарегистрирован. В идеальном случае, покидая область, пользователь также должен сообщить об этом внешнему агенту, однако на практике многие пользователи, закончив свои дела, просто выключают свои компьютеры.

Когда пакет посылается мобильному пользователю, он направляется в его домашнюю локальную сеть, как указывает домашний адрес пользователя. Пакеты, посланные в домашнюю локальную сеть мобильного пользователя, перехватываются внутренним агентом, который просматривает свою таблицу и узнает из нее адрес внешнего агента локальной сети, в которой в данный момент находится мобильный пользователь. Затем внутренний агент выполняет следующие действия. Во-первых, он помещает пакет, предназначающийся мобильному пользователю, в поле полезной нагрузки внешнего пакета, который посылается внешнему агенту. Такая техника называется туннелированием. Получив пакет, внешний агент извлекает из поля данных оригинальный пакет, который пересылает мобильному пользователю в виде кадра уровня передачи данных. Затем внутренний агент сообщает отправителю, что в дальнейшем следует посылать пакеты мобильному хосту не на домашний адрес, а вкладывать их в поле данных пакетов, явно адресованных внешнему агенту. Последующие пакеты теперь могут направляться напрямую пользователю через внешнего агента, полностью минуя домашний адрес мобильного пользователя.

Еще одна проблема состоит в том, что делать с невежливыми мобильными хостами, которые уходят, не попрощавшись. Для решения этой проблемы регистрация хоста считается действительной только в течение ограниченного интервала времени. Если она периодически не обновляется, то считается устаревшей, после чего внешний агент может удалить запись о прибывшем хосте из своих таблиц.

Еще одним вопросом является безопасность. Когда внутренний агент получает просьбу пересылать все пакеты, приходящие на имя «Катя», на некий IP-адрес, он не должен подчиняться, пока он не убедится, что источником этого запроса является именно «Катя», а не кто-либо, пытающийся выдать себя за Катю. Для этого применяются протоколы криптографической аутентификации.

Наконец, еще один вопрос связан с уровнями мобильности. Представьте себе самолет с установленной на борту сетью Ethernet, используемой навигационными и авиационными компьютерами. В этой сети есть стандартный маршрутизатор, общающийся с неподвижным Интернетом на земле по радиосвязи. В один прекрасный день кому-нибудь приходит в голову идея установить Ethernet-разъемы во всех подлокотниках кресел, так чтобы пассажиры с мобильными компьютерами могли подключаться к сети. Таким образом, мы получаем два уровня мобильности: компьютеры самолета, неподвижные относительно сети Ethernet, и компьютеры пассажиров, являющиеся мобильными относительно нее. Кроме того, бортовой маршрутизатор является мобильным относительно наземных маршрутизаторов. Мобильность относительно системы, которая сама является мобильной, может поддерживаться при помощи рекурсивного туннелирования.

Контрольные вопросы к главе 7

1. Какие типы адресов используются в стеке TCP/IP? Опишите каждый тип адресации.
2. Из каких частей состоит IP-адрес? Каковы основные форматы IP-адресов?
3. В чем заключается принцип использования масок для адресации узлов IP-сети?
4. Для чего используется разбиение сети на подсети?
5. Для чего служит протокол ICMP в сети интернет?
6. Какие протоколы сети Интернет служат для установления соответствия между IP-адресом и локальным адресом?
7. Каков принцип организации доменных имен?
8. Проанализируйте статистику состояния основных тенденций развития российского сегмента Интернет на основе данных компании RU-CENTER (www.nic.ru).
9. Для чего используется протокол OSPF?
10. В чем заключается особенность маршрутизации для мобильных хостов?

ГЛАВА 8

ФИЗИЧЕСКИЕ ОСНОВЫ ПЕРЕДАЧИ ДАННЫХ

Любая сетевая технология должна обеспечить надежную и быструю передачу дискретных данных по линиям связи. И хотя между технологиями имеются большие различия, они базируются на общих принципах передачи дискретных данных. Эти принципы находят свое воплощение в методах представления двоичных единиц и нулей с помощью импульсных или синусоидальных сигналов в линиях связи различной физической природы, методах обнаружения и коррекции ошибок, методах компрессии и методах коммутации.

8.1. Линии связи

8.1.1. Типы линий связи

Линия связи состоит в общем случае из физической среды, по которой передаются электрические информационные сигналы, аппаратуры передачи данных и промежуточной аппаратуры. *Физическая среда передачи данных* (физические носители информации) может представлять собой кабель, то есть набор проводов, изоляционных и защитных оболочек и соединительных разъемов, а также земную атмосферу или космическое пространство, через которые распространяются электромагнитные волны. Физические носители можно разделить на две группы: управляемые носители, такие как медный провод и оптоволоконный кабель, и неуправляемые, например радиоканалы наземной и спутниковой связи, а также передача по лазерному лучу без кабеля. Упрощенная схема классификации физических носителей информации представлена на рисунке 8.1.

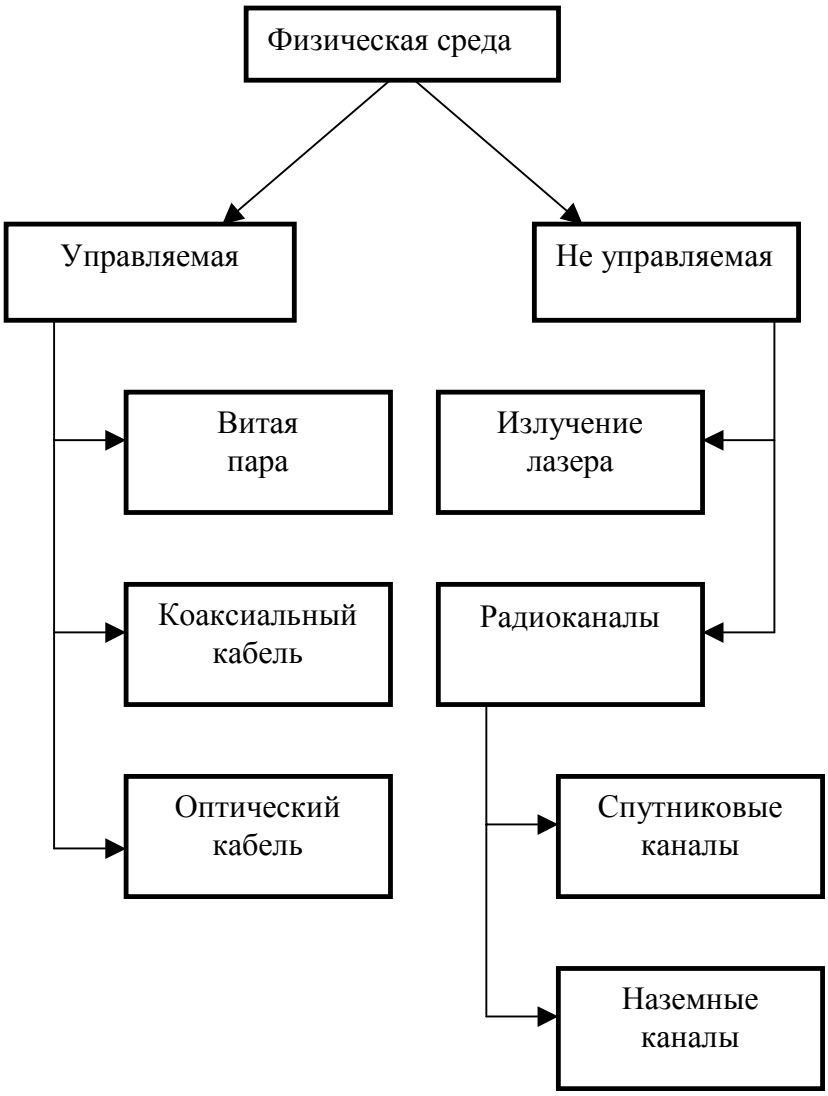


Рис. 8.1. Классификация физических носителей информации

Кабельные линии представляют собой достаточно сложную конструкцию. Кабель состоит из проводников, заключенных в несколько слоев изоляции: электрической, электромагнитной, механической. Кроме того, кабель может быть оснащен разъемами, позволяющими быстро выполнять присоединение к нему различного оборудования. В компьютерных сетях применяются три основных типа кабеля: кабели на основе скрученных пар медных проводов, коаксиальные кабели с медной жилой, а также волоконно-оптические кабели.

Скрученная пара проводов называется *витой парой* (twisted pair). Витая пара существует в экранированном варианте (Shielded Twisted Pair, *STP*), когда пара медных проводов оберты-вается в изоляционный экран, и неэкранированном (Unshielded

Twisted pair, *UTP*), когда изоляционная обертка отсутствует. Скручивание проводов снижает влияние внешних помех на полезные сигналы, передаваемые по кабелю.

Коаксиальный кабель (coaxial) состоит из внутренней медной жилы и оплетки, отделенной от жилы слоем изоляции. Он лучше экранирован, чем витая пара, поэтому может обеспечить передачу данных на более дальние расстояния с более высокими скоростями. Существует несколько типов коаксиального кабеля, отличающихся характеристиками и областями применения – для локальных сетей, для глобальных сетей, для кабельного телевидения и другие.

Волоконно-оптический кабель (optical fiber) состоит из тонких (5–60 микрон) волокон, по которым распространяются световые сигналы. Это наиболее качественный тип кабеля – он обеспечивает передачу данных с очень высокой скоростью (до 10 Гбит/с и выше) и лучше других типов передающей среды обеспечивает защиту данных от внешних помех.

Радиоканалы наземной и спутниковой связи образуются с помощью передатчика и приемника радиоволн. Существует большое количество различных типов радиоканалов, отличающихся как используемым частотным диапазоном, так и дальностью канала. Диапазоны коротких, средних и длинных волн (КВ, СВ и ДВ), называемые также диапазонами амплитудной модуляции (Amplitude Modulation, AM) по типу используемого в них метода модуляции сигнала, обеспечивают дальнюю связь, но при невысокой скорости передачи данных. Более скоростными являются каналы, работающие на диапазонах ультракоротких волн (УКВ), для которых характерна частотная модуляция (Frequency Modulation, FM), а также диапазонах сверхвысоких частот (СВЧ или microwaves). В диапазоне СВЧ (свыше 4 ГГц) сигналы не отражаются ионосферой Земли и для устойчивой связи требуется наличие прямой видимости между передатчиком и приемником. Поэтому такие частоты используют либо спутниковые каналы, либо радиорелейные каналы, где это условие выполняется.

Разновидностью беспроводной связи является также связь в инфракрасном диапазоне с помощью лазерного излучения. Существует мнение, что в будущем останется только два типа связи: оптоволоконная и беспроводная. Все стационарные (то есть не

переносные) компьютеры, телефоны, факсы и т.д. будут соединяться оптоволоконными кабелями, а все переносные – с помощью беспроводной связи. Однако беспроводная связь имеет свои преимущества и для некоторых стационарных устройств. Например, если прокладка кабеля к зданию сложна из-за условий местности, беспроводная связь может оказаться предпочтительнее.

В компьютерных сетях сегодня применяются практически все описанные типы физических сред передачи данных, но наиболее перспективными являются волоконно-оптические. На них сегодня строятся как магистрали крупных территориальных сетей, так и высокоскоростные линии связи локальных сетей. Популярной средой является также витая пара, которая характеризуется отличным соотношением качества к стоимости, а также простотой монтажа. С помощью витой пары обычно подключают конечных абонентов сетей на расстояниях до 100 метров от концентратора. Спутниковые каналы и радиосвязь используются чаще всего в тех случаях, когда кабельные связи применить нельзя – например, при прохождении канала через малонаселенную местность или же для связи с мобильным пользователем сети.

8.1.2. Аппаратура линий связи

Структурно связь между двумя узлами сети можно представить в виде схемы, представленной на рисунке 8.2.

Рис. 8.2. Схема связи двух узлов

Аппаратура передачи данных (АПД или DCE – Data Circuit terminating Equipment) непосредственно связывает компьютеры или локальные сети пользователя с линией связи и является, таким образом, пограничным оборудованием. Традиционно аппаратуру передачи данных включают в состав линии связи. Примерами DCE являются модемы, терминальные адаптеры сетей ISDN, устройства подключения к цифровым каналам. Обычно

DCE работает на физическом уровне, отвечая за передачу и прием сигнала нужной формы и мощности в физическую среду.

Аппаратура пользователя линии связи, вырабатывающая данные для передачи по линии связи и подключаемая непосредственно к аппаратуре передачи данных, обобщенно носит название *оконечное оборудование данных* (ООД или DTE – Data Terminal Equipment). Примером DTE могут служить компьютеры или маршрутизаторы локальных сетей. Эту аппаратуру не включают в состав линии связи. Разделение оборудования на классы DCE и DTE в локальных сетях является достаточно условным. Например, адаптер локальной сети можно считать как принадлежностью компьютера, то есть DTE, так и составной частью канала связи, то есть DCE.

Промежуточная аппаратура обычно используется на линиях связи большой протяженности. Промежуточная аппаратура решает две основные задачи:

– улучшение качества сигнала;

– создание постоянного составного канала связи между двумя абонентами сети.

В локальных сетях промежуточная аппаратура может совсем не использоваться, если протяженность физической среды (кабелей или радиоэфира) позволяет одному сетевому адаптеру принимать сигналы непосредственно от другого сетевого адаптера, без промежуточного усиления. В противном случае применяются устройства типа повторителей и концентраторов.

В глобальных сетях необходимо обеспечить качественную передачу сигналов на расстояния в сотни и тысячи километров. Поэтому без усилителей сигналов, установленных через определенные расстояния, построить территориальную линию связи невозможно. В глобальной сети необходима также и промежуточная аппаратура другого рода – мультиплексоры, демультиплексоры и коммутаторы. Эта аппаратура создает между двумя абонентами сети составной канал из некоммутируемых отрезков физической среды.

Промежуточная аппаратура канала связи прозрачна для пользователя, он ее не замечает и не учитывает в своей работе. Для него важно только качество полученного канала, влияющее на скорость передачи дискретных данных. В действительности же

промежуточная аппаратура образует сложную сеть, которую называют первичной сетью, так как сама по себе она никаких высокоуровневых служб (например, файловой или передачи голоса) не поддерживает, а только служит основой для построения компьютерных, телефонных или иных сетей.

В зависимости от типа промежуточной аппаратуры все линии связи делятся на аналоговые и цифровые. В *аналоговых линиях* промежуточная аппаратура предназначена для усиления аналоговых сигналов, то есть сигналов, которые имеют непрерывный диапазон значений. Такие линии связи традиционно применялись в телефонных сетях для связи АТС между собой.

В *цифровых линиях* связи передаваемые сигналы имеют конечное число состояний. Как правило, элементарный сигнал, то есть сигнал, передаваемый за один такт работы передающей аппаратуры, имеет 2 или 3 состояния, которые передаются в линиях связи импульсами прямоугольной формы. С помощью таких сигналов передаются как компьютерные данные, так и оцифрованные речь и изображение. В цифровых каналах связи используется промежуточная аппаратура, которая улучшает форму импульсов и обеспечивает их ресинхронизацию, то есть восстанавливает период их следования.

Аппаратура передачи дискретных компьютерных данных по аналоговым и цифровым линиям связи существенно отличается, так как в первом случае линия связи предназначена для передачи сигналов произвольной формы и не предъявляет никаких требований к способу представления единиц и нулей аппаратурой передачи данных, а во втором – все параметры передаваемых линией импульсов стандартизованы. Другими словами, на цифровых линиях связи протокол физического уровня определен, а на аналоговых линиях – нет.

8.1.3. Характеристики линий связи

К основным характеристикам линий связи относятся: амплитудно-частотная характеристика; полоса пропускания; затухание; помехоустойчивость; перекрестные наводки на ближнем конце линии; пропускная способность; достоверность передачи данных.

Чтобы лучше понять дальнейшее изложение, необходимо вспомнить некоторые понятия из физики. При движении электронов возникают электромагнитные волны, которые могут перемещаться в пространстве (даже в вакууме). Эти волны были предсказаны физиком Джеймсом Клерком Максвеллом в 1865 г. Впервые их произвел и наблюдал немецкий физик Генрих Герц в 1887 г. Число электромагнитных колебаний в секунду называется *частотой*, f и измеряется в герцах (в честь Генриха Герца). Расстояние между двумя последовательными максимумами (или минимумами) называется *длиной волны*, обозначаемой греческой буквой λ (лямбда). Если к электрической цепи присоединить антенну соответствующего размера, то электромагнитные волны могут успешно передаваться и приниматься приемником на некотором расстоянии. На этом принципе основаны почти все беспроводные системы связи.

В вакууме все электромагнитные волны распространяются с одной и той же скоростью, независимо от их частоты. Эта скорость называется *скоростью света*, c. Ее величина приблизительно равна $3 \cdot 10^8$ м/с, или около одного фута (30 см) за наносекунду. В меди или стекле скорость света составляет примерно 2/3 от этой величины, кроме того, слегка зависит от частоты. Скорость света современная наука считает пределом скорости. Быстрее скорости света не может двигаться никакой объект или сигнал. Величины f, λ и c (в вакууме) связаны фундаментальным соотношением: $f\lambda = c$. Существует мнемоническое правило $f\lambda \approx 300$, если λ измеряется в метрах, а f в мегагерцах.

На рис. 8.3 изображен электромагнитный спектр и его применение в связи. Радио, микроволновый, инфракрасный диапазоны, а также видимый свет могут быть использованы для передачи информации с помощью амплитудной, частотной или фазовой модуляции волн. Ультрафиолетовое, рентгеновское и гамма-излучение были бы даже лучше благодаря их высоким частотам, однако их сложно генерировать и модулировать, они плохо проходят сквозь здания и, кроме того, они опасны для всего живого. Диапазоны, перечисленные в нижней части рис. 8.3, представляют собой официальные названия, основанные на длинах волн, так, например, длинноволновый диапазон (LF, Low Frequency) охватывает длины волн от 1 км до 10 км (что приблизительно со-

ответствует диапазону частот от 30 кГц до 300 кГц). Сокращения LF, MF и HF обозначают Low Frequency (низкая частота), Medium Frequency (средняя частота) и High Frequency (высокая частота) соответственно.

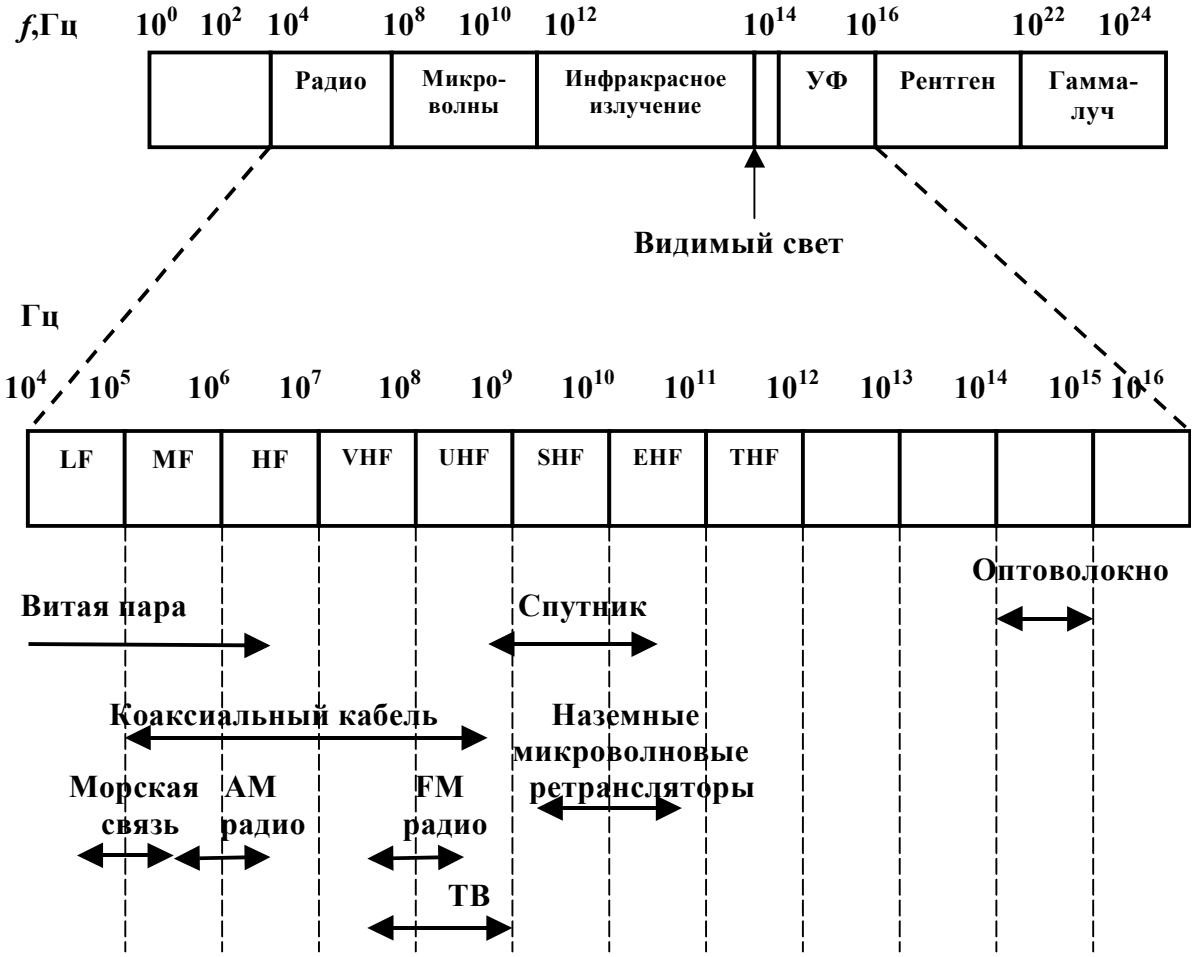


Рис. 8.3. Электромагнитный спектр частот и его использование в передаче информации

Очевидно, при назначении диапазонам названий никто не предполагал, что будут использоваться частоты выше 10 МГц, поэтому более высокие диапазоны получили названия *VHF* (very high frequency – очень высокая частота), *UHF* (ultrahigh frequency– ультравысокая частота, УВЧ), *SHF* (superhigh frequency – сверхвысокая частота, СВЧ), *EHF* (Extremely High Frequency – чрезвычайно высокая частота) и *THF* (Tremendously High Frequency – ужасно высокая частота). Выше последнего диапазона имена пока не придуманы.

В первую очередь разработчика вычислительной сети интересуют пропускная способность и достоверность передачи данных, поскольку эти характеристики прямо влияют на производительность и надежность создаваемой сети.

Пропускная способность и достоверность – это характеристики как линии связи, так и способа передачи данных. Поэтому если способ передачи (протокол) уже определен, то известны и эти характеристики. Однако нельзя говорить о пропускной способности линии связи, до того как для нее определен протокол физического уровня. Именно в таких случаях, когда только предстоит определить, какой из множества существующих протоколов можно использовать на данной линии, очень важными являются остальные характеристики линии, такие, как полоса пропускания, перекрестные наводки, помехоустойчивость и другие.

При передаче информации по физическим каналам связи происходит искажение передаваемого сигнала. Если это аналоговый сигнал, передающий речь, то на выходе изменяется тембр голоса. При передаче импульсных сигналов, характерных для компьютерных сетей, фронты импульсов теряют свою прямоугольную форму (рис. 8.4). Вследствие этого на приемном конце линии сигналы могут плохо распознаваться. Линия связи искажает передаваемые сигналы из-за того, что ее физические параметры отличаются от идеальных. Даже волоконно-оптический кабель имеет отклонения, мешающие идеальному распространению света. Если линия связи включает промежуточную аппаратуру, то она также может вносить дополнительные искажения.

Кроме искажений сигналов, вносимых внутренними физическими параметрами линии связи, существуют и внешние помехи, которые вносят свой вклад в искажение формы сигналов на выходе линии. Эти помехи создают различные электрические двигатели, электронные устройства, атмосферные явления и т.д. Несмотря на защитные меры, предпринимаемые разработчиками кабелей и усилительно-коммутирующей аппаратуры, полностью компенсировать влияние внешних помех не удается. Степень искажения синусоидальных сигналов линиями связи оценивается с помощью таких характеристик, как амплитудно-частотная характеристика, полоса пропускания и затухание на определенной частоте.

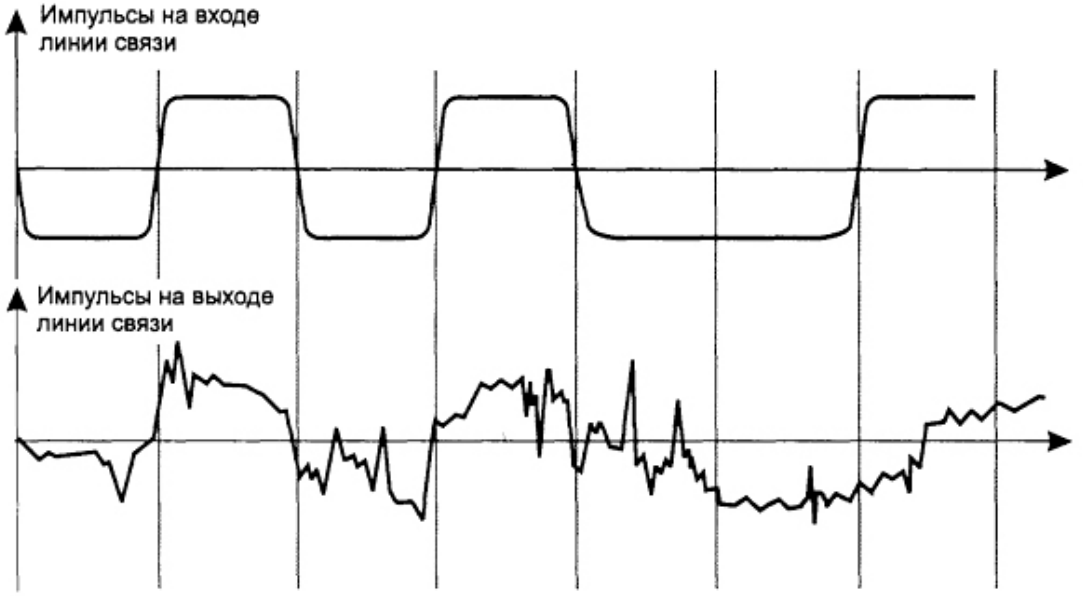


Рис. 8.4. Искажение сигнала в линиях связи

Амплитудно-частотная характеристика показывает, как затухает амплитуда синусоиды на выходе линии связи по сравнению с амплитудой на ее входе для всех возможных частот передаваемого сигнала.

Полоса пропускания – это непрерывный диапазон частот, для которого отношение амплитуды выходного сигнала к амплитуде входного превышает некоторый заранее заданный предел, обычно 0,5. То есть полоса пропускания определяет диапазон частот синусоидального сигнала, при которых этот сигнал передается по линии связи без значительных искажений.

Затухание определяется как относительное уменьшение амплитуды или мощности сигнала при передаче по линии сигнала определенной частоты.

Таким образом, амплитудно-частотная характеристика, полоса пропускания и затухание являются универсальными характеристиками, и их знание позволяет сделать вывод о том, как через линию связи будут передаваться сигналы любой формы.

Пропускная способность линии характеризует максимально возможную скорость передачи данных по линии связи. Пропускная способность измеряется в битах в секунду – бит/с, а также в производных единицах, таких как, килобит в секунду (Кбит/с), мегабит в секунду (Мбит/с), гигабит в секунду (Гбит/с) и т.д. Пропускная способность линий связи и коммуникационного се-

тевого оборудования традиционно измеряется в битах в секунду, а не в байтах в секунду. Это связано с тем, что данные в сетях передаются последовательно, то есть побитно, а не параллельно, байтами, как это происходит между устройствами внутри компьютера. Такие единицы измерения, как килобит, мегабит или гигабит, в сетевых технологиях строго соответствуют степеням 10 (то есть килобит – это 1000 бит, а мегабит – это 1 000 000 бит), как это принято во всех отраслях науки и техники, а не близким к этим числам степеням 2, как это принято в программировании, где приставка «кило» равна 2^{10} =1024

Помехоустойчивость линии определяет ее способность уменьшать уровень помех, создаваемых во внешней среде, на внутренних проводниках. Помехоустойчивость линии зависит от типа используемой физической среды, а также от экранирующих и подавляющих помехи средств самой линии. Наименее помехоустойчивыми являются радиолинии, хорошей устойчивостью обладают кабельные линии и отличной – волоконно-оптические линии, малочувствительные ко внешнему электромагнитному излучению. Обычно для уменьшения помех, появляющихся из-за внешних электромагнитных полей, проводники экранируют и/или скручивают.

Достоверность передачи данных характеризует вероятность искажения для каждого передаваемого бита данных. Иногда этот же показатель называют *интенсивностью битовых ошибок* (Bit Error Rate, BER). Величина BER для каналов связи без дополнительных средств защиты от ошибок составляет, как правило, 10^{-4} – 10^{-6}, в оптоволоконных линиях связи – 10^{-9}. Значение достоверности передачи данных, например, в 10^{-4} говорит о том, что в среднем из 10 000 бит искажается значение одного бита.

8.1.4. Кабели на основе витой пары

Медный неэкранированный кабель *UTP* (Unshielded Twisted Pair) в зависимости от электрических и механических характеристик разделяется на 5 категорий. Кабели категорий 1 и 2 в настоящее время не используются, как устаревшие. Кабель категории 3 предназначен как для передачи данных, так и для передачи голоса. Кабели *категории 4* представляют собой несколько

улучшенный вариант кабелей категории 3, но на практике используются редко. Кабели *категории 5* были специально разработаны для поддержки высокоскоростных протоколов. Большинство новых высокоскоростных стандартов ориентируются на использование витой пары 5 категории. На этом кабеле работают протоколы со скоростью передачи данных 100 Мбит/с – FDDI, Fast Ethernet, 100VG-AnyLAN, а также более скоростные протоколы – ATM на скорости 155 Мбит/с, и Gigabit Ethernet на скорости 1000 Мбит/с. Кабель категории 5 пришел на замену кабелю категории 3, и сегодня все новые кабельные системы крупных зданий строятся именно на этом типе кабеля (в сочетании с волоконно-оптическим).

Все кабели UTP независимо от их категории выпускаются в 4-парном исполнении. Каждая из четырех пар кабеля имеет определенный цвет и шаг скрутки. Обычно две пары предназначены для передачи данных, а две – для передачи голоса. Для соединения кабелей с оборудованием используются вилки и розетки RJ-45, представляющие 8-контактные разъемы, похожие на обычные телефонные разъемы RJ-11.

Особое место занимают кабели *категорий 6 и 7*, которые промышленность начала выпускать сравнительно недавно. Кабели категории 7 обязательно экранируются, причем как каждая пара, так и весь кабель в целом. Кабель категории 6 может быть как экранированным, так и неэкранированным. Основное назначение этих кабелей – поддержка высокоскоростных протоколов на отрезках кабеля большей длины, чем кабель UTP категории 5. Некоторые специалисты сомневаются в необходимости применения кабелей категории 7, так как стоимость кабельной системы при их использовании получается соизмеримой по стоимости сети с использованием волоконно-оптических кабелей, а характеристики кабелей на основе оптических волокон выше.

Экранированная витая пара *STP* (Shielded Twisted Pair) имеет множество разновидностей. Она хорошо защищает передаваемые сигналы от внешних помех, а также меньше излучает электромагнитных колебаний вовне, что защищает, в свою очередь, пользователей сетей от вредного для здоровья излучения. Наличие заземляемого экрана повышает стоимость кабеля и усложняет его прокладку, так как требует выполнения качественного заземления.

Экранированный кабель применяется только для передачи данных, а голос по нему не передают. Основным стандартом, определяющим параметры экранированной витой пары, является фирменный стандарт IBM. В этом стандарте кабели делятся не на категории, а на типы: Type 1, Type 2,..., Type 9. Основным типом экранированного кабеля является кабель Type 1 стандарта IBM. Он состоит из 2-х пар скрученных проводов, экранированных проводящей оплеткой, которая заземляется. Электрические параметры кабеля Type 1 примерно соответствуют параметрам кабеля UTP категории 5. Экранированные витые пары используются также в кабеле IBM Type 2, который представляет кабель Type 1 с добавленными 2 парами неэкранированного провода для передачи голоса. Для присоединения экранированных кабелей к оборудованию используются разъемы конструкции IBM.

8.1.5. Коаксиальные кабели

Существует большое количество типов коаксиальных кабелей, используемых в сетях различного типа – телефонных, телевизионных и компьютерных. Ниже приводятся основные типы и характеристики этих кабелей.

RG-8 и RG-11 – «толстый» коаксиальный кабель, разработанный для сетей Ethernet 10Base-5. Этот кабель имеет достаточно толстый внутренний проводник диаметром 2,17 мм, который обеспечивает хорошие механические и электрические характеристики, но его сложно монтировать – он плохо гнется. RG-58/U, RG-58 A/U и RG-58 C/U – разновидности «тонкого» коаксиального кабеля для сетей Ethernet 10Base-2. Все эти разновидности кабеля имеют волновое сопротивление 50 Ом, но обладают худшими механическими и электрическими характеристиками по сравнению с «толстым» коаксиальным кабелем. Для соединения кабелей с оборудованием используется разъем типа BNC. RG-59 – телевизионный кабель с волновым сопротивлением 75 Ом. Широко применяется в кабельном телевидении.

8.1.6. Волоконно-оптические кабели

Волоконно-оптические кабели состоят из центрального проводника света (сердцевины) – стеклянного волокна, окруженно-

го другим слоем стекла – оболочкой, обладающей меньшим показателем преломления, чем сердцевина. Распространяясь по сердцевине, лучи света не выходят за ее пределы, отражаясь от покрывающего слоя оболочки. В зависимости от распределения показателя преломления и от величины диаметра сердечника различают:

– многомодовое волокно со ступенчатым изменением показателя преломления (рис. 8.5, *а*);

– многомодовое волокно с плавным изменением показателя преломления (рис. 8.5, *б*);

– одномодовое волокно (рис. 8.5, *в).*

Понятие «мода» описывает режим распространения световых лучей во внутреннем сердечнике кабеля. В *одномодовом кабеле* (Single Mode Fiber, SMF) используется центральный проводник очень малого диаметра, соизмеримого с длиной волны света – от 5 до 10 мкм. При этом практически все лучи света распространяются вдоль оптической оси световода, не отражаясь от внешнего проводника.

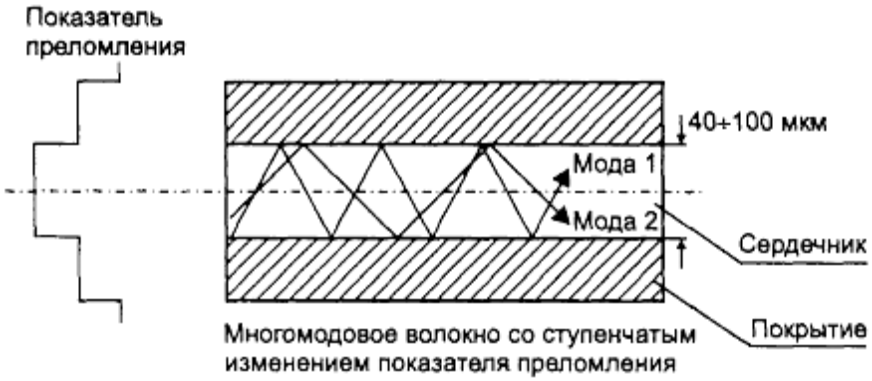


Рис. 8.5, *а*. Схема распространения сигнала в оптическом волокне

Рис. 8.5, *б*. Схема распространения сигнала в оптическом волокне

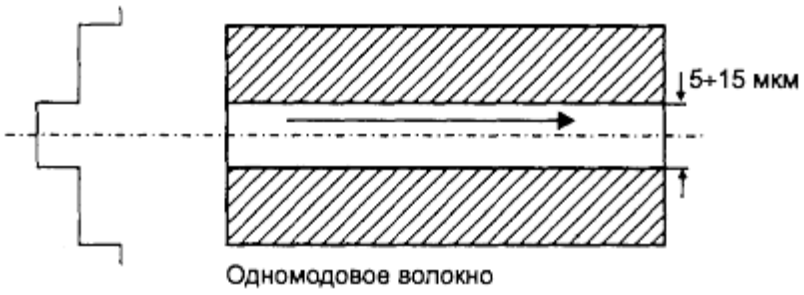


Рис. 8.5, *в*. Схема распространения сигнала в оптическом волокне

Полоса пропускания одномодового кабеля очень широкая – до сотен гигагерц на километр. Изготовление тонких качественных волокон для одномодового кабеля представляет сложный технологический процесс, что делает одномодовый кабель достаточно дорогим. Кроме того, в волокно такого маленького диаметра достаточно сложно направить пучок света, не потеряв при этом значительную часть его энергии.

В *многомодовых кабелях* (Multi Mode Fiber, MMF) используются более широкие внутренние сердечники, которые легче изготовить технологически. В многомодовых кабелях во внутреннем проводнике одновременно существует несколько световых лучей, отражающихся от внешнего проводника под разными углами. Угол отражения луча называется модой луча. В многомодовых кабелях с плавным изменением коэффициента преломления режим распространения каждой моды имеет более сложный характер. Многомодовые кабели имеют более узкую полосу пропускания – от 500 до 800 МГц/км. Сужение полосы происходит из-за потерь световой энергии при отражениях, а также из-за интерференции лучей разных мод.

В качестве источников излучения света в волоконно-оптических кабелях применяются светодиоды и полупроводниковые лазеры. Для одномодовых кабелей применяются только полупроводниковые лазеры, так как при таком малом диаметре оптического волокна световой поток, создаваемый светодиодом, невозможно без больших потерь направить в волокно. Для многомодовых кабелей используются более дешевые светодиодные излучатели. Волоконно-оптические кабели обладают отличными характеристиками всех типов: электромагнитными, механическими (хорошо гнутся, а в соответствующей изоляции обладают

хорошей механической прочностью). Однако у них есть один серьезный недостаток – сложность соединения волокон с разъемами (MIC, ST и SC) и между собой при необходимости наращивания длины кабеля.

На рисунке 8.6 изображена отдельная оптоволоконная жила (а) и поперечное сечение трехжильного кабеля.

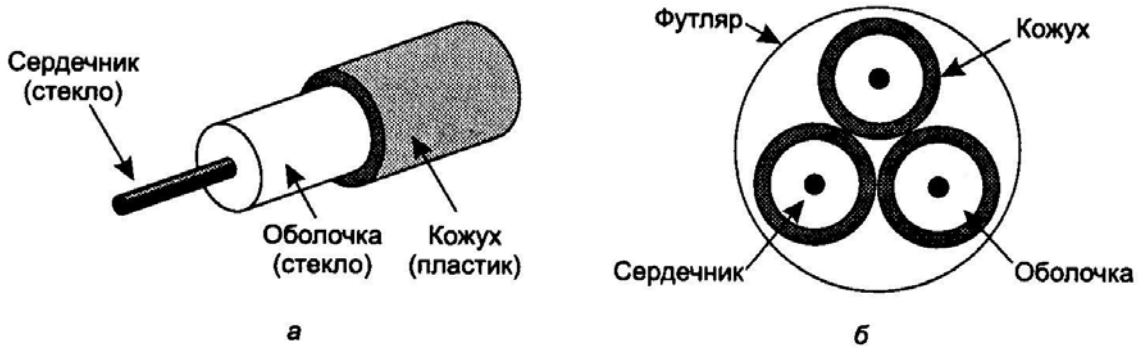


Рис. 8.6. Структура оптоволоконной жилы (*а*) и кабеля из трех волокон (*б*)

Соединение отрезков кабеля может осуществляться тремя способами. Во-первых, на конец кабеля может прикрепляться специальный разъем, с помощью которого кабель вставляется в оптическую розетку. Подобное соединение приводит к потере 10-20% силы света, зато оно позволяет легко изменить конфигурацию системы.

Во-вторых, они могут механически сращиваться – два аккуратно отрезанных конца кабеля укладываются рядом друг с другом и зажимаются специальной муфтой. Улучшение прохождения света достигается выравниванием концов кабеля. При этом через соединение пропускается свет, и задачей является добиться максимального соответствия мощности выходного сигнала мощности входного. Одно механическое сращивание кабелей занимает у опытного монтажника сетей около 5 минут и дает в результате потерю 10 % мощности света.

В-третьих, два куска кабеля могут быть сплавлены вместе. Сплавное соединение почти так же хорошо, как и сплошной кабель, но даже при таком методе происходит небольшое уменьшение мощности света.

Во всех трех типах соединений в точке соединения могут возникнуть отражения, и отраженный свет может интерферировать с сигналом.

Сама стоимость волоконно-оптических кабелей ненамного превышает стоимость кабелей на витой паре, однако проведение монтажных работ с оптоволокном обходится намного дороже из-за трудоемкости операций и высокой стоимости применяемого монтажного оборудования. Так, присоединение оптического волокна к разъему требует проведения высокоточной обрезки волокна в плоскости, строго перпендикулярной оси волокна, а также выполнения соединения путем сложной операции склеивания, – а не обжатия, как это делается для витой пары. Выполнение же некачественных соединений сразу резко сужает полосу пропускания волоконно-оптических кабелей и линий.

Несмотря на относительную дороговизну, оптоволоконная передача обладает целым рядом преимуществ.

Оптоволокно имеет высокую пропускную способность, исчисляемую гигабитами в секунду, и малые потери сигнала. По сравнению с медью допускает большую длину сегментов (участков кабеля без промежуточного активного оборудования), исчисляемую километрами.

Оптоволокно легче и компактнее медного кабеля.

Оптоволокно обеспечивает *гальваническую* развязку соединяемых узлов с любым необходимым напряжением изоляции. Это относится к чисто диэлектрическим кабелям, не использующим металлических силовых элементов, и не имеющим медных жил.

Оптоволокно безопасно с точки зрения применения во взрывоопасной среде.

Оптоволоконный кабель практически нечувствителен к электромагнитным помехам (кроме сверхмощных, возникающих при ядерном взрыве) и сам не является источником помех.

Оптоволоконная связь обеспечивает высокую защищенность информации от несанкционированного доступа. Для съема информации необходимо физическое подключение к волокну – врезка ответвителя, которую затруднительно осуществить незаметно.

По всем техническим характеристикам одномодовое волокно превосходит многомодовое, причем цена одномодового волокна

заметно ниже. Однако, стоимость оконечного оборудования для него существенно выше, что обусловлено сложностью генерации узконаправленного длинноволнового луча и более высокими требованиями к прецизионности элементов. По этой причине одномодовое волокно в основном применяют для связи на дальние расстояния, а многомодовое шире применяют в локальных сетях. Утверждение, что оптические линии, проложенные для существующих технологий, для повышения пропускной способности ожидают только новых источников и приемников сигналов, безусловно, справедливо лишь для одномодового волокна. Далеко не все многомодовые кабели обладают полосой пропускания, достаточной для работы Gigabit Ethernet с максимальной длиной магистрали.

За высокие параметры оптоволокна приходится платить пока что довольно высокую цену, поскольку дорого все – и активное оборудование, и разъемы, и инструмент, и работы по оконцовке кабеля. Сам кабель по цене вполне сопоставим с медным. В отличие от оконцовки медного кабеля, где установка разъема может занимать меньше минуты, установка и полировка оптического коннектора занимает гораздо больше времени и требует высокой квалификации и умелых рук инсталлятора. Для оконцовки требуется большое количество специальных инструментов и расходных материалов. Соединители новых поколений, не требующие полировки, имеют более высокую цену. Сварка оптоволокна требует применения дорогостоящего оборудования. Прокладка оптоволоконного кабеля требует осторожности: превышение растягивающего усилия, особенно в сочетании с изгибом, может привести к обрыву волокна. Монтаж и оконцовка медного кабеля гораздо проще и дешевле.

Работа с оптоволокном требует соблюдения особых правил техники безопасности. В отличие от почти безобидных медных проводов, работа с оптоволокном может представлять серьезную опасность для здоровья:

Обрезки световодов – это микроскопические иголки, трудно видимые невооруженным глазом. Они могут переноситься ветром. Попадая на кожу или слизистые оболочки (особенно глаза), могут вызывать серьезные травмы.

Лучи источников, особенно лазерных, при попадании в глаз могут привести к травме органов зрения. Большинство излучателей работает в невидимом инфракрасном спектре, так что опасного луча и не видно. При работе с оптоволокном соблюдайте технику безопасности. С обнаженным волокном работайте в защитных очках. Не разбрасывайте обрезки волокна – их удобно собирать на колечко из липкой ленты (скотча), закрепленное на рабочем месте. Не заглядывайте в торец волокна!

8.2. Беспроводные сети

Идея цифровой беспроводной связи не нова. В 1901 году впервые была продемонстрирована телеграфная связь между кораблем и берегом при помощи азбуки Морзе, состоящей из точек и тире, что весьма похоже на двоичный код. Сегодняшние цифровые радиосистемы обладают более высокой производительностью, однако в их основе лежит та же идея. Все беспроводные сети можно разбить на следующие три категории:

– взаимодействующие системы;

– беспроводные ЛВС (LAN);

– беспроводные глобальные сети (WAN).

Под взаимодействующими системами понимается, прежде всего, связывание между собой компонентов компьютера с использованием радиоволн малого радиуса действия. Почти любой компьютер состоит из нескольких частей: монитора, клавиатуры, мыши, принтера... Каждое из этих внешних устройств, как известно, подсоединяется к системному блоку с помощью кабелей. В настоящее время разработана система беспроводной связи компонентов компьютера. Кроме стандартных устройств, с ее помощью можно подключать к компьютеру цифровые камеры, сканеры, мультимедиапроекторы и др. То есть теперь практически любые цифровые устройства, располагающиеся недалеко от системного блока, можно соединить с ним беспроводной сетью.

Следующим шагом в развитии этого направления стали беспроводные локальные вычислительные сети. В них каждый компьютер оборудован радиомодемом и антенной, с их помощью он

может обмениваться данными с другими компьютерами. В 1997 году введен стандарт 802.11, который на профессиональном жаргоне получил прозвище *WiFi*. Ко времени начала процесса стандартизации Ethernet уже играл доминирующую роль среди технологий ЛВС, поэтому было решено сделать стандарт 802.11 совместимым с Ethernet. В частности, это коснулось возможности посылать IP-пакеты по беспроводной ЛВС таким же способом, как и по обычной сети Ethernet. Данный стандарт подразумевает возможность работы в двух режимах: с базовой станцией и без базовой станции. В первом случае связь осуществляется посредством базовой станции, называемой в терминологии 802.11 точкой доступа. Во втором случае компьютеры общаются непосредственно друг с другом. Этот режим иногда называют специальной сетью. Типичным примером является случай, когда несколько людей создают беспроводную локальную сеть, объединяя в нее свои ноутбуки. При этом они обычно находятся в помещении, в котором отсутствует базовая станция.

Оба режима показаны на рис. 8.7. Иногда беспроводная ЛВС состоит из нескольких секций, в каждую из которых входит одна базовая станция, подключенная к Ethernet. Тогда в целом система выглядит как единая сеть Ethernet. Это показано на рис. 8.8. Элемент, соединяющий 802.11 с внешним миром, называется порталом.

Рис. 8.7. Варианты организации беспроводной сети

Первые беспроводные локальные сети работали на скорости 1 Мбит/с, но позднее скорость доведена до 10-50 Мбит/с. Несо-

мненно, 802.11 вскоре приведет к настоящей революции в компьютерном мире и в технологиях доступа в Интернет. Беспроводные сети уже устанавливаются в аэропортах, на железнодорожных станциях, в отелях, больших магазинах и образовательных учреждениях и становятся все более популярными.

Рис. 8.8. Организация портала

Третий тип беспроводных сетей используется в глобальных сетях. Примером может служить система сотовой связи. Первые сотовые сети были аналоговыми и предназначались только для передачи речи. Второе поколение было уже цифровым, но ничего, кроме речи, передавать по-прежнему было нельзя. Наконец, нынешнее, третье поколение – цифровое, причем появилась возможность передачи, как голоса, так и других данных.

В некотором смысле, сотовые сети – это те же беспроводные ЛВС, разница лишь в зоне охвата и более низкой скорости передачи. Если обычные беспроводные сети могут работать со скоростью до 50 Мбит/с на расстоянии десятков метров, то сотовые системы передают данные на скорости 1 Мбит/с, но расстояние от базовой станции до компьютера или телефона исчисляется километрами, а не метрами. Сейчас развиваются высокопроизводительные глобальные беспроводные сети. Эта технология имеет свой стандарт, IEEE 802.16.

В скором времени следует ожидать широкого распространения стандарта 802.16e, реализованного в портативных компьютерах. Он имеет следующие характеристики: частотный диапазон от 2 до 11 ГГц, пропускная способность до 75 Mb/сек, радиус действия до 45 км.

Радиосвязь в последние годы получает все большее распространение в беспроводных сетях передачи информации. Ее уста-

навливают как в помещениях, так и вне зданий. Радиоволны просто сгенерировать, они могут преодолевать большие расстояния, проходить сквозь стены, огибать здания.

Свойства радиоволн зависят от частоты. При работе на низких частотах радиоволны хорошо проходят сквозь препятствия, однако мощность сигнала в воздухе резко падает по мере удаления от передатчика. На высоких частотах радиоволны вообще имеют тенденцию распространяться исключительно по прямой линии и отражаться от препятствий. Кроме того, они поглощаются, например, дождем. Радиосигналы любых частот подвержены помехам со стороны электрического оборудования. Благодаря способности радиоволн распространяться на большие расстояния взаимные помехи, вызываемые одновременно работающими пользователями, представляют собой серьезную проблему. Поэтому все государства ведут очень строгий учет владельцев радиопередатчиков.

В диапазонах LF и MF (см. рис. 8.3) радиоволны распространяются вдоль поверхности земли. Эти волны можно поймать радиоприемником на расстоянии около 1000 км. Радиоволны этих диапазонов легко проникают сквозь здания. Основным препятствием для использования этих диапазонов для передачи данных является их относительно низкая пропускная способность.

Радиоволны диапазонов HF и VHF поглощаются землей. Однако те из них, которые доходят до ионосферы, представляющей собой слой заряженных частиц, расположенный на высоте от 100 до 500 км, отражаются ею и посылаются обратно к поверхности Земли. Такие диапазоны частот используются для дальней связи.

На частотах выше 100 МГц радиоволны распространяются почти по прямой, поэтому могут быть сфокусированы в узкие пучки. Концентрация энергии в виде узкого пучка при помощи параболической антенны (вроде всем известной спутниковой телевизионной тарелки) приводит к улучшению соотношения сигнал/шум, однако для подобной связи передающая и принимающая антенны должны быть довольно точно направлены друг на друга. Кроме того, подобная направленность позволяет использовать несколько передатчиков, установленных в ряд, сигналы от которых принимаются также установленными в ряд приемными антеннами без взаимных помех.

Потребности во все большем диапазоне частот заставляют постоянно совершенствовать технологию, благодаря чему для связи используются все более высокие частоты. Микроволновая связь стала настолько широко использоваться, что начала ощущаться нехватка ширины спектра, поэтому при использовании частот существуют определенные международные и национальные соглашения.

Для связи на небольших расстояниях широко применяются инфракрасное и миллиметровое излучения. Дистанционные пульты управления для телевизоров, видеомагнитофонов и стереоаппаратуры используют инфракрасное излучение. Они относительно направленные, дешевые и легкоустанавливаемые, но имеют один важный недостаток: инфракрасное излучение не проходит сквозь твердые объекты.

С другой стороны, тот факт, что инфракрасные волны не проходят сквозь стены, является также и положительным. Ведь это означает, что инфракрасная система в одной части здания не будет интерферировать с подобной системой в соседней комнате. Кроме того, это повышает защищенность инфракрасной системы от прослушивания по сравнению с радиосистемой. По этой причине для использования инфракрасной системы связи не требуется государственная лицензия. Связь в инфракрасном диапазоне применяется в настольных вычислительных системах (например, для связи ноутбуков с принтерами), но все же не играет значимой роли в телекоммуникации.

Достаточно широкое распространение получила беспроводная связь для соединения локальных сетей между зданиями при помощи лазеров, установленных на крышах. Связь с помощью когерентных волн лазера является сугубо однонаправленной, поэтому для двусторонней связи необходимо на каждой крыше установить по лазеру и по фотодетектору. Такая технология позволяет организовать связь с очень высокой пропускной способностью при очень низкой цене. Кроме того, такая система довольно просто монтируется и, в отличие от микроволновой связи, не требует лицензии.

Узкий луч лазера наряду с преимуществами, создает некоторые проблемы. Чтобы попасть узким лучом в фотодетектор, необходима точная настройка. Недостатком луча является также

его отклонение и даже неспособность проходить сквозь густой туман и дождь, а также отклонение из-за конвекции горячего воздуха (см. рис. 8.9).

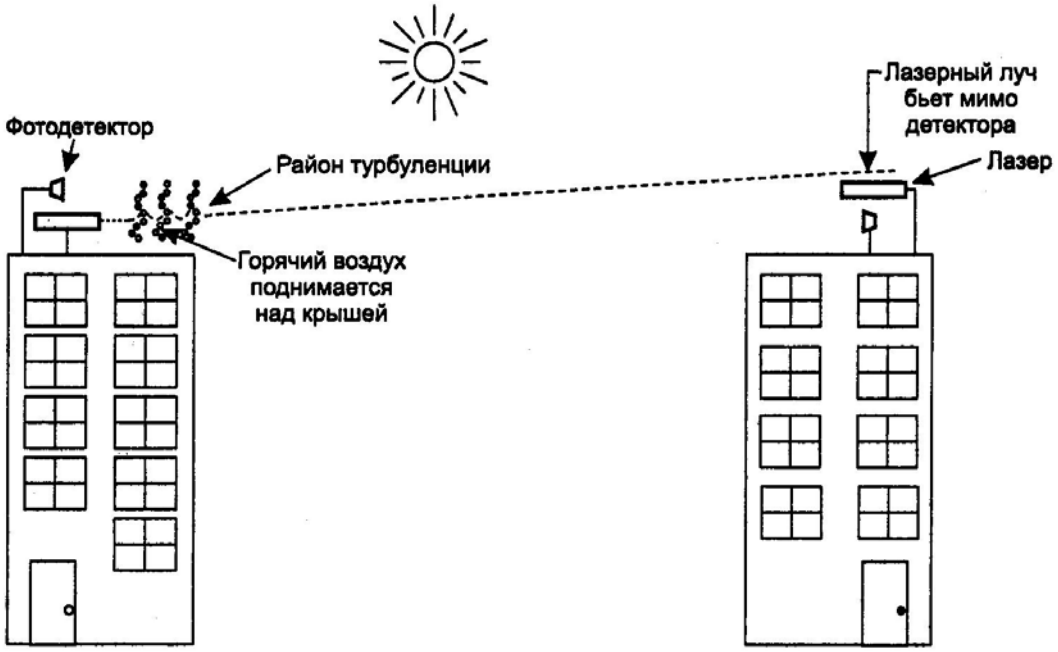


Рис. 8.9. Связь с помощью лазера

В создании беспроводных коммуникаций важная роль принадлежит спутникам связи. Спутникам связи присущи определенные свойства, делающие их чрезвычайно привлекательными для самых разных областей применения. Спутник связи можно представить в виде огромного микроволнового повторителя, висящего в небе. Он включает в себя несколько *транспондеров*, каждый из которых настроен на определенную часть частотного спектра. Транспондеры усиливают сигналы и преобразуют их на новую частоту, чтобы при отправке на Землю отраженный сигнал не накладывался на прямой. Нисходящий луч может быть как широким, покрывающим огромные пространства на Земле, так и узким, который можно принять в области, ограниченной лишь несколькими сотнями километров. Последний метод называется *трубой*.

В соответствии с законом Кеплера, период обращения спутника зависит от его орбиты. Вблизи поверхности Земли период обращения вокруг нее составляет примерно 90 минут. Следовательно, спутники, расположенные на малой высоте, слишком быстро исчезают из вида приемно-передающих устройств, располо-

женных на Земле, поэтому необходимо организовывать непрерывные зоны покрытия.

На высоте 35800 км располагаются *геостационарные спутники* (GEO) с периодом обращения 24 часа. В технологии GEO задержка передачи сигнала составляет около 270 мс. Важным свойством спутников является то, что они являются исключительно широковещательным средством передачи данных. На отправку сообщения сотням абонентов, находящихся в зоне следа спутника, не затрачивается никаких дополнительных ресурсов по сравнению с отправкой сообщения одному из них. Для некоторых применений это свойство очень полезно. Например, можно представить себе кэширование на спутнике популярных веб-страниц, что резко повысит скорость их загрузки на сотни компьютеров, находящихся довольно далеко друг от друга. С другой стороны, с точки зрения защиты информации и конфиденциальности данных, спутники доставляют большие проблемы, так как их может прослушивать кто угодно. Здесь на защиту тех, кому важен ограниченный доступ к информации, встает криптография. Спутники связи обладают еще одним замечательным свойством – независимостью стоимости передачи от расстояния между узлами. Космические телекоммуникационные технологии, кроме того, обеспечивают очень высокую степень защиты от ошибок и могут быть развернуты на местности практически мгновенно.

Средневысотные спутники вращаются вокруг земли на высоте около 18000 км. Если смотреть на них с Земли, то будет заметно их медленное дрейфование по небосводу. Средневысотные спутники делают полный оборот вокруг нашей планеты примерно за 6 часов. Поскольку эти спутники находятся гораздо ниже, чем геостационарные, то и «засвечиваемое» ими пятно на поверхности Земли имеет более скромные размеры. Зато для связи с ними требуются менее мощные передатчики.

На высоте около 1000 км вращаются *низкоорбитальные спутники*. Для того чтобы создать целостную систему, охватывающую весь земной шар, нужно большое количество таких спутников. Причиной тому является, прежде всего, высокая скорость их движения по орбите. С другой стороны, благодаря относительно небольшому расстоянию между наземными передатчиками и спутниками не требуется мощных передатчиков, а задержки со-

ставляют несколько миллисекунд. Примером низкоорбитальных спутников являются проекты Iridium и Globalstar. Система Iridium состоит из 66 спутников, вращающихся на высоте 750 км. Эта система обеспечивает пересылку данных между удаленными абонентами путем передачи сигналов от одного спутника к другому. Связь предоставляется с любой точки земного шара при помощи ручных устройств. Система Globalstar построена на 48 спутниках

Проект Teledesic предназначен для пользователей Интернета по всему миру, которым требуется высокая пропускная способность канала. Целью Teledesic было обеспечить миллионы пользователей Интернета спутниковым каналом связи со скоростью 100 Мбит/с. Система состоит из 30 спутников, вращающихся на высоте 130 км. Передача должна осуществляться в высокочастотном диапазоне с широкой полосой. Teledesic представляет собой космическую систему с коммутацией пакетов, при этом каждый спутник является маршрутизатором и может пересылать данные на соседние спутники. Когда пользователь запрашивает полосу для передачи данных, она предоставляется ему динамически на 50 мс. Систему предполагается запустить в 2005 году.

На сегодняшний день оптоволоконные кабели стали победителями среди средств связи. Тем не менее, у спутников имеются свои области применения, в которых оптоволокно, увы, бессильно. Во-первых, несмотря на то, что у отдельно взятого оптического волокна пропускная способность выше, чем у всех спутников вместе взятых, большинству пользователей это мало что дает. Пока что оптоволоконные кабели используются в основном в телефонных сетях для обеспечения большого количества одновременных звонков. При применении спутниковой системы достаточно установить антенну на крыше дома, и пользователь получит очень неплохую пропускную способность линии, никак не связанной с телефонной сетью. Эту идею использует, например, Teledesic.

Второй областью применения спутниковой связи является мобильная телефония. Третья область касается вопросов, в которых принципиально широковещание. Сообщение, отправленное через спутник, могут получить одновременно тысячи абонентов

на Земле. В-четвертых, нельзя забывать о местах, куда очень тяжело протянуть кабель.

В целом, основным средством телекоммуникаций на Земле, вероятно, будет комбинация оптоволокна и сотовой радиосвязи. Хотя оптоволоконные кабели обладают очень высокой пропускной способностью, беспроводные системы, как наземные, так и спутниковые, будут вести очень жесткую политику ценовой конкуренции. Если будет продолжаться удешевление спутниковых систем, а низкоорбитальные спутники постепенно будут все больше использоваться в телекоммуникациях, то не исключено, что оптоволоконные сети уйдут с ведущих ролей на большинстве рынков.

8.3. Режимы передачи информации

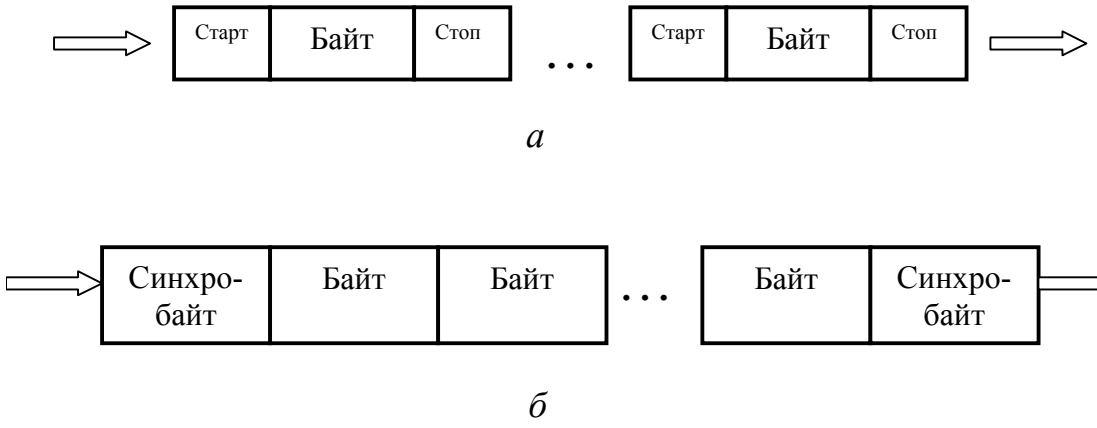
При обмене данными на физическом уровне единицей информации является бит, поэтому средства физического уровня всегда поддерживают побитовую синхронизацию между приемником и передатчиком. Канальный уровень оперирует кадрами данных и обеспечивает синхронизацию между приемником и передатчиком на уровне кадров. В обязанности приемника входит распознавание начала первого байта кадра, распознавание границ полей кадра и распознавание признака окончания кадра. Обычно достаточно обеспечить синхронизацию на указанных двух уровнях – битовом и кадровом, чтобы передатчик и приемник смогли обеспечить устойчивый обмен информацией.

Однако при плохом качестве линии связи для удешевления аппаратуры и повышения надежности передачи данных вводят дополнительные средства синхронизации на уровне байт. Такой режим работы называется асинхронным или старт-стопным. Другой причиной использования такого режима работы является наличие устройств, которые генерируют байты данных в случайные моменты времени. Так работает клавиатура, с которой человек вводит данные для обработки их компьютером. В асинхронном режиме каждый байт данных сопровождается специальными сигналами «старт» и «стоп». Назначение этих сигналов состоит в том, чтобы, во-первых, известить приемник о

приходе данных и, во-вторых, чтобы дать приемнику достаточно времени для выполнения некоторых функций, связанных с синхронизацией, до поступления следующего байта.

При синхронном режиме передачи старт-стопные биты между каждой парой байт отсутствуют. Пользовательские данные собираются в кадр, который начинается и заканчивается байтами синхронизации. Байт синхронизации – это байт, содержащий заранее известный код, например 0111110, который оповещает приемник о приходе кадра данных. При его получении приемник должен войти в режим байтовой синхронизации с передатчиком, то есть правильно понимать начало очередного байта кадра.

На рисунке 8.10 изображены схемы асинхронной (*а*) и синхронной (*б*) передачи на уровне байтов.



а

б

Рис. 8.10. Схема асинхронной (*а*) и синхронной (*б*) передачи

В зависимости от направления возможной передачи данных способы передачи данных по линии связи делятся на следующие типы:

симплексный – передача осуществляется по линии связи только в одном направлении;

полудуплексный – передача ведется в обоих направлениях, но попеременно во времени (примером такой передачи служит технология Ethernet);

дуплексный – передача ведется одновременно в двух направлениях.

Дуплексный режим – наиболее универсальный и производительный способ работы канала. Самым простым вариантом организации дуплексного режима является использование двух неза-

висимых физических каналов (двух пар проводников или двух световодов) в кабеле, каждый из которых работает в симплексном режиме, то есть передает данные в одном направлении. Именно такая идея лежит в основе реализации дуплексного режима работы во многих сетевых технологиях, например Fast Ethernet или ATM. Иногда такое простое решение оказывается недоступным или неэффективным. Чаще всего это происходит в тех случаях, когда для дуплексного обмена данными имеется всего один физический канал, а организация второго связана с большими затратами. Например, при обмене данными с помощью модемов через телефонную сеть у пользователя имеется только один физический канал связи с АТС – двухпроводная линия. В таких случаях дуплексный режим работы организуется на основе разделения канала на два логических подканала с помощью технологии частотного мультиплексирования (Frequency Division Multiplexing, FDM) или временного мультиплексирования (Time Division Multiplexing, TDM).

Модемы для организации дуплексного режима работы на двухпроводной линии применяют технику FDM. Модемы, использующие частотную модуляцию, работают на четырех частотах: две частоты – для кодирования единиц и нулей в одном направлении, а остальные две частоты – для передачи данных в обратном направлении.

При цифровом кодировании дуплексный режим на двухпроводной линии организуется с помощью техники TDM. Часть тайм-слотов используется для передачи данных в одном направлении, а часть – для передачи в другом направлении. Обычно тайм-слоты противоположных направлений чередуются. TDM-разделение линии характерно, например, для цифровых сетей с интеграцией услуг (ISDN) на абонентских двухпроводных окончаниях. В волоконно-оптических кабелях с одним оптическим волокном для организации дуплексного режима работы применяется передача данных в одном направлении с помощью светового пучка одной длины волны, а в обратном – с другой длины волны.

При передаче кадров данных на канальном уровне используются как дейтаграммные процедуры, работающие без установления соединения, так и процедуры с предварительным установлением логического соединения.

При дейтаграммной передаче кадр посылается в сеть «без предупреждения», и никакой ответственности за его утерю протокол не несет (рис. 8.11, *а*). Предполагается, что сеть всегда готова принять кадр от конечного узла. Дейтаграммный метод работает быстро, так как никаких предварительных действий перед отправкой данных не выполняется. Однако при таком методе трудно организовать в рамках протокола отслеживание факта доставки кадра узлу назначения. Этот метод не гарантирует доставку пакета.

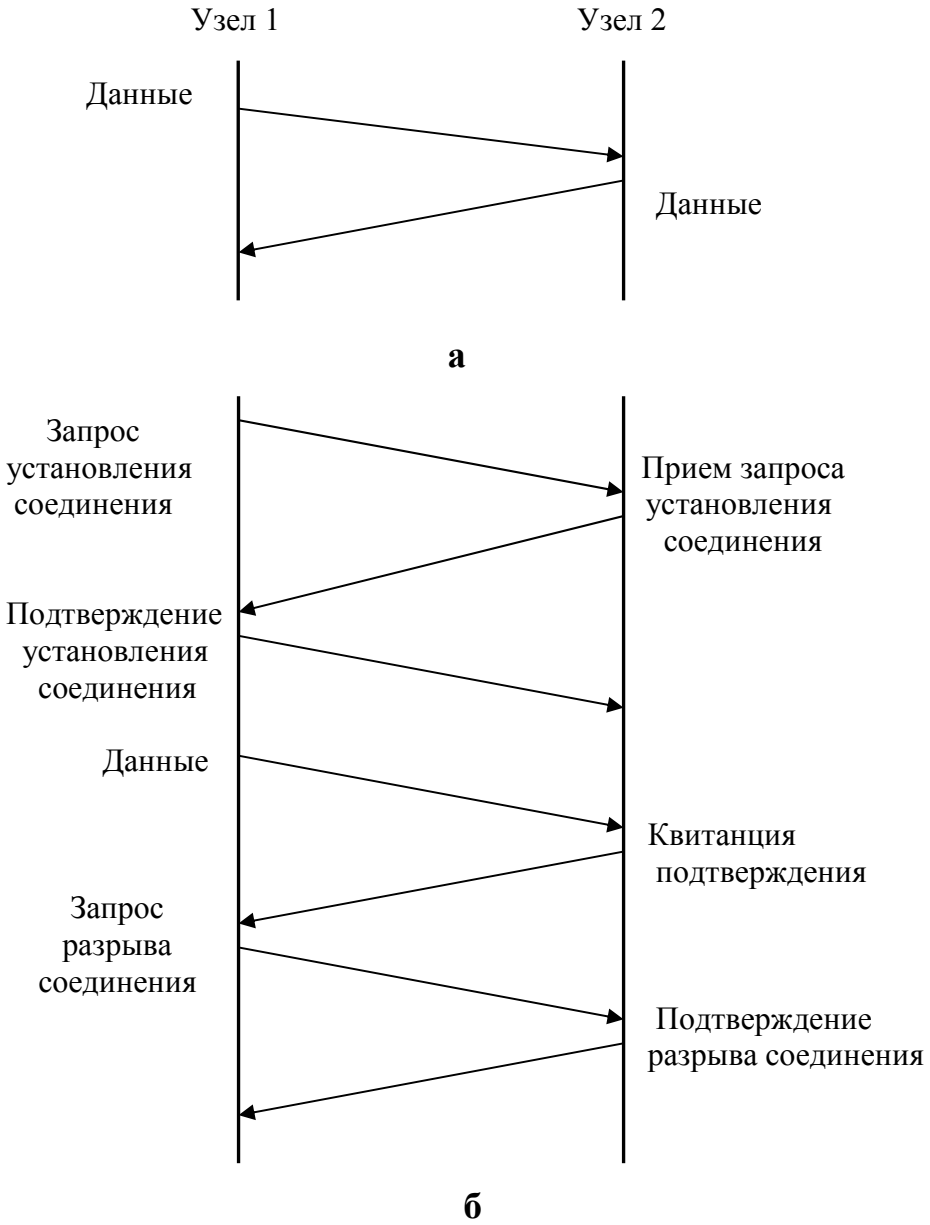


Рис. 8.11. Схема дейтаграммной передачи (*а*) и передачи с установлением соединения (*б*)

Передача с установлением соединения более надежна, но требует больше времени для передачи данных и вычислительных затрат от конечных узлов. В этом случае узлу-получателю отправляется служебный кадр специального формата с предложением установить соединение (рис. 8.11, *б*). Если узел-получатель согласен с этим, то он посылает в ответ другой служебный кадр, подтверждающий установление соединения и предлагающий для данного логического соединения некоторые параметры, например идентификатор соединения, максимальное значение поля данных кадров, которые будут использоваться в рамках данного соединения и другие. Узел-инициатор соединения может завершить процесс установления соединения отправкой третьего служебного кадра, в котором сообщит, что предложенные параметры ему подходят. На этом логическое соединение считается установленным, и в его рамках можно передавать информационные кадры с пользовательскими данными.

После передачи некоторого законченного набора данных, например определенного файла, узел инициирует разрыв данного логического соединения, посылая соответствующий служебный кадр.

Заметим, что, в отличие от протоколов дейтаграммного типа, которые поддерживают только один тип кадра – информационный, протоколы, работающие по процедуре с установлением соединения, должны поддерживать несколько типов кадров – служебные, для установления (и разрыва) соединения и информационные, переносящие собственно пользовательские данные.

8.4. Компрессия данных

Компрессия (сжатие) данных применяется для сокращения времени их передачи. Так как на компрессию данных передающая сторона тратит дополнительное время, к которому нужно еще прибавить аналогичные затраты времени на декомпрессию этих данных принимающей стороной, то выгоды от сокращения времени на передачу сжатых данных обычно бывают заметны только для низкоскоростных каналов. Этот порог скорости для современной аппаратуры составляет около 64 Кбит/с. Многие

программные и аппаратные средства сети способны выполнять *динамическую компрессию* данных, в отличие от статической, когда данные предварительно компрессируются (например, с помощью популярных архиваторов типа WinZip), а уже затем отсылаются в сеть. На практике может использоваться ряд алгоритмов компрессии, каждый из которых применим к определенному типу данных. Некоторые модемы (называемые интеллектуальными) предлагают *адаптивную компрессию*, при которой в зависимости от передаваемых данных выбирается определенный алгоритм компрессии. Рассмотрим некоторые из общих алгоритмов компрессии данных.

Десятичная упаковка. Когда данные состоят только из чисел, значительную экономию можно получить путем уменьшения количества используемых на цифру бит с 7 до 4, используя простое двоичное кодирование десятичных цифр вместо кода ASCII. Просмотр таблицы ASCII показывает, что старшие три бита всех кодов десятичных цифр содержат комбинацию 011. Если все данные в кадре информации состоят из десятичных цифр, то, поместив в заголовок кадра соответствующий управляющий символ, можно существенно сократить длину кадра.

Относительное кодирование. Альтернативой десятичной упаковке при передаче числовых данных с небольшими отклонениями между последовательными цифрами является передача только этих отклонений вместе с известным опорным значением.

Символьное подавление. Часто передаваемые данные содержат большое количество повторяющихся байт. Например, при передаче черно-белого изображения черные поверхности будут порождать большое количество нулевых значений, а максимально освещенные участки изображения – большое количество байт, состоящих из всех единиц. Передатчик сканирует последовательность передаваемых байт и, если обнаруживает последовательность из трех или более одинаковых байт, заменяет ее специальной трехбайтовой последовательностью, в которой указывает значение байта, количество его повторений, а также отмечает начало этой последовательности специальным управляющим символом.

Коды переменной длины. В этом методе кодирования используется тот факт, что не все символы в передаваемом кадре встре-

чаются с одинаковой частотой. Поэтому во многих схемах кодирования коды часто встречающихся символов заменяют кодами меньшей длины, а редко встречающихся – кодами большей длины. Такое кодирование называется также статистическим кодированием. Из-за того, что символы имеют различную длину, для передачи кадра возможна только бит-ориентированная передача. При статистическом кодировании коды выбираются таким образом, чтобы при анализе последовательности бит можно было бы однозначно определить соответствие определенной порции бит тому или иному символу или же запрещенной комбинации бит. Если данная последовательность бит представляет собой запрещенную комбинацию, то необходимо к ней добавить еще один бит и повторить анализ.

Например, если при неравномерном кодировании для наиболее часто встречающегося символа «Р» выбран код 1, состоящий из одного бита, то значение 0 однобитного кода будет запрещенным. Иначе мы сможем закодировать только два символа. Для другого часто встречающегося символа «О» можно использовать код 01, а код 00 оставить как запрещенный. Тогда для символа «А» можно выбрать код 001, для символа «П» – код 0001 и т.п. Вообще, неравномерное кодирование наиболее эффективно, когда неравномерность распределения частот передаваемых символов достаточно велика, как при передаче длинных текстовых строк. Напротив, при передаче двоичных данных, например кодов программ, оно малоэффективно, так как 8-битовые коды при этом распределены почти равномерно.

Многие модели коммуникационного оборудования, такие, как модемы, мосты, коммутаторы и маршрутизаторы, поддерживают протоколы динамической компрессии, позволяющие сократить объем передаваемой информации в 4, а иногда и в 8 раз. В таких случаях говорят, что протокол обеспечивает коэффициент сжатия 1:4 или 1:8. Существуют стандартные протоколы компрессии, например V.42bis, а также большое количество нестандартных, фирменных протоколов. Реальный коэффициент компрессии зависит от типа передаваемых данных, так, графические и текстовые данные обычно сжимаются хорошо, а коды программ – хуже.

8.5. Структурированные кабельные системы локальных сетей

8.5.1. Назначение и типы стандартов СКС

Кабельная система является основой любой сети. Чем больше сеть, тем сложнее кабельная система и тем больше эффективность работы сети зависит от функционирования кабельной системы. В связи с этим разработаны специальные стандарты по кабельной системе – структурированная кабельная система (СКС, SCS – Structured Cabling System). СКС представляет собой набор коммутационных элементов (кабелей, разъемов, кроссовых шкафов и панелей), а также набор правил (стандартов) их совместного использования без привязки к конкретным сетевым технологиям. В настоящее время детально разработаны стандарты кабельных систем для зданий. Использование структурированной кабельной системы вместо хаотически проложенных кабелей дает предприятию много преимуществ.

Универсальность. Структурированная кабельная система при продуманной организации может стать единой средой для передачи компьютерных данных в локальной вычислительной сети, организации локальной телефонной сети, передачи видеоинформации и даже для передачи сигналов от датчиков пожарной безопасности или охранных систем. Это позволяет автоматизировать многие процессы контроля, мониторинга и управления хозяйственными службами и системами жизнеобеспечения предприятия.

Увеличение срока службы. Срок морального старения хорошо структурированной кабельной системы может составлять 10 – 15 лет.

Уменьшение стоимости добавления новых пользователей и изменения их мест размещения. Известно, что стоимость кабельной системы значительна и определяется в основном не стоимостью кабеля, а стоимостью работ по его прокладке. Поэтому выгоднее провести однократную работу по прокладке кабеля, возможно, с большим запасом по длине, чем несколько раз выполнять прокладку, наращивая длину кабеля. При таком подходе все

работы по добавлению или перемещению пользователя сводятся к подключению компьютера к уже имеющейся розетке.

Возможность легкого расширения сети. Структурированная кабельная система является модульной, поэтому ее легко расширять. Например, к магистрали можно добавить новую подсеть, не оказывая никакого влияния на существующие подсети. Можно заменить в отдельной подсети тип кабеля независимо от остальной части сети. Структурированная кабельная система является основой для деления сети на легко управляемые логические сегменты, так как она сама уже разделена на физические сегменты.

Более эффективное обслуживание. Структурированная кабельная система облегчает обслуживание и поиск неисправностей по сравнению с шинной кабельной системой. При шинной организации кабельной системы отказ одного из устройств или соединительных элементов приводит к трудно локализуемому отказу всей сети. В структурированных кабельных системах отказ одного сегмента не действует на другие, так как объединение сегментов осуществляется с помощью концентраторов. Концентраторы диагностируют и локализуют неисправный участок.

Надежность. Структурированная кабельная система имеет повышенную надежность, поскольку производитель такой системы гарантирует не только качество ее отдельных компонентов, но и их совместимость.

К структурированным кабельным системам относятся три основных стандарта, действующих в настоящее время:

EIA/TIA-568-A (американский);
ISO/IEC IS 11801 (международный);
EN 50173 (европейский).

Вышеперечисленные стандарты описывают почти одинаковые кабельные системы и по многим позициям предъявляют к кабелям идентичные требования, но несколько различаются в терминологии и определениях норм для родственных параметров.

Спецификации данных стандартов ориентированы на офисное применение. В случае монтажа СКС в промышленных помещениях должна быть учтена их специфика. Целью данных спецификаций является:

– Определить общую кабельную систему для передачи голоса и данных, поддерживающую подключение аппаратуры различных производителей.

– Определить направления в разработке телекоммуникационного оборудования и кабельной продукции.

– Обеспечить планирование и установку СКС, удовлетворяющей различным требованиям персонала.

– Установить критерии пропускной способности и технические характеристики различных типов кабелей и соединительной аппаратуры.

Выполнение требований к СКС должно обеспечивать срок жизни (с учетом морального старения) системы более 10 лет. В стандартах приводятся спецификации по следующим областям: среда передачи данных, топология, допустимая длина кабелей, интерфейс подключения пользователей, кабели и соединительная аппаратура, пропускная способность, практика установки.

8.5.2. Стандарт ISO/IEC IS 11801

Стандарт на универсальную кабельную систему для помещений заказчика ISO/IEC IS 11801 был принят в 1995 году. Ниже приводится краткое изложение положений этого стандарта.

Статья 1 определяет *применимость стандарта*: он предназначен для кабельной сети проводов витая пара и оптических волокон, охватывающей одно или несколько зданий. Географическая протяженность до 3 км, площадь помещений до 1 000 000 м^2, количество обслуживаемого персонала – от 50 до 50 000 человек. Структура системы оптимизирована под эти параметры, но стандарт применим и при выходе за эти границы. Кабельная система поддерживает широкий спектр сервисов, включая голосовую связь (телефонию), передачу данных, текста, изображений и видео. Стандарт задает:

– Структуру и минимальную конфигурацию для прокладки универсальной кабельной сети.

– Требования к реализации.

– Требования к производительности отдельных кабельных линий.

– Требования соответствия и процедуры верификации.

Стандарт не распространяется на кабели и шнуры, используемые для подключения к универсальной кабельной сети оборудования, специфичного для конкретного приложения. Однако в расчетах приводятся ограничения на их длины и требования к пропускной способности.

Статья 2 содержит *ссылки на нормативные документы*, относящиеся к применяемым компонентам, процедурам тестирования, электромагнитной совместимости и т.п.

Статья 3 дает толкование используемых *терминов и сокращений*.

Статья 4 определяет *критерии соответствия кабельной проводки* данному стандарту.

Статья 5 описывает *структуру универсальной кабельной системы*, которая строится независимо от используемых коммуникационных (сетевых) приложений. СКС строится иерархически, как представлено на рис. 8.12.

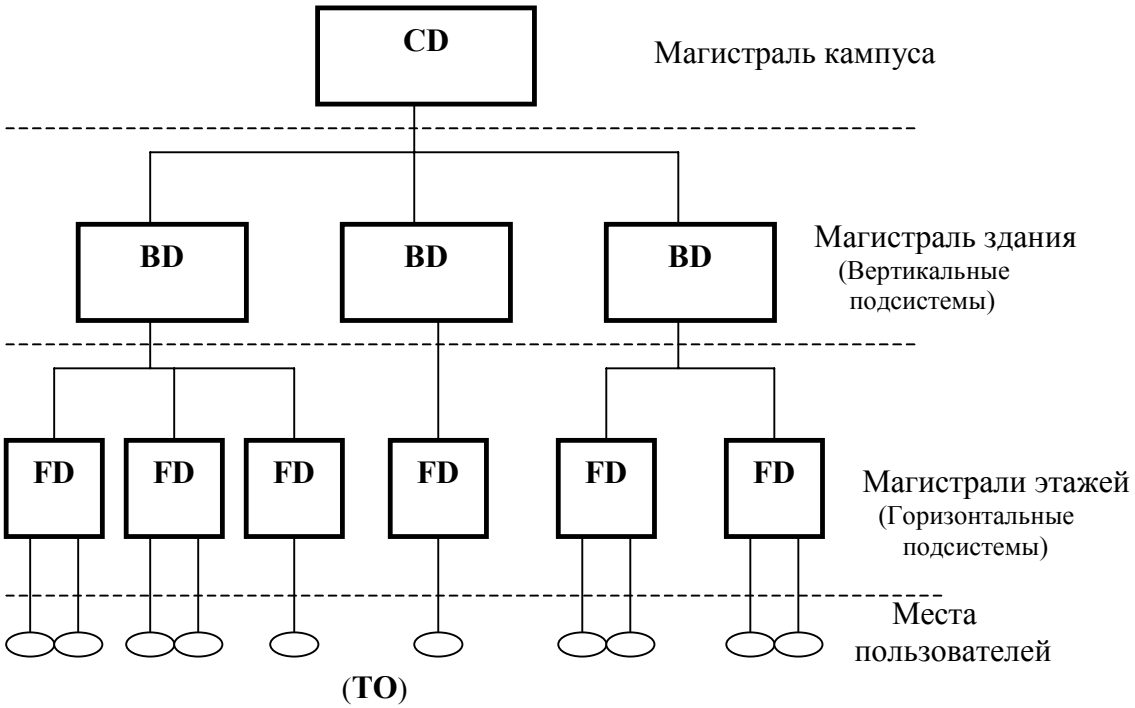


Рис. 8.12. Иерархическая структура СКС

Структура СКС состоит из следующих частей: магистраль кампуса (между зданиями), вертикальные подсистемы (внутри здания между этажами), горизонтальные подсистемы (на этажах здания).

Согласно концепции СКС по всей площади здания, на которой потенциально могут располагаться рабочие места, устанавливаются абонентские *телекоммуникационные розетки* ТО (Telecommunication Outlet). От каждой абонентской розетки прокладываются кабели к распределительным панелям, расположенным в *телекоммуникационных помещениях* ТС (Telecommunication Closet). Телекоммуникационные помещения обычно располагаются на каждом этаже здания.

Распределительные шкафы, в которых собираются кабели от абонентских розеток, называются *этажными распределителями* FD (Floor Distributor). Кабели от рабочих мест называют *горизонтальными,* хотя фактически они могут иметь и вертикальные участки (в некоторых случаях даже и межэтажные переходы, если распределители устанавливаются не на всех этажах). Этажные распределители связываются магистральными линиями с *домовым распределителем* BD (Building Distributor), эти линии называют *вертикальными*. Если сеть связывает несколько близко расположенных зданий (кампус), то домовые распределители связываются с *распределителем комплекса зданий* (кампусным распределителем) CD (Campus Distributor) магистралью комплекса зданий (кампусной магистралью). К розеткам до аппаратуры пользователей (компьютеров, принтеров и т.п.) подключаются *абонентские кабели* (шнуры) рабочей зоны. Они не являются постоянными, а специфичны для конкретных приложений и стандартом не охватываются.

Структура связей между элементами является иерархической звездообразной. В зависимости от масштабов сети она может ограничиваться и одним-двумя нижними уровнями. В большом здании возможно размещение и всех трех уровней иерархии. Кабели прокладываются между соседними уровнями иерархии распределителей, возможна прокладка кабелей и между распределителями одного уровня. Эти дополнительные линии могут использоваться некоторыми приложениями для резервирования и/или повышения пропускной способности магистрали.

Распределители размещаются в аппаратных комнатах или телекоммуникационных помещениях. Кабели прокладываются в коробах, лотках, трубах и т.п. Рекомендованные типы кабеля – витая пара и оптоволокно. В горизонтальных подсистемах, как

правило, используется витая пара. Для магистрали здания может использоваться как витая пара (средняя скорость передачи), так и оптоволокно (высокая скорость передачи). Для кампусной магистрали рекомендуется оптоволокно, а витая пара – только для телефонии (если не требуется обязательно оптоволокно по условиям эксплуатации).

При построении СКС телекоммуникационные розетки устанавливаются по всей площади, на которой могут быть расположены рабочие места, даже если в данный момент этого не требуется. Таким образом, СКС строится избыточной. Это может сэкономить средства в будущем, так как изменения в подключении новых устройств можно производить за счет перекоммутации, а стоимость последующего расширения кабельной системы может превзойти стоимость избыточности.

Телекоммуникационные помещения ТС служат для размещения распределительных шкафов и активного сетевого оборудования. Кроме того, в них обеспечиваются непрерывная подача электропитания необходимой мощности, а также требуемые климатические условия (температура, влажность, защищенность от пыли). *Аппаратные* комнаты могут не содержать распределительных панелей, в них устанавливают крупное оборудование – например, телефонные станции, серверы и т.п. В них могут устанавливаться и распределители одного и более уровней (например, CD/BD/FD).

Ввод в здание представляет собой место окончания наружных кабелей кампусной магистрали и кабелей связи с внешними сетями (например, телефонной). Здесь кабели наружного исполнения переходят в более компактные внутренние распределительные кабели, отвечающие пожарным нормам прокладки внутри помещения. По противопожарным нормам длина наружных кабелей внутри помещения до точки окончания не должна превышать 15 м. При разработке кабельной системы должны учитываться стандарты на допустимый уровень *электромагнитного излучения и чувствительности к помехам*. Кабельная сеть здания является пассивной и не тестируется на электромагнитную совместимость отдельно от приложений. Требования к электромагнитной совместимости устанавливаются отдельными стандартами. *Заземление* и соединение защитных экранирующих оболочек должны

выполняться в соответствии с требованиями HD384.5.54 и инструкциями производителей активного оборудования.

Статья 6 описывает *реализацию кабельной системы*. Применяемые кабели и соединительная аппаратура должны соответствовать ст. 8 и 9. Для электрических линий применяют симметричные кабели и соединительную аппаратуру. Горизонтальные кабели по механической длине от розетки до распределительной панели не должны превышать 90 м для любой среды (даже для оптики). Длина коммутационного шнура или провода не должна превышать 5 м. Остающиеся до 100 м «механические» 5 м распределяются между длинами абонентских и сетевых шнуров.

Магистральные кабели не могут иметь более двух иерархических уровней кроссировки. Это требование ограничивает деградацию сигналов на соединителях и упрощает администрирование. Возможны варианты и с одноуровневой иерархией, если сеть охватывает лишь одно здание или этажные распределители непосредственно связаны с кампусным распределителем. В качестве магистральных кабелей используется витая пара, одномодовое или многомодовое оптоволокно.

Максимальное расстояние от этажного распределителя до распределителя здания не должно превышать 500 м, а суммарное расстояние от этажного до кампусного распределителя не должно превышать 2 км. Эти ограничения подразумевают применение оптоволоконного кабеля, а медный кабель такой длины может применяться только для телефонных линий.

Статья 7 определяет *требования к пропускной способности линий*.

Статья 8 определяет *требования к используемым кабелям* в плане конструктивных характеристик и пропускной способности.

Конструктивные требования для симметричных электрических кабелей задают диаметр проводника, максимальный внешний диаметр кабеля, диапазон температур при эксплуатации, минимальный радиус изгиба при протягивании. При применении 4-парного кабеля UTP для горизонтальных магистралей радиус изгиба должен составлять 4 диаметра оболочки (около 2,5 см.). Статья определяет также электрические требования к кабелям. Для оптоволоконных кабелей задается номинальный диаметр, максимальное погонное затухание, минимальная полоса пропускания.

Статья 9 посвящена *соединительной аппаратуре* – средствам соединения двух кабелей или кабельных элементов. Соединительная аппаратура устанавливается в распределителях (кампусном, домовом, этажном). Аппаратура должна предоставлять:

– Средства соединения кабелей с кроссировочными шнурами и шнурами абонентской и коммуникационной аппаратуры.

– Средства идентификации кабелей для инсталляции и администрирования.

– Средства организации (укладки и закрепления) кабелей.

– Защиту от физических повреждений.

– Средства соединения экранов и заземления (если используются).

Соединительная аппаратура должна работать в диапазоне температур -10... +60°С. От прямого воздействия влаги и других коррозионных воздействий ее защищают установкой внутри помещений или в подходящие защитные кожухи (коробки, шкафы). Соединители монтируются на стенах, в стенах, в стойках и т.п.

Соединительная аппаратура должна как можно меньше ухудшать условия передачи сигналов и эффективность экранирования. При установке соединительной аппаратуры должно быть обеспечено удобство монтажа и администрирования. Кабели нужно защищать от резких изгибов, растяжений, передавливания. При монтаже необходимо предусмотреть место для установки коммуникационного оборудования, в этом случае удобен монтаж в стойках и шкафах. Маркировка обязательна, она может быть цветовой и/или алфавитно-цифровой. Если используются похожие по виду кабели с разными свойствами, маркировка должна обеспечивать их безошибочную идентификацию.

Каждый горизонтальный кабель должен оканчиваться телекоммуникационной розеткой. Соединительная аппаратура для оптоволокна должна иметь корректную маркировку по типам волокна и идентификационную маркировку, необходимую для администрирования.

Статья 10 дает общие указания по *экранированию и заземлению*, если применяемые кабели имеют общий экран или экранированные элементы. Непрерывность экрана должна обеспечиваться по всей длине канала, включая абонентские, коммутационные и шнуры подключения коммуникационного оборудования.

Соединительная аппаратура не должна ухудшать эффективность экранирования.

Все экраны должны соединяться в телекоммуникационном помещении. Обычно для этого используются металлические каркасы шкафов и стоек. Все металлические части должны соединяться с проводом заземления. Этот провод рекомендуется соединять с заземлителем, используемым для силового электропитания здания.

Статья 11 дает краткие указания по *администрированию кабельной системы*. Все элементы должны быть промаркированы и зарегистрированы, все изменения должны отражаться в документации. Рекомендуется электронная форма ведения административных документов.

Все элементы кабельной системы, а также трассы прокладки кабелей должны быть идентифицируемы. Каждый кабель, распределитель и телекоммуникационная розетка должны иметь собственный идентификатор. Каждый кабель должен быть промаркирован с обоих концов.

Документация на кабельную систему должна содержать схемы расположения кабельных трасс, розеток и распределителей с обозначенными идентификаторами. В документации должны храниться и ссылки на результаты тестирования линий. Документация должна соответствовать состоянию кабельной системы на текущий момент.

Стандарт ISO/IEC IS 11801 содержит кроме статей еще 9 приложений (A – J).

Приложения A и **B** содержат сведения о методике измерения параметров линии. Эти методики реализованы в современных кабельных тестерах.

Приложение C определяет *свойства многожильного* (гибкого) *симметричного кабеля*, применяемого для коммутационных, абонентских и шнуров оборудования.

Приложение D кратко описывает *основные топологии сетей* (шина, кольцо, звезда, дерево, сетка). В нем приводятся примеры приложений кабельной системы с разным типом топологий.

Приложение E уточняет *терминологию по отношению к экранированию.* Здесь подчеркивается, что название *STP* относится к кабелям, у которых каждый элемент (пара или четверка прово-

дов) имеет отдельный экран. Название *UTP* относится к кабелям без экранирования отдельных элементов.

Приложение F содержит краткие сведения о *передаче сигнала* по симметричному кабелю и по оптоволокну.

Приложение G содержит *перечень приложений*, поддерживаемых универсальной кабельной системой. Здесь же приводятся сведения по совместимости приложений с конкретной средой передачи.

Приложение H дает рекомендации по *планированию оптических соединений*.

Приложение J содержит *список документов*, большинство из которых описывает поддерживаемые приложения (библиография).

8.6. Аксессуары кабельных систем

К аксессуарам кабельных систем относятся различные стойки и шкафы для размещения активного и пассивного оборудования, кабелепроводы, монтажные коробки для абонентских розеток, вспомогательные материалы. Самым популярным форматом для телекоммуникационного оборудования является формат 19-дюймовых (19”) стоек и шкафов. На рисунке 8.13 представлены примеры настенных шкафов (*а*), напольного шкафа (*б*), открытой стойки (*в*).

Формат подразумевает унификацию размеров – лицевые панели должны быть прямоугольниками шириной 19” (483 мм), а высота должна быть кратна модулю U (unit) в 1,75” (44,5 мм) или его половине. Реальная высота элемента может быть и меньше, но ее округляют в большую сторону до ближайшего целого или половинного значения. Так, типовая коммутационная панель с одним рядом гнезд RJ-45 имеет высоту 1U. Панели крепятся на двух вертикальных направляющих стойках или в шкафах, которые могут быть открытыми, устанавливаемыми на полу или на стене.

Высоту стоек и шкафов обозначают в тех же единицах – «юнитах». Распространены напольные шкафы высотой 15 – 42U и настенные шкафы высотой 6 – 12U. В шкафах обычно устанавливается две пары стоек (спереди и сзади), на которые можно

монтировать специальные полки. На полки можно ставить и оборудование иных форматов (например, источники бесперебойного питания). Боковые дверцы обычно съемные, что позволяет объединять шкафы, установленные рядом. Нижняя часть шкафа снабжается съемными крышками, позволяющими подводить кабелепроводы. Под крышей предусматривается место для вентиляторов.

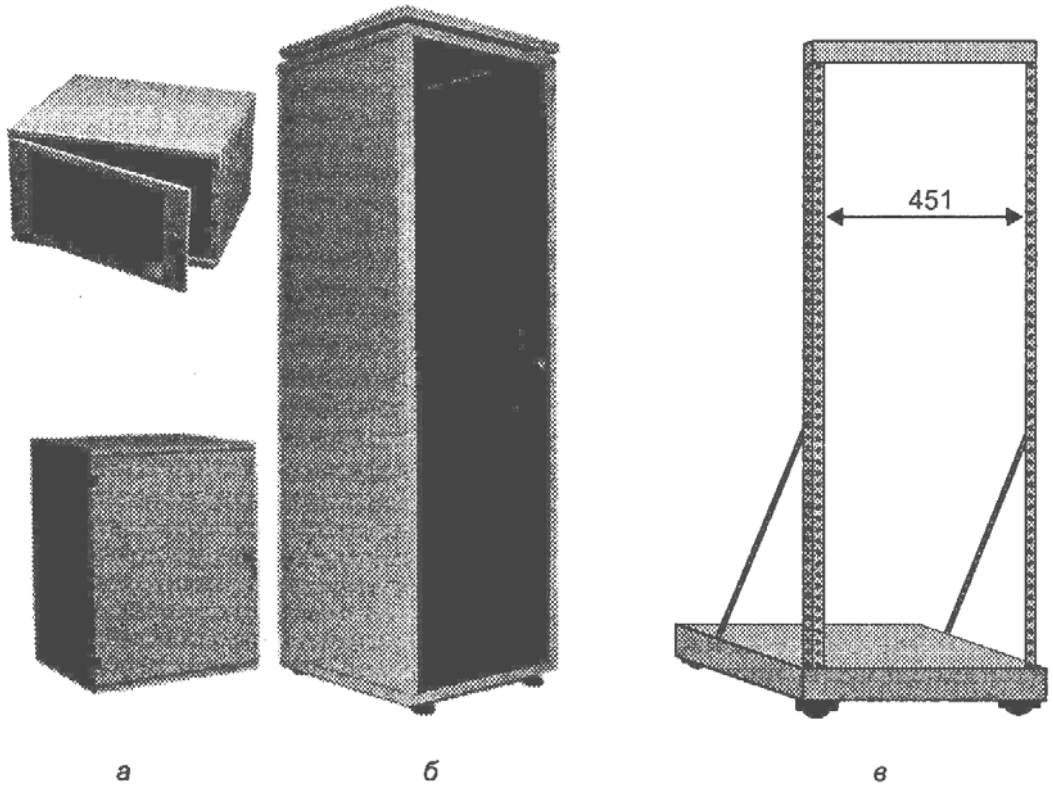


Рис. 8.13. Шкафы и стойки для телекоммуникационного оборудования

Непременным атрибутом шкафа являются запирающиеся дверцы, предотвращающие несанкционированный доступ. Все металлические части (каркас, стенки, дверцы) электрически соединяются между собой и с внутренней шиной заземления с помощью заземляющих проводов.

В шкафах монтируются распределительные и коммутационные панели (*patch panel*), средства «организации» кабелей, а также активное сетевое оборудование.

На рисунке 8.14 представлены коммутационная панель (а), блок коннекторов (б) и средства организации кабелей (в, г, д). К ним относятся различные держатели, стяжки, скобки, хомуты,

крепежные элементы и т.п. Они поддерживают коммутационные и сетевые шнуры, кабели стационарной проводки. С их помощью кабельная проводка становится надежной и элегантной.

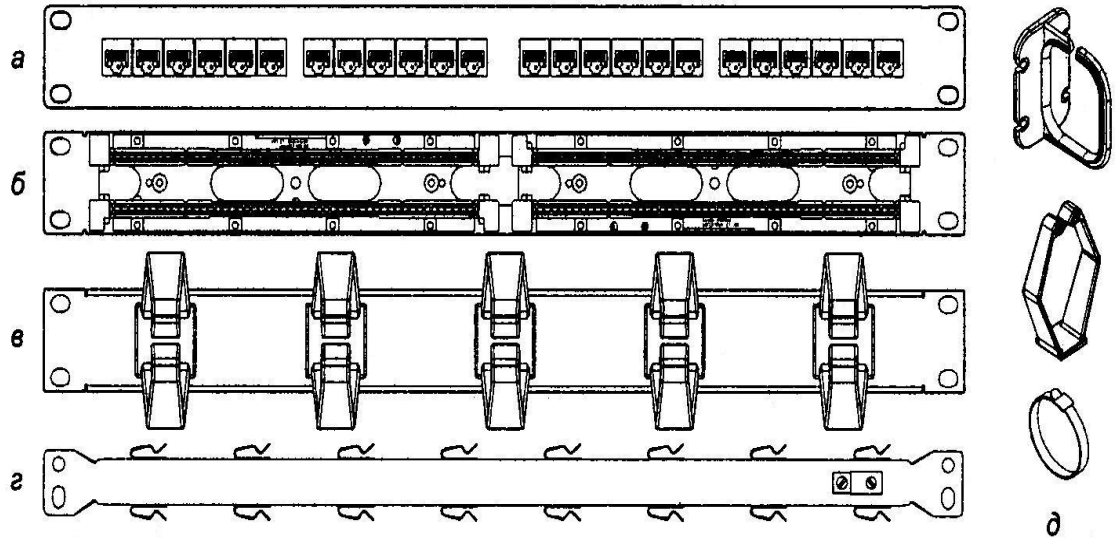


Рис. 8.14. Коммутационная панель и средства организации кабелей

На рисунке 8.15 представлен пример расположения оборудования в шкафах.

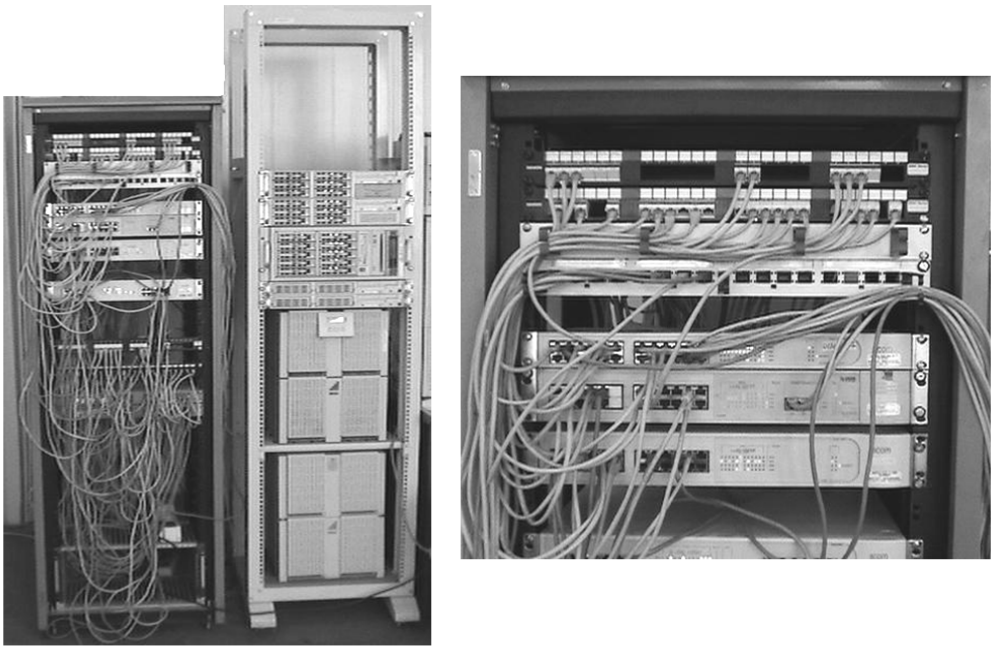


Рис. 8.15. Пример расположения оборудования в шкафах

Для укладки кабельной проводки применяются кабелепроводы различной конструкции – короба, трубы, лотки. Короба бывают различных размеров, с внутренними перегородками и без них. Короба состоят из основания, в которое укладываются кабели, и съемной крышки. Примеры сечений коробов приведены на рисунке 8.16.

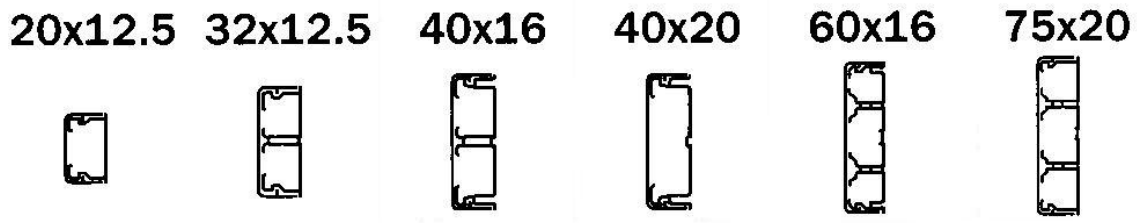


Рис. 8.16. Примеры сечений коробов

Для коробов выпускается множество вспомогательных элементов: углы (внутренние и внешние), повороты, ответвления, стыки, заглушки, рамки для оформления прохода короба через стену, переходники для стыковки коробов различного сечения, монтажные коробки для розеток и другие. На рисунке 8.17 изображен пример монтажа кабелепровода с аксессуарами (переходниками, электрическими и информационными розетками).

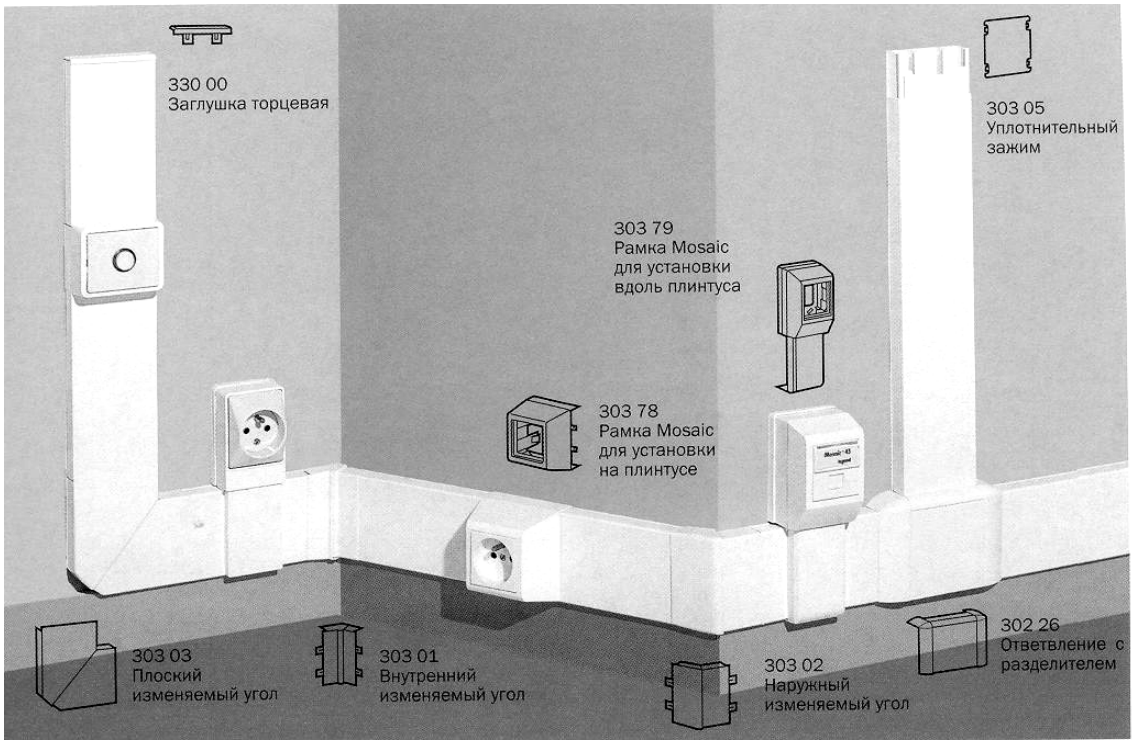


Рис. 8.17. Пример монтажа кабелепровода

Широкие (более 70 мм) короба обычно устанавливают по периметру помещений и в них же устанавливают блоки телекоммуникационных и питающих розеток. Широкие короба бывают секционированными (с внутренними перегородками). Секционированные короба позволяют развести питающие и информационные кабели на необходимое расстояние. Короба меньшего сечения используют только для прокладки кабелей, розетки приходится устанавливать в отдельных коробках (или пользоваться розетками для наружной проводки). Сечение коробов выбирается, исходя из количества и сечения прокладываемых кабелей. Следует помнить, что полностью занять все сечение кабелями не удается. При групповой прокладке можно ориентироваться на использование около 60% сечения, при индивидуальной укладке каждого кабеля можно достичь и несколько большего заполнения, но при этом перекладка кабелей может оказаться проблематичной. В углах коробов все сечение не может быть использовано полностью, поскольку необходимо соблюдать минимальный радиус изгиба кабелей. Закрытые короба в основном используют для «фасадной» части кабельной проводки. Магистрали, прокладываемые над фальш-потолком или под фальш-полом, чаще укладывают в лотки. Для прохода через стены и в некоторых других случаях применяются трубы разнообразного профиля.

Средства маркировки необходимы для организации администрирования кабельной системы. Для маркировки выпускаются различные наборы надписей и обозначений на самоклеящейся бумаге. Согласно стандартам, каждый элемент СКС должен быть промаркирован, а кабели должны маркироваться с обоих концов. Для этого можно пользоваться и несмываемым маркером, но лучше воспользоваться готовыми наклейками или клипсами с цифробуквенными обозначениями.

При проектировании кабельных систем следует придерживаться требований стандартов СКС на топологию и применяемые компоненты. Исходными данными для проектирования обычно является план помещений (а лучше строительные чертежи) с указанием размещения рабочих мест (или областей их размещения). При проектировании всегда следует брать запас по количеству рабочих мест, которое со временем может увеличиваться (появляются новые рабочие места или сетевые периферийные устрой-

ства, для которых тоже требуются телекоммуникационные розетки). По этому плану выбираются места для организации телекоммуникационных помещений с таким расчетом, чтобы горизонтальные кабели не выходили за ограничение по длине и проходили бы по удобным трассам.

Вопрос о количестве и размещении телекоммуникационных помещений решается с учетом многих местных факторов. Увеличивать их количество ради экономии суммарной длины горизонтальных кабелей далеко не всегда целесообразно, поскольку организация качественного телекоммуникационного помещения требует значительных затрат. Далее определяются трассы и возможные способы прокладки кабелей. После этого, выбрав необходимые компоненты, можно составлять спецификацию на необходимые материалы и инструменты. Процесс проектирования может быть итерационным, поскольку планы и даже чертежи помещений не всегда учитывают конкретные условия эксплуатации (соседство «неблагоприятного» оборудования, кабелей и трубопроводов и т.п.).

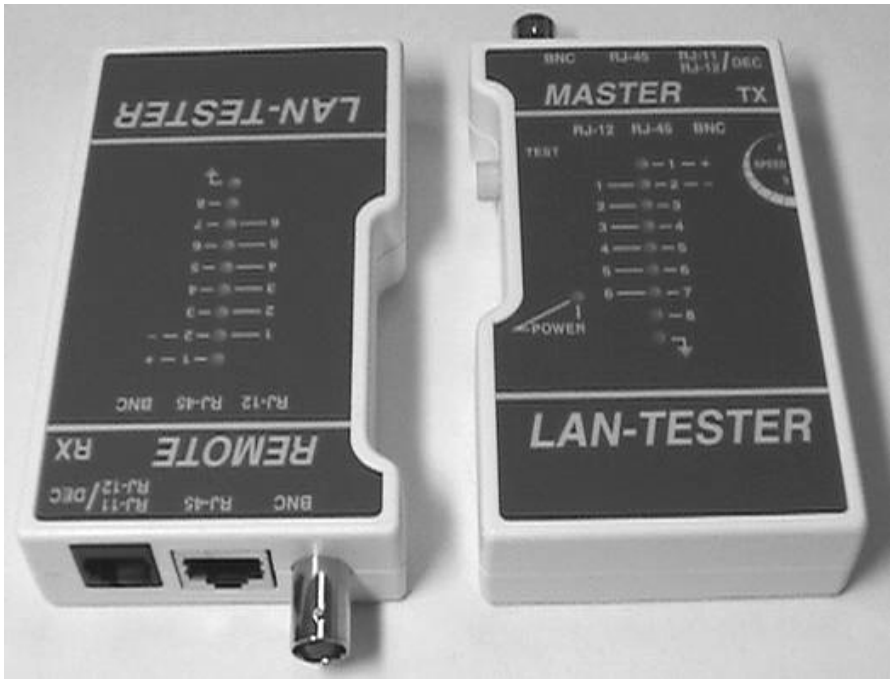


Рис. 8.18. Кабельный тестер

После выполнения монтажа кабельной системы производится ее тестирование на соответствие передаточных характеристик требованиям стандартов. Тестирование производится с помощью специальной аппаратуры. На рисунке 8.18 представлен простей-

ший портативный кабельный тестер для диагностики кабельных систем. Он позволяет определить обрывы проводников, короткие замыкания и правильность разводки кабеля по парам (например, типа UTP).

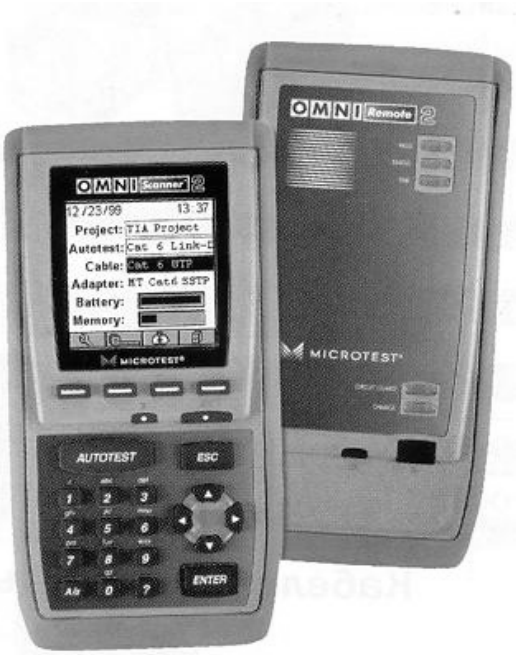


Рис. 8.19. Прибор для сертификации кабельных сетей

Рис. 8.20. Приставка для тестирования оптоволоконных линий

На рисунке 8.19 представлен прибор OMNI Scanner 2 для сертификации кабельных систем. Прибор имеет вычислительное устройство, которое с высокой точностью производит измерение

параметров трактов СКС категории 5е (затухание, длину кабеля, сопротивление и т.п.). Объем измерений позволяет дать заключение о возможности использования оборудования Gigabit Ethernet.

Прибор OMNI Scanner 2 имеет специальную приставку, позволяющую тестировать оптоволоконные кабельные линии (OMNI Fiber, рис. 8.20).

По результатам тестирования кабельных систем оформляется специальный протокол на соответствие стандартам и нормам пожарной безопасности.

Контрольные вопросы к главе 8

1. Дайте классификацию физических сред передачи данных.
2. Перечислите основные физические характеристики линий связи.
3. Дайте характеристику коаксиальных кабелей и кабелей на основе витой пары.
4. Опишите физический принцип передачи информации по оптическому волокну.
5. В чем недостатки и преимущества оптоволоконных линий связи?
6. Опишите виды и принципы организации беспроводных каналов связи.
7. Опишите принцип передачи информации с установлением соединения. В чем его отличие от дейтаграммной передачи?
8. Для чего используется компрессия данных? Каковы основные алгоритмы компрессии?
9. Для чего введены стандарты на СКС?
10. Основные положения международного стандарта на СКС.
11. Что относится к аксессуарам кабельных систем?

ГЛАВА 9

ТЕХНОЛОГИИ ЛОКАЛЬНЫХ СЕТЕЙ

9.1. Общая характеристика протоколов локальных сетей

К технологиям локальных сетей относятся классические технологии *Ethernet*, *Token Ring*, *ARCNET*, *FDDI*, а также новые технологии *Fast Ethernet*, *Gigabit Ethernet*, *100VG-AnyLAN*. Сетевые технологии локальных сетей реализуют два нижних уровня модели *OSI*. При организации взаимодействия узлов в локальных сетях основная роль отводится протоколу канального уровня. Однако для того, чтобы канальный уровень мог справиться с этой задачей, структура локальных сетей должна быть четко определенной. Например, протокол канального уровня технологии Ethernet рассчитан на параллельное подключение всех узлов сети к общей шине (отрезку коаксиального кабеля) или иерархической древовидной структуре сегментов. Протокол Token Ring также рассчитан на вполне определенную конфигурацию – соединение компьютеров в виде логического кольца.

Подобный подход, заключающийся в использовании простых структур кабельных соединений между компьютерами локальной сети, соответствовал основной цели, которую ставили перед собой разработчики первых локальных сетей. Эта цель заключалась в нахождении простого и дешевого решения для объединения в вычислительную сеть нескольких компьютеров, находящихся в пределах одного здания. Для упрощения и удешевления аппаратных и программных решений разработчики первых локальных сетей остановились на совместном использовании кабелей всеми компьютерами сети в режиме разделения времени. Использование разделяемых сред позволяет упростить логику работы сети.

Использование в локальных сетях очень простых конфигураций (общая шина и кольцо) наряду с положительными сторонами имело и отрицательные последствия. Наиболее важными из них являются ограничения по производительности и надежности. Наличие только одного пути передачи информации, разделяемого всеми узлами сети, в принципе ограничивало пропускную способность сети пропускной способностью этого пути, а надежность сети – надежностью этого пути. Поэтому по мере повышения популярности локальных сетей и расширения их сфер применения все больше стали применяться специальные коммуникационные устройства – мосты и маршрутизаторы, – которые в значительной мере снимали ограничения единственной разделяемой среды передачи данных. Базовые конфигурации в форме общей шины и кольца превратились в элементарные структуры локальных сетей, которые можно теперь соединять друг с другом более сложным образом, образуя параллельные основные или резервные пути между узлами. Тем не менее, внутри базовых структур по-прежнему работают все те же протоколы разделяемых единственных сред передачи данных.

В последние несколько лет наметилось движение к отказу от разделяемых сред передачи данных в локальных сетях и переходу к применению активных коммутаторов, к которым конечные узлы присоединяются индивидуальными линиями связи. При использовании коммутаторов у традиционных технологий появился новый режим работы – *полнодуплексный* (full-duplex). В разделяемом сегменте станции всегда работают в *полудуплексном режиме* (half-duplex), так как в каждый момент времени сетевой адаптер станции либо передает свои данные, либо принимает чужие, но никогда не делает это одновременно. В полнодуплексном режиме сетевой адаптер может одновременно передавать свои данные в сеть и принимать из сети чужие данные. Такой режим несложно обеспечивается при прямом соединении с мостом/коммутатором или маршрутизатором, так как вход и выход каждого порта такого устройства работают независимо друг от друга, каждый со своим буфером кадров. Сегодня каждая технология локальных сетей приспособлена для работы как в полудуплексном, так и полнодуплексном режимах.

Несмотря на появление новых технологий, классические протоколы локальных сетей Ethernet и Token Ring по прогнозам специалистов будут использоваться по крайней мере еще 5–10 лет. Кроме того, некоторые современные высокопроизводительные технологии, такие, как Fast Ethernet и Gigabit Ethernet, в значительной степени сохраняют преемственность со своими предшественниками.

В 1980 году в институте инженеров по электротехнике и радиоэлектронике IEEE (Institute of Electrical and Electronics Engineers) был организован комитет 802 по стандартизации локальных сетей, в результате работы которого было принято семейство стандартов IEEE 802. x, которые содержат рекомендации по проектированию нижних уровней локальных сетей. Позже результаты работы этого комитета легли в основу комплекса международных стандартов ISO. В настоящее время комитет 802 включает следующий ряд подкомитетов:

– 802.1 – Internetworking – объединение сетей;

– 802.2 – Logical Link Control, LLC – управление логической передачей данных;

– 802.3 – Ethernet с методом доступа CSMA/CD;

– 802.4 – Token Bus LAN – локальные сети с методом доступа Token Bus;

– 802.5 – Token Ring LAN – локальные сети с методом доступа Token Ring;

– 802.6 – Metropolitan Area Network, MAN – сети мегаполисов;

– 802.7 – Broadband Technical Advisory Group – техническая консультационная группа по широкополосной передаче;

– 802.8 – Fiber Optic Technical Advisory Group – техническая консультационная группа по волоконно-оптическим сетям;

– 802.9 – Integrated Voice and data Networks – интегрированные сети передачи голоса и данных;

– 802.10 – Network Security – сетевая безопасность;

– 802.11 – Wireless Networks – беспроводные сети;

– 802.12 – Demand Priority Access LAN, 100VG-AnyLAN – локальные сети с методом доступа по требованию с приоритетами.

Стандарты, разрабатываемые подкомитетом 802.1, носят общий для всех технологий характер. В подкомитете 802.1 были разработаны общие определения локальных сетей и их свойств,

определена связь трех уровней модели IEEE 802 с моделью OSI. Но наиболее практически важными являются стандарты 802.1, которые описывают взаимодействие между собой различных технологий, а также стандарты по построению более сложных сетей на основе базовых топологий. Эта группа стандартов носит общее название стандартов межсетевого взаимодействия. Подкомитет 802.2 разрабатывает стандарты на логические процедуры передачи кадров и связь с сетевым уровнем.

Стандарты семейства IEEE 802. x охватывают только два нижних уровня семиуровневой модели OSI – физический и канальный (рис. 9.1.). Это связано с тем, что именно эти уровни в наибольшей степени отражают специфику локальных сетей. Старшие уровни модели, начиная с сетевого, в значительной степени имеют общие черты, как для локальных, так и для глобальных сетей.

Специфика локальных сетей нашла свое отражение в разделении канального уровня на два подуровня: логической передачи данных (Logical Link Control, LLC) и управления доступом к среде (Media Access Control, MAC).

Уровень MAC появился из-за существования в локальных сетях разделяемой среды передачи данных. Именно этот уровень обеспечивает корректное совместное использование общей среды, предоставляя ее в соответствии с определенным алгоритмом в распоряжение той или иной станции сети. В современных локальных сетях получили распространение несколько протоколов уровня MAC, реализующих различные алгоритмы доступа к разделяемой среде и определяющих специфику таких технологий, как Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI, 100VG-AnyLAN.

Уровень LLC отвечает за передачу кадров данных между узлами с различной степенью надежности, а также реализует функции интерфейса с прилегающим к нему сетевым уровнем. Именно через уровень LLC сетевой протокол запрашивает у канального уровня нужную ему транспортную операцию с нужным качеством. Протокол LLC занимает уровень между сетевыми протоколами и протоколами уровня MAC. Протоколы сетевого уровня передают через межуровневый интерфейс данные для протокола LLC – свой пакет (например, пакет IP), адресную информацию об

узле назначения, а также требования к качеству транспортных услуг, которое протокол LLC должен обеспечить. Протокол LLC помещает пакет протокола верхнего уровня в свой кадр, который дополняется необходимыми служебными полями. Далее через межуровневый интерфейс протокол LLC передает свой кадр вместе с адресной информацией об узле назначения соответствующему протоколу уровня MAC, который упаковывает кадр LLC в свой кадр (например, кадр Ethernet).

Протоколы уровней MAC и LLC взаимно независимы – каждый протокол уровня MAC может применяться с любым протоколом уровня LLC, и наоборот.

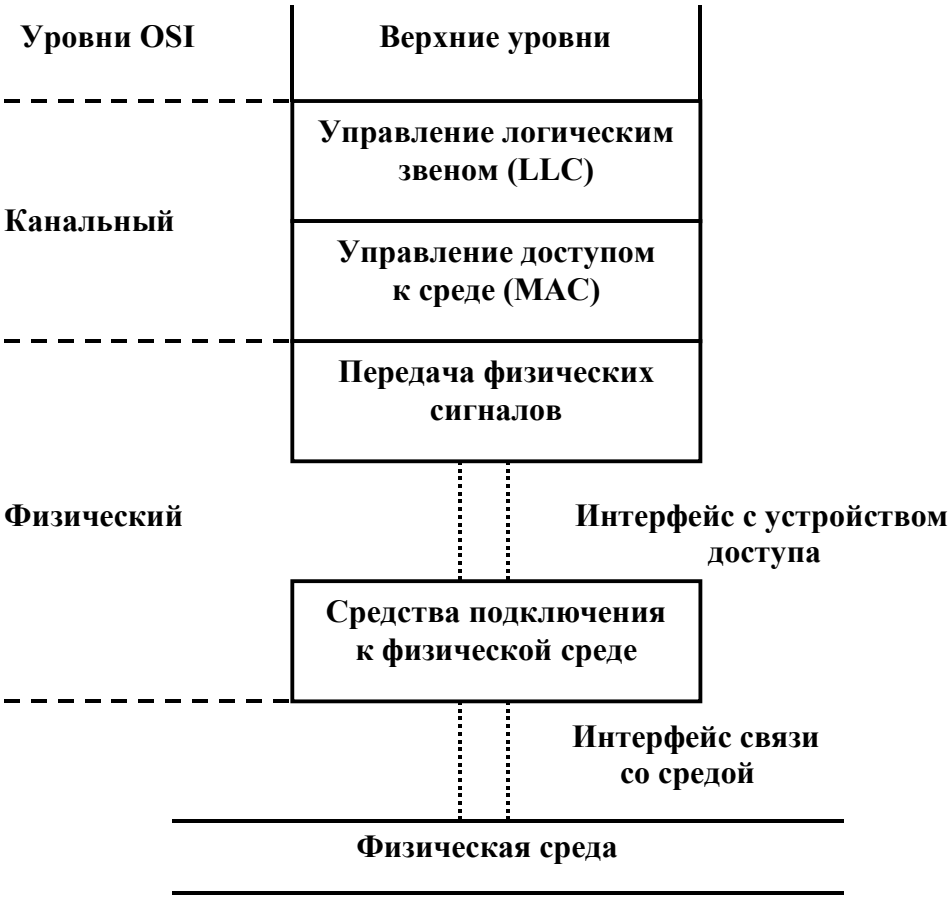


Рис. 9.1. Применение модели OSI к технологиям локальных сетей

9.2. Технология Ethernet

Ethernet – это самый распространенный на сегодняшний день сетевой стандарт локальных сетей. Он основан на экспериментальной сети Ethernet Network, разработанной и реализованной фирмой Xerox в 1975 г. В 1980 г. фирмы DEC, Intel и Xerox совместно разработали и опубликовали стандарт Ethernet для сети, построенной на основе коаксиального кабеля. На основе этого стандарта был разработан стандарт IEEE 802.3, который в зависимости от типа физической среды имеет модификации: 10Base-5, 10Base-2, 10Base-T, 10Base-F. Все виды стандартов Ethernet основаны на одинаковом методе разделения среды передачи данных. Этот метод называется CSMA/CD (Carrier Sense Multiple Access / Collision Detection, множественный доступ с контролем носителя и обнаружением столкновений) и обеспечивают скорость передачи по шине 10 Мбит/с. Физические спецификации технологии Ethernet по стандарту IEEE 802.3 на сегодняшний день включают следующие среды передачи данных:

– 10Base-5 – коаксиальный кабель диаметром 0,5" («толстый» коаксиал) с волновым сопротивлением 50 Ом и максимальной длинной сегмента 500 м (без повторителей);

– 10Base-2 – коаксиальный кабель диаметром 0,25" («тонкий» коаксиал) с волновым сопротивлением 50 Ом и максимальной длинной сегмента 185 м (без повторителей);

– 10Base-T – кабель с неэкранированной витой парой (UTP), образующий звездообразную топологию на основе концентратора, расстояние между концентратором и конечным узлом не более 100 м;

– 10Base-F – волоконно-оптический кабель с топологией аналогичной топологии стандарта 10Base-T.

В сетях Ethernet используется множественный метод доступа к среде, позволяющий вести передачу в каждый момент только одной станции. При попытке двух или более станций начать передачу одновременно возникает конфликт доступа к среде – столкновение (коллизия). В этом случае все конфликтующие станции должны прервать передачу данных и возобновлять по-

пытки по истечении случайного интервала времени (паузы). Длительность паузы определяется по формуле:

$$P=L\times I,$$

где I – интервал отсрочки, а L – случайное целое число в диапазоне $[0,2^N]$ при N от 1 до 10. Интервал отсрочки равен 512 битовым интервалам. Битовый интервал соответствует времени между появлением двух последовательных бит на кабеле (для скорости 10 Мбит/с величина битового интервала равна 0,1 мкс).

Хотя в сетях Ethernet коллизии являются нормальным явлением, они увеличивают задержку и приводят к излишнему расходу полосы пропускания среды. Пакеты или их фрагменты, переданные во время конфликта, должны быть отброшены.

С ростом уровня загрузки сети (расход полосы), вероятность конфликтов возрастает. В большой сети на обнаружение коллизии, оповещение об этом сигналом «затора» и разрешение конфликта затрачивается достаточно много времени. Кроме того, на разрешение конфликтов расходуется часть полосы пропускания сетевой среды.

Домен коллизий (collision domain) – это часть сети Ethernet, все узлы которой распознают коллизию независимо от того, в какой части этой сети коллизия возникла. Сеть Ethernet, построенная на повторителях, всегда образует один домен коллизий. Домен коллизий соответствует одной разделяемой среде. Мосты, коммутаторы и маршрутизаторы делят сеть Ethernet на несколько доменов коллизий. Протокол CSMA/CD, используемый в сетях Ethernet для разрешения конфликтов при получении доступа к среде передачи, налагает ряд ограничений на устройства и кабельную систему сетей. В сегменте (домен коллизий) не может находиться более 1024 устройств и 4 концентраторов между любыми двумя станциями (для 10Base-T).

Промежуток времени между окончанием одного пакета и началом следующего, равный 9,6 мкс, позволяет ясно различать отдельные пакеты. При передаче пакетов через повторители этот промежуток может уменьшаться. Повторитель восстанавливает синхронизацию сигналов для устранения искажений при передаче через сетевую среду.

Четкое распознавание коллизий всеми станциями сети является необходимым условием корректной работы сети Ethernet. Если какая-либо передающая станция не распознает коллизию и решит, что кадр данных ею передан верно, то этот кадр данных будет утерян. Из-за наложения сигналов при коллизии информация кадра исказится, и он будет отбракован принимающей станцией. Скорее всего, искаженная информация будет повторно передана каким-либо протоколом верхнего уровня, например транспортным или прикладным, работающим с установлением соединения. Но повторная передача сообщения протоколами верхних уровней произойдет через значительно более длительный интервал времени (иногда даже через несколько секунд) по сравнению с микросекундными интервалами, которыми оперирует протокол Ethernet. Поэтому если коллизии не будут надежно распознаваться узлами сети Ethernet, то это приведет к заметному снижению полезной пропускной способности данной сети.

Для надежного распознавания коллизий должно выполняться следующее соотношение:

$$T_{min} \geq PDV,$$

где T_{min} – время передачи кадра минимальной длины, а PDV – время, за которое сигнал коллизии успевает распространиться до самого дальнего узла сети. Так как в худшем случае сигнал должен пройти дважды между наиболее удаленными друг от друга станциями сети (в одну сторону проходит неискаженный сигнал, а на обратном пути распространяется уже искаженный коллизией сигнал), то это время называется *временем двойного оборота (Path Delay Value, PDV)*. При выполнении этого условия передающая станция должна успевать обнаружить коллизию, которую вызвал переданный ею кадр, еще до того, как она закончит передачу этого кадра.

В стандарте Ethernet принято, что минимальная длина поля данных кадра составляет 46 байт (что вместе со служебными полями дает минимальную длину кадра 64 байт, а вместе с преамбулой – 72 байт или 576 бит). В 10-мегабитном Ethernet время передачи кадра минимальной длины равно 575 битовых интервалов, следовательно, время двойного оборота должно быть меньше 57,5 мкс.

Стандарты 10Base-5 и 10Base-2 на основе коаксиального кабеля в настоящее время почти не применяются. Наибольшее распространение в последние годы получили стандарты 10Base-T и 10Base-F.

Стандарт 10Base-T принят в 1991 году как дополнение к существующему набору стандартов Ethernet, и имеет обозначение 802.3i. Сети 10Base-T используют в качестве среды передачи данных две неэкранированные витые пары (UTP). Конечные узлы соединяются по топологии «точка-точка» со специальным устройством – многопортовым повторителем (концентратором) с помощью двух витых пар. Одна витая пара требуется для передачи данных от станции к повторителю, а другая – для передачи данных от повторителя к станции. Концентратор принимает сигналы от одного из конечных узлов и синхронно передает их на все свои остальные порты, кроме того, с которого поступили сигналы. Концентратор осуществляет функции повторителя сигналов на всех отрезках витых пар, подключенных к его портам, так что образуется единая среда передачи данных (логическая общая шина). Стандарт определяет битовую скорость передачи данных 10 Мбит/с и максимальное расстояние отрезка витой пары между двумя непосредственно связанными узлами (станциями и концентраторами) не более 100 м.

Концентраторы 10Base-T можно соединять друг с другом с помощью тех же портов, которые предназначены для подключения конечных узлов. Для обеспечения синхронизации станций при реализации процедур доступа CSMA/CD и надежного распознавания станциями коллизий в стандарте определено максимальное число концентраторов между любыми двумя станциями сети, а именно 4. Это правило носит название «правила четырех хабов». При создании сети 10Base-T с большим числом станций концентраторы можно соединять друг с другом иерархическим способом, образуя древовидную структуру (рис.9.2).

Примечание. Технология Ethernet основана на использовании единой разделяемой среды передачи данных (логическая общая шина). Даже, если использовать концентраторы для образования звездообразной или древовидной структуры (рис. 9.2) физической топологии сети, все равно такая сеть будет соответствовать логической общей шине. Это связано с тем, что все порты кон-

центратора электрически соединены и сигналы, поступающие на один из портов, передаются автоматически на все порты. Поэтому сеть, изображенная на рис. 9.2, представляет собой единую разделяемую среду (единый домен коллизий). Для логической структуризации сети (деления единой сети на несколько сетей) используются мосты, коммутаторы и маршрутизаторы.

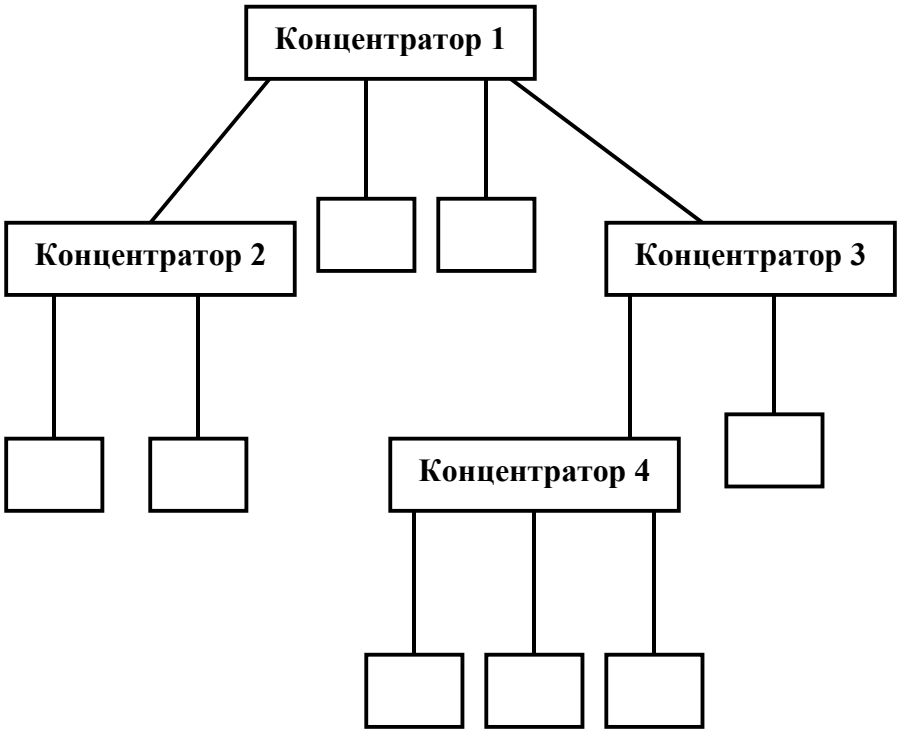


Рис. 9.2. Древовидная структура сети Ethernet

Максимальная длина сети понимается как максимальное расстояние между любыми двумя конечными узлами сети (часто применяется также термин «максимальный диаметр сети»). Очевидно, что если между любыми двумя узлами сети не должно быть больше 4-х повторителей, то максимальный диаметр сети 10Base-T составляет 5x100 = 500 м. Сети, построенные на основе стандарта 10Base-T, обладают по сравнению с коаксиальными вариантами Ethernet многими преимуществами. Эти преимущества связаны с разделением общего физического кабеля на отдельные кабельные отрезки, подключенные к центральному коммуникационному устройству. И хотя логически эти отрезки попрежнему образуют общую разделяемую среду, их физическое разделение позволяет индивидуально контролировать их состояние и отключать в случае обрыва, короткого замыкания или не-

исправности сетевого адаптера. Это обстоятельство существенно облегчает эксплуатацию больших сетей Ethernet, так как концентратор обычно автоматически выполняет такие функции, уведомляя при этом администратора сети о возникшей проблеме.

Стандарт 10Base-F в качестве среды передачи данных использует оптическое волокно. Функционально сеть Ethernet на оптическом кабеле состоит из тех же элементов, что и сеть стандарта 10Base-T – сетевых адаптеров, многопортового повторителя и отрезков кабеля, соединяющих адаптер с портом повторителя. Максимальное расстояние между узлом и концентратором увеличилось до 2000 м, а максимальное расстояние между станциями (длина сети) – до 2500 м.

9.3. Технология Fast Ethernet

Технология Fast Ethernet является эволюционным развитием классической технологии Ethernet и официально утверждена в 1995 году. Ее основными достоинствами являются:

– увеличение пропускной способности сегментов сети до 100 Мбит/с;

– сохранение метода случайного доступа Ethernet;

– сохранение звездообразной топологии сетей и поддержка традиционных сред передачи данных – витой пары и оптоволоконного кабеля.

Указанные свойства позволяют осуществлять постепенный переход от сетей 10Base-T – наиболее популярного на сегодняшний день варианта Ethernet – к скоростным сетям, сохраняющим значительную преемственность с хорошо знакомой технологией. Fast Ethernet не требует коренного переобучения персонала и замены оборудования во всех узлах сети.

Отличия Fast Ethernet от Ethernet сосредоточены на физическом уровне. Форматы кадров технологии Fast Ethernet не отличаются от форматов кадров технологий простого Ethernet. Все времена передачи кадров Fast Ethernet в 10 раз меньше соответствующих времен технологии простого Ethernet.

Для технологии Fast Ethernet разработаны различные варианты физического уровня, отличающиеся не только типом кабеля и

электрическими параметрами импульсов, но и способом кодирования сигналов и количеством используемых в кабеле проводников. Поэтому физический уровень Fast Ethernet имеет более сложную структуру, чем классический Ethernet. Физический уровень состоит из трех подуровней (рис.9.3):

– уровень согласования (reconciliation sublayer);

– независимый от среды интерфейс (MII – Media Independent Interface);

– устройство физического уровня (PHY – Physical Layer Device).

Устройство физического уровня PHY обеспечивает кодирование данных, поступающих от MAC-подуровня для передачи их по кабелю определенного типа, синхронизацию передаваемых по кабелю данных, а также прием и декодирование данных в узле-приемнике. Интерфейс MII поддерживает независимый от используемой физической среды способ обмена данными между MAC-подуровнем и подуровнем PHY. Этот интерфейс аналогичен по назначению интерфейсу классического Ethernet. Подуровень согласования нужен для того, чтобы согласовать работу подуровня MAC с интерфейсом MII.

В классическом Ethernet для любых вариантов кабеля использовался одинаковый метод физического кодирования – манчестерский код, а в стандарте Fast Ethernet используются три – FX, TX и T4. Официальный стандарт 802.3u установил три различных спецификации для физического уровня Fast Ethernet:

– 100Base-TX для двухпарного кабеля на неэкранированной витой паре UTP категории 5 или экранированной витой паре STP;

– 100Base-T4 для четырехпарного кабеля на неэкранированной витой паре UTP категории 3, 4 или 5;

– 100Base-FX для многомодового оптоволоконного кабеля, используются два волокна.

Спецификация 100Base-FX определяет работу протокола Fast Ethernet по многомодовому оптоволокну в полудуплексном и полнодуплексном режимах. В качестве среды передачи данных спецификация 100Base-TX использует кабель UTP категории 5 или кабель STP Type 1. Максимальная длина кабеля в обоих случаях – 100 м. Спецификация 100Base-T4 была разработана для того, чтобы можно было использовать для высокоскоростного

Ethernet имеющуюся проводку на витой паре категории 3 или 5. Эта спецификация позволяет повысить общую пропускную способность за счет одновременной передачи потоков бит по всем 4 парам кабеля. Максимальная длина сегмента для витой пары остается равной 100 м.

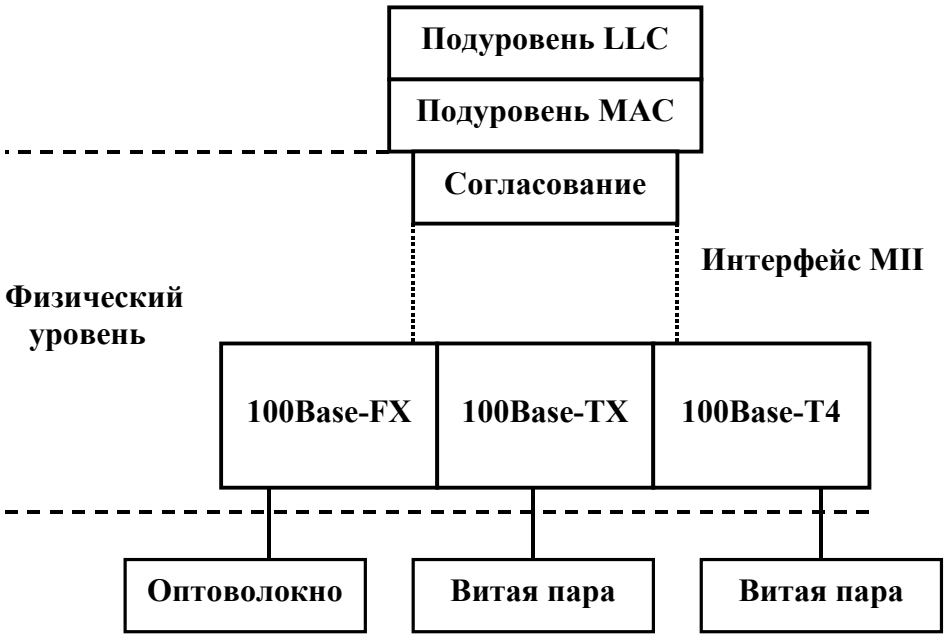


Рис. 9.3. Структура уровней стека протоколов технологии Fast Ethernet

Технология Fast Ethernet при работе на витой паре позволяет за счет процедуры автопереговоров, реализуемой на физическом уровне, двум портам выбирать наиболее эффективный режим работы – скорость 10 Мбит/с или 100 Мбит/с, а также полудуплексный или полнодуплексный режим.

9.4. Технология 100VG-AnyLAN

В качестве альтернативы технологии Fast Ethernet, фирмы AT&T и HP выдвинули проект новой технологии со скоростью передачи данных 100 Мбит/с – 100 Base-VG. В этом проекте было предложено усовершенствовать метод доступа с учетом потребности мультимедийных приложений и при этом сохранить совместимость формата пакета с форматом пакета сетей 802.3. В сентябре 1993 г. по инициативе фирм IBM и HP был образован

комитет IEEE 802.12, который занялся стандартизацией новой технологии. Проект был расширен за счет поддержки в одной сети кадров не только формата Ethernet, но и формата Token Ring. В результате новая технология получила название 100VG-AnyLAN, т. е. технология для любых сетей (Any LAN – любые сети), имея в виду, что в локальных сетях технологии Ethernet и Token Ring используются в подавляющем количестве узлов. В 1995 г. технология 100VG-AnyLAN получила статус стандарта IEEE 802.12.

В технологии 100VG-AnyLAN определены новый метод доступа Demand Priority и новая схема квартетного кодирования Quartet Coding, использующая избыточный код 5B/6B.

Метод доступа Demand Priority основан на передаче концентратору функций арбитра, решающего проблему доступа к разделяемой среде. Метод Demand Priority повышает пропускную способность сети за счет введения детерминированного доступа к общей среде, использующего два уровня приоритетов: низкий – для обычных приложений и высокий – для мультимедийных.

Сеть 100VG-AnyLAN всегда включает центральный концентратор, называемый концентратором уровня 1 или корневым концентратором. Корневой концентратор имеет связи с каждым узлом сети, образуя топологию «звезда». Он представляет собой интеллектуальный центральный контроллер, который управляет доступом к сети, постоянно выполняя цикл кругового сканирования своих портов и проверяя наличие запросов на передачу кадров от присоединенных к ним узлов. Концентратор принимает кадр от узла, выдавшего запрос, и передает его только через тот порт, к которому присоединен узел с адресом, совпадающим с адресом назначения, указанным в кадре.

Метод Demand Priority (приоритетный доступ по требованию) основан на том, что узел, которому нужно передать кадр по сети, передает запрос (требование) на выполнение этой операции концентратору. Каждый запрос может иметь либо низкий, либо высокий приоритеты. Высокий приоритет отводиться для трафика чувствительных к задержкам мультимедийных приложений.

Высокоприоритетные запросы всегда обслуживаются раньше низкоприоритетных. Требуемый уровень приоритета кадра устанавливается протоколами верхних уровней, не входящими в технологию 100VG-AnyLAN и передается для отработки уровню

MAC. Концентратор уровня 1 постоянно сканирует запросы узлов, используя алгоритм кругового опроса. Это сканирование позволяет концентратору определить, какие узлы требуют передачи кадров через сеть и каковы их приоритеты.

В течение одного цикла кругового сканирования каждому узлу разрешается передать один кадр данных через сеть. Концентраторы, присоединенные как узлы к концентраторам верхних уровней иерархии, также выполняют свои циклы сканирования и передают запрос на передачу кадров концентратору. Концентратор нижнего уровня с *N* портами имеет право передать *N* кадров в течение одного цикла опроса. Каждый концентратор ведет отдельные очереди для низкоприоритетных и высокоприоритетных запросов. Низкоприоритетные запросы обслуживаются только до тех пор, пока не получен высокоприоритетный запрос. В этом случае текущая передача низкоприоритетного кадра завершается и обрабатывается высокоприоритетный запрос. Перед возвратом к обслуживанию низкоприоритетных кадров должны быть обслужены все высокоприоритетные запросы. Чтобы гарантировать доступ для низкоприоритетных запросов в периоды высокой интенсивности поступления высокоприоритетных запросов, вводится порог ожидания запроса. Если у какого-либо низкоприоритетного запроса время ожидания превышает этот порог, то ему присваивается высокий приоритет.

Операции передачи данных на 4-парном кабеле используют как полнодуплексный, так и полудуплексный режимы. Полнодуплексные операции применяют для одновременной передачи в двух направлениях (от узла к концентратору и от концентратора к узлу) сигнальной информации о состоянии линии. Полудуплексные операции используются для передачи данных от концентратора узлу и от узла концентратору по всем четырем парам.

9.5. Технология Gigabit Ethernet

Основная идея разработчиков стандарта Gigabit Ethernet состояла в максимальном сохранении идей классической технологии Ethernet при достижении битовой скорости в 1000 Мбит/с. Стандарт был принят в 1998 году на заседании комитета IEEE 802.3.

В технологии Gigabit Ethernet:

– сохраняются все форматы кадров Ethernet;

– сохраняется полудуплексная версия протокола, поддерживающая метод доступа CSMA/CD, и полнодуплексная версия, работающая с коммутаторами;

– поддерживаются все основные виды кабелей, используемых в Ethernet и Fast Ethernet: волоконно-оптический, витая пара категории 5 и коаксиальный кабель.

Для передачи по витой паре категории 5 данных со скоростью 1000 Мбит/с организуется параллельная передача одновременно по всем 4 парам кабеля (так же, как и в технологии 100VG-AnyLAN) с использованием специального метода кодирования. Подуровень MAC стандарта Gigabit Ethernet использует тот же самый протокол передачи CSMA/CD, что и Ethernet и Fast Ethernet. Основные ограничения на максимальную длину сегмента (или коллизионного домена) определяются этим протоколом.

Технология Gigabit Ethernet позволяет эффективно строить крупные локальные сети, в которых мощные серверы и магистрали нижних уровней сети работают на скорости 100 Мбит/с, а магистраль Gigabit Ethernet объединяет их, обеспечивая достаточно большой запас пропускной способности.

9.6. Технология Token Ring

Сеть Token Ring разработана компанией IBM в 1984 г. Она по-прежнему является основной технологией IBM для локальных сетей. Фактически по образцу Token Ring IBM была создана спецификация IEEE 802.5, которая почти идентична и полностью совместима с сетью Token Ring. В сети Token Ring кольцо образуется отрезками кабеля, соединяющими соседние станции. Таким образом, каждая станция связана со своей предшествующей и последующей станцией и может непосредственно обмениваться данными только с ними. В сети Token Ring любая станция всегда непосредственно получает данные только от одной станции – той, которая является предыдущей в кольце. Передачу же данных станция всегда осуществляет своему ближайшему соседу вниз по потоку данных. Переданные данные проходят по кольцу всегда в одном направлении от одной станции к другой.

Сети Token Ring и IEEE 802.5 являются примерами сетей с передачей маркера. Сети с передачей маркера перемещают вдоль сети небольшой блок данных, называемый маркером. Владение этим маркером гарантирует право передачи. Если узел, принимающий маркер, не имеет информации для отправки, он просто переправляет маркер к следующей станции. Каждая станция может удерживать маркер в течение определенного времени, после истечения которого станция обязана прекратить передачу собственных данных (текущий кадр разрешается завершить) и передать маркер далее по кольцу. Станция может успеть передать за время удержания маркера один или несколько кадров в зависимости от размера кадров и величины времени удержания маркера.

Если у станции, владеющей маркером, есть информация для передачи, она захватывает маркер, изменяет у него один бит (в результате чего маркер превращается в последовательность «начало блока данных»), дополняет информацией, которую он хочет передать и, наконец, отсылает эту информацию к следующей станции кольцевой сети. Когда информационный блок циркулирует по кольцу, маркер в сети отсутствует, поэтому другие станции, желающие передать информацию, вынуждены ожидать. Следовательно, в сетях Token Ring не может быть коллизий. Если обеспечивается раннее высвобождение маркера, то новый маркер может быть выпущен после завершения передачи блока данных.

Информационный блок циркулирует по кольцу, пока не достигнет предполагаемой станции назначения, которая копирует информацию для дальнейшей обработки. Информационный блок продолжает циркулировать по кольцу; он удаляется после достижения станции, отославшей этот блок. Станция отправки может проверить вернувшийся блок, чтобы убедиться, что он был просмотрен и затем скопирован станцией назначения.

В отличие от сетей CSMA/CD (например, Ethernet) сети с передачей маркера являются сетями с детерминированным методом доступа. Это означает, что можно вычислить максимальное время, которое пройдет, прежде чем любая конечная станция сможет передавать. Это предсказуемое значение максимального времени делает сеть Token Ring идеальной для применений, где задержка должна быть известна и важна устойчивость функционирования сети.

Технология Token Ring обеспечивает скорости передачи 4 Мбит/с или 16 Мбит/с. В сетях Token Ring со скоростью передачи 16 Мбит/с используется алгоритм доступа к кольцу, называемый алгоритмом раннего освобождения маркера (Early Token Release). В соответствии с ним станция передает маркер доступа следующей станции сразу же после окончания передачи последнего бита кадра, не дожидаясь возвращения по кольцу этого кадра с битом подтверждения приема. В этом случае пропускная способность кольца используется более эффективно и приближается к 80% от номинальной. Время удержания одной станцией маркера ограничивается тайм-аутом, после истечения которого станция обязана передать маркер далее по кольцу.

Стандарт Token Ring фирмы IBM изначально предусматривал построение связей в сети с помощью концентраторов. Сеть Token Ring может включать до 260 узлов. Концентратор Token Ring может быть активным или пассивным. Пассивный концентратор просто соединяет порты внутренними связями так, чтобы станции, подключаемые к этим портам, образовали кольцо. Активный концентратор выполняет функции регенерации сигналов и поэтому иногда называется повторителем, как в стандарте Ethernet. В общем случае сеть Token Ring имеет комбинированную звездно-кольцевую конфигурацию. Конечные узлы подключаются к концентратору по топологии звезды, а сами концентраторы объединяются через специальные порты Ring In (RI) и Ring Out (RO) для образования магистрального физического кольца. Физическая конфигурация сети Token Ring изображена на рисунке 9.4.

Все станции в кольце должны работать на одной скорости – либо 4 Мбит/с, либо 16 Мбит/с. Кабели, соединяющие станцию с концентратором, называются ответвительными, а кабели, соединяющие концентраторы, – магистральными.

Технология Token Ring позволяет использовать для соединения конечных станций и концентраторов различные типы кабеля: экранированную и неэкранированную витую пару (STP Type 1, UTP Type 3, UTP Type 6), а также волоконно-оптический кабель. При использовании экранированной витой пары STP Type 1 из номенклатуры кабельной системы IBM в кольцо допускается объединять до 260 станций при длине ответвительных кабелей до 100 метров, а при использовании неэкранированной витой пары

максимальное количество станций сокращается до 72 при длине ответвительных кабелей до 45 метров.

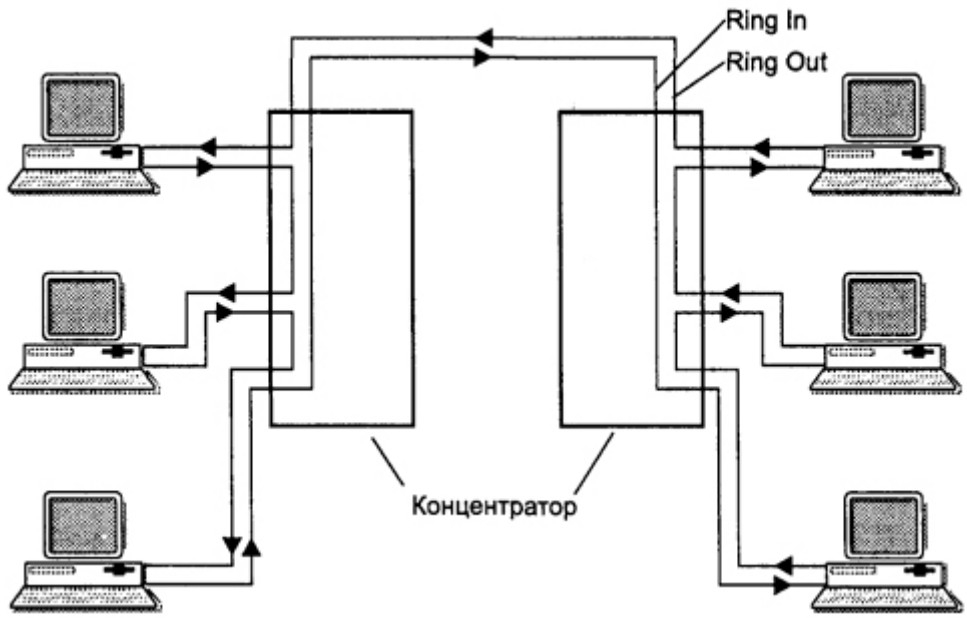


Рис. 9.4. Физическая конфигурация сети Token Ring

Расстояние между пассивными концентраторами может достигать 100 м при использовании кабеля STP Type 1 и 45 м при использовании кабеля UTP Type 3. Между активными концентраторами максимальное расстояние увеличивается соответственно до 730 м или 365 м в зависимости от типа кабеля. Максимальная длина кольца Token Ring составляет 4000 м.

Технология Token Ring является более сложной технологией, чем Ethernet. Она обладает свойствами отказоустойчивости. В сети Token Ring определены процедуры контроля работы сети, которые используют обратную связь кольцеобразной структуры – посланный кадр всегда возвращается в станцию-отправитель. В некоторых случаях обнаруженные ошибки в работе сети устраняются автоматически, например может быть восстановлен потерянный маркер.

Для контроля сети одна из станций выполняет роль так называемого *активного монитора*. Активный монитор выбирается во время инициализации кольца как станция с максимальным значением MAC-адреса. Если активный монитор выходит из строя, процедура инициализации кольца повторяется и выбирается новый активный монитор. Чтобы сеть могла обнаружить отказ ак-

тивного монитора, последний в работоспособном состоянии каждые 3 секунды генерирует специальный кадр своего присутствия. Если этот кадр не появляется в сети более 7 секунд, то остальные станции сети начинают процедуру выборов нового активного монитора.

9.7. Технология FDDI

Технология *FDDI* (Fiber Distributed Data Interface) – оптоволоконный интерфейс распределенных данных – это первая технология локальных сетей, в которой средой передачи данных является волоконно-оптический кабель. В 1988 году разработана начальная версия стандарта FDDI, который обеспечивает передачу кадров со скоростью 100 Мбит/с по двойному волоконно-оптическому кольцу длиной до 100 км.

Сеть FDDI строится на основе двух оптоволоконных колец, образующих основной и резервный пути передачи данных между узлами сети. Использование двух колец – это основной способ повышения отказоустойчивости в сети FDDI. Узлы сети подключаются к обоим кольцам. В нормальном режиме работы сети данные проходят через все узлы и все участки кабеля первичного (Primary) кольца, поэтому этот режим назван режимом Thru – «сквозным» или «транзитным». Вторичное кольцо (Secondary) в этом режиме не используется.

В случае какого-либо вида отказа, когда часть первичного кольца не может передавать данные (например, обрыв кабеля или отказ узла), первичное кольцо объединяется с вторичным (рис. 9.5), образуя вновь единое кольцо. Этот режим работы сети называется *Wrap*, т. е. «свертывание» или «сворачивание» колец. Операция свертывания проводится концентраторами и/или сетевыми адаптерами FDDI. Для упрощения этой операции данные по первичному кольцу всегда передаются против часовой стрелки, а по вторичному – по часовой. Поэтому при образовании общего кольца из двух колец передатчики станций по-прежнему остаются подключенными к приемникам соседних станций, что позволяет правильно передавать и принимать информацию соседними станциями.

Рис. 9.5. Свертывание колец

В стандартах FDDI отводится много внимания различным процедурам, позволяющим определить наличие отказа в сети и провести необходимую реконфигурацию. Сеть FDDI может полностью восстанавливать свою работоспособность в случае единичных отказов ее элементов. При множественных отказах сеть распадается на несколько несвязанных сетей.

Кольца в сетях FDDI рассматриваются как общая разделяемая среда передачи данных, поэтому для нее определен специальный метод доступа. Этот метод очень близок к методу доступа сетей Token Ring и также называется методом маркерного кольца – token ring. Отличия метода доступа в сетях FDDI заключаются в том, что время удержания маркера не является постоянной величиной, как в сети Token Ring. Это время зависит от загрузки кольца: при небольшой загрузке оно увеличивается, а при больших перегрузках может уменьшиться до нуля.

В качестве физической среды технология FDDI может использовать кроме волоконно-оптического кабеля и кабель UTP категории 5 (этот вариант физического уровня называется TP-PMD).

Максимальная общая длина кольца FDDI составляет 100 километров, максимальное число станций с двойным подключением в кольце – 500. Максимальные расстояния между соседними узлами для многомодового кабеля равны 2 км, для витой пары

UPT категории 5 – 100 м, а для одномодового оптоволокна зависят от его качества.

Технология FDDI разрабатывалась для применения в ответственных участках сетей – на магистральных соединениях между крупными сетями, например сетями зданий, а также для подключения к сети высокопроизводительных серверов. Поэтому главным для разработчиков было обеспечить высокую скорость передачи данных, отказоустойчивость на уровне протокола и большие расстояния между узлами сети. Все эти цели были достигнуты. В результате технология FDDI получилась качественной, но весьма дорогой. Даже появление более дешевого варианта для витой пары не намного снизило стоимость подключения одного узла к сети FDDI. Поэтому практика показала, что основной областью применения технологии FDDI стали магистрали сетей, состоящих из нескольких зданий, а также сети масштаба крупного города, то есть класса MAN. Для подключения клиентских компьютеров и даже небольших серверов технология оказалась слишком дорогой.

9.8. Структуризация локальных сетей

При построении сетей с небольшим количеством станций, как правило, используется одна из типовых физических топологий. Многие организации имеют по нескольку локальных сетей (иногда построенных на базе различных сетевых технологий), которые необходимо объединить между собой. Причин этому может быть несколько.

Во-первых, например, если взять высшее учебное заведение, то в соответствии с задачами логично организовать сети на каждом факультете, а также в некоторых отделах, например бухгалтерия, ректорат и т.п. Эти сети могут объединять рабочие станции, общие принтеры и свои сервера. Однако рано или поздно возникает задача их взаимодействия, например обращение к единой базе данных системы управления или пересылки почты.

Во-вторых, факультеты могут располагаться в разных зданиях. Может оказаться дешевле создать несколько локальных сетей и объединить их, например, с помощью лазерных линий связи. Кроме того, расстояния между станциями могут быть недопустимо большими для построения одной локальной сети.

В-третьих, иногда бывает более эффективным логически разделить одну большую локальную сеть, состоящую из сотен станций, на несколько малых сетей, чтобы снизить нагрузку на каналы связи и увеличить пропускную способность.

В-четвертых, несколько объединенных сетей надежнее, чем единая локальная сеть с точки зрения технической эксплуатации. Например, если какой-либо компьютер сети Ethernet с физической общей шиной из-за сбоя начинает непрерывно передавать данные по общему кабелю, то вся сеть выходит из строя. Если сеть Ethernet построена с использованием концентратора, то он в таких случаях может автоматически отключить свой порт, выполняя функцию некоторого управляющего узла.

В-пятых, в таких сетях можно эффективнее построить систему безопасности. Каждую локальную сеть можно защитить от утечки информации и от вторжения извне.

Для объединения (или разделения) локальных сетей используются различные методы структуризации сетей. На практике различают физическую структуру сети (топологию физических связей) и логическую структуру (топологию логических связей, определяющих маршруты передачи информации в сети).

Физическая структуризация сети осуществляется с помощью повторителей и концентраторов, позволяющих не только увеличить расстояния между узлами сети, но и повысить ее надежность.

Физическая структуризация сети полезна во многих отношениях, однако в ряде случаев, обычно относящихся к сетям большого и среднего размера, невозможно обойтись без логической структуризации сети. Наиболее важной проблемой, не решаемой путем физической структуризации, остается проблема перераспределения передаваемого трафика между различными физическими сегментами сети. В большой сети естественным образом возникает неоднородность информационных потоков. Сеть с типовой топологией (шина, кольцо, звезда), в которой все физические сегменты рассматриваются в качестве одной разделяемой среды, оказывается неадекватной структуре информационных потоков в большой сети. Например, в сети с общей шиной взаимодействие любой пары компьютеров занимает ее на все время обмена, поэтому при увеличении числа компьютеров в сети шина

становится узким местом. Компьютеры одной рабочей группы (отдела) вынуждены ждать, когда окончит обмен пара компьютеров другого отдела, тогда как необходимость в связи между компьютерами двух разных отделов возникает гораздо реже и требует совсем небольшой пропускной способности.

Таким образом, встает задача локализации сетевого трафика в пределах сегментов сети. Решение этой задачи заключается в логической структуризации сети – разбиение ее на логические сегменты (подсети) с локализованным трафиком. Каждый логический сегмент представляет собой самостоятельную разделяемую среду передачи данных. Крупные сети практически никогда не строятся без логической структуризации. Разделение сети на логические сегменты и организация взаимодействия между этими сегментами осуществляется с помощью следующих коммуникационных устройств: мосты, коммутаторы, маршрутизаторы и шлюзы.

Мост (bridge) делит разделяемую среду передачи сети на части (подсети, логические сегменты), передавая информацию из одного сегмента в другой только в том случае, если такая передача действительно необходима, то есть если адрес компьютера назначения принадлежит другой подсети. Тем самым мост изолирует трафик одной подсети от трафика другой, повышая общую производительность передачи данных в сети. Локализация трафика не только экономит пропускную способность, но и уменьшает возможность несанкционированного доступа к данным, так как кадры не выходят за пределы своего сегмента и их сложнее перехватить злоумышленнику.

Мосты используют для локализации трафика аппаратные адреса компьютеров. Это затрудняет распознавание принадлежности того или иного компьютера к определенному логическому сегменту. Поэтому мост достаточно упрощенно представляет деление сети на сегменты. Он запоминает, через какой порт на него поступил кадр данных от каждого компьютера сети, и в дальнейшем передает кадры, предназначенные для этого компьютера, на этот порт. Точной топологии связей между логическими сегментами мост не знает.

Коммутатор (switch) по принципу обработки кадров ничем не отличается от моста. Основное его отличие от моста состоит в

том, что он является своего рода коммуникационным мультипроцессором, так как каждый его порт оснащен специализированным процессором, который обрабатывает кадры независимо от процессоров других портов. За счет этого общая производительность коммутатора обычно намного выше производительности традиционного моста, имеющего один процессорный блок.

Маршрутизатор (router) более надежно и более эффективно, чем мост, изолирует трафик отдельных частей сети друг от друга. Маршрутизаторы образуют логические сегменты посредством явной адресации, поскольку используют не плоские аппаратные, а составные числовые адреса. В этих адресах имеется поле номера сети, так что все компьютеры, у которых значение этого поля одинаково, принадлежат к одному сегменту (подсети). Кроме локализации трафика маршрутизаторы выполняют еще много других полезных функций, например, выбор наиболее рационального маршрута из нескольких возможных. Другой очень важной функцией маршрутизаторов является их способность связывать в единую сеть подсети, построенные с использованием разных сетевых технологий.

Кроме перечисленных устройств отдельные части сети может соединять **шлюз** (gateway). Обычно основной причиной, по которой в сети используют шлюз, является необходимость объединить сети с разными типами системного и прикладного программного обеспечения.

Все перечисленные устройства при использовании в сетях порой выполняют сходные функции, а иногда их роли существенно различаются. Принципиальное отличие заключается в том, что они используются на разных уровнях модели передачи данных и оперируют с разными единицами информации (рис. 9.6).

Типичный сценарий передачи данных таков: у пользователя появляются какие-то данные, которые необходимо отправить на удаленную машину. Они передаются на транспортный уровень, который добавляет к ним свой заголовок (например, заголовок TCP) и передает результирующую единицу информации на сетевой уровень. Тот, в свою очередь, тоже добавляет свой заголовок, в результате чего формируется пакет сетевого уровня (например, IP-пакет). Пакет отправляется на уровень передачи данных (канальный уровень), где обрастает еще одним заголовком и форми-

руется кадр, который спускается на физический уровень и может быть передан по локальной сети.

Рис. 9.6. Соответствие коммуникационных устройств уровням модели OSI

На самом нижнем, физическом уровне работают повторители. Это аналоговые устройства, к которым подсоединяются концы двух сегментов кабеля. Сигнал, появляющийся на одном из них, усиливается повторителем и выдается на второй. Повторители не знают слов «пакет», «кадр» или «заголовок». Они знают слово «напряжение». В классическом Ethernet допускается установка четырех повторителей, что позволяет расширять максимальную длину кабеля с 500 до 2500 м.

Теперь обратимся к концентраторам. Концентратор (хаб) имеет несколько входов, объединяемых электрически. Кадры, прибывающие на какой-либо вход, передаются на все остальные линии. Если одновременно по разным линиям придут два кадра, они столкнутся, как в коаксиальном кабеле. То есть концентратор представляет собой одну область столкновений. Все линии, подсоединяемые к нему, образуют один домен коллизий. Концентраторы отличаются от повторителей тем, что они обычно не усиливают входные сигналы. Их задача заключается в обеспечении согласованной работы нескольких линий с похожими параметрами. Впрочем, во всем остальном хабы не очень отличаются от повторителей. Ни те, ни другие не анализируют и не используют адреса стандарта 802. Принцип работы концентратора показан на рис. 9.7.

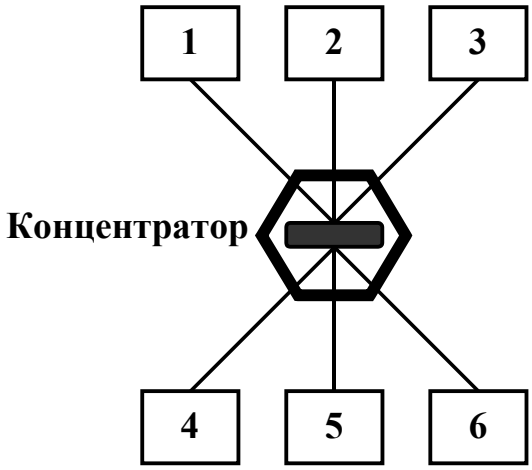


Рис. 9.7. Принцип работы концентратора

Перейдем теперь на уровень передачи данных (канальный). Здесь работают мосты и коммутаторы. Мост соединяет две или более ЛВС, как показано на рис. 9.8. Когда прибывает кадр, мост программно извлекает из заголовка и анализирует адрес назначения, сопоставляя его с таблицей и определяя, куда этот кадр должен быть передан. Мост может иметь несколько плат (портов), благодаря чему может работать с сетями разных типов. Каждая линия, подключенная к мосту, является областью столкновений, в отличие от линий концентратора.

Коммутаторы похожи на мосты в том, что для маршрутизации используют адреса кадров. На самом деле многие употребляют эти понятия как синонимы. Различаются они тем, что коммутаторы чаще всего используются для соединения отдельных компьютеров (рис. 9.9), а не сетей. Следовательно, если хост 1 (рис. 9.8) отправит кадр на хост 2, мост получит этот кадр, но отвергнет его. Вместе с тем, коммутатор на рис. 9.9 должен самым активным образом способствовать передаче кадра от хоста 1 к хосту 2. Так как каждый порт коммутатора обычно соединен с одним компьютером, в коммутаторах должно быть гораздо больше разъемов для сетевых плат, чем в мостах, поскольку последние соединяют целые сети. Каждый порт содержит буфер для хранения пришедших кадров. Поскольку каждый порт является областью столкновений, то кадры из-за коллизий теряться не могут. Однако если скорость передачи данных по каналу превысит максимальную скорость их обработки, буфер может переполниться и продолжающие приходить кадры, будут отвергаться.

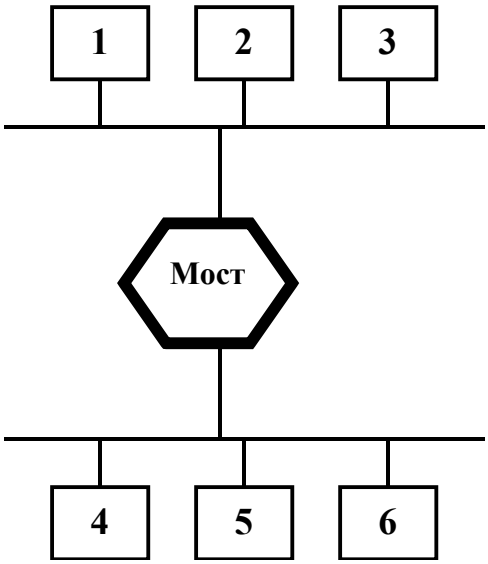


Рис. 9.8. Принцип работы моста

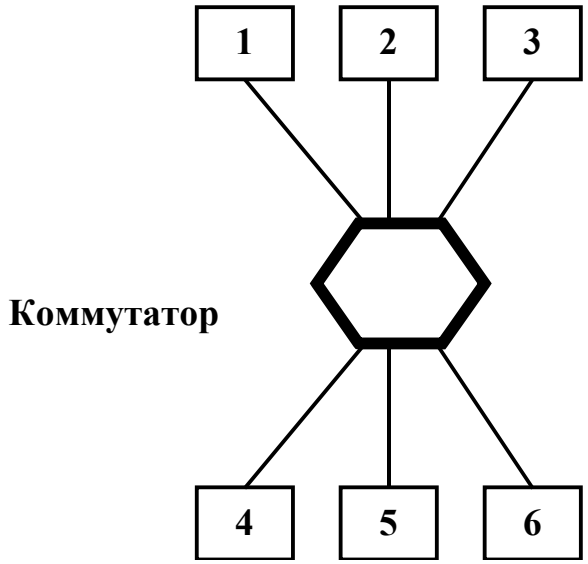


Рис. 9.9. Принцип работы коммутатора

Когда пакет прибывает на маршрутизатор, отрезаются заголовки и концевики кадров, которые и передаются программному обеспечению маршрутизатора. Далее анализируется заголовок пакета, и в соответствии с ним выбирается его дальнейший путь. Если это IP-пакет, то в заголовке будет содержаться 32-битный (IPv4) или 128-битный (IPv6) адрес. Программное обеспечение маршрутизатора не интересуется адресами кадров и даже не знает, откуда эти кадры взялись (то ли с ЛВС, то ли с двухточечной линии).

Поднявшись еще на уровень выше, мы обнаружим транспортные шлюзы. Они служат для соединения компьютеров, использующих различные транспортные протоколы, ориентированные на установление соединения. Например, такая ситуация возникает, когда компьютеру, использующему TCP/IP, необходимо передать данные компьютеру, использующему технологию ATM. Транспортный шлюз может копировать пакеты, одновременно приводя их к нужному формату.

Наконец, шлюзы приложений уже работают с форматами и содержимым пакетов, занимаясь переформатированием на более высоком уровне. Например, шлюз e-mail может переводить электронные письма в формат SMS-сообщений для мобильных телефонов.

9.9. Виртуальные локальные сети

Коммутаторы в сетях позволяют не только увеличивать пропускную способность, но и локализовать потоки информации и управлять ими на основе использования фильтров. Группа узлов сети, трафик которой изолирован от других узлов, называется виртуальной сетью (Virtual LAN, VLAN). Использование технологии виртуальных сетей дает возможность настройки сетей не по физическим связям, а логически. Это позволяет группировать пользователей сети не по принципу физического расположения компьютеров, а в соответствии со структурой организации, что позволяет увеличить степень защиты информации.

Допустим, что сотрудник переходит в другое помещение, не меняя принадлежность к отделу, либо наоборот меняет отдел, не переходя в другое помещение. Физическая смена структуры в этом случае заключается в перекоммутации кабеля в распределительном шкафу (подключение к другому коммутатору). Однако на практике это не всегда осуществимо. Технология виртуальных сетей позволяет это сделать программным способом без переключения кабеля рабочей станции.

Для связи виртуальных сетей в общую сеть требуется привлечение сетевого уровня. Он реализуется в отдельном маршрутизаторе, либо реализуется программным обеспечением коммутатора, который в этом случае является комбинированным устройством (коммутатором третьего уровня). При создании виртуальной сети производится группировка портов коммутатора – каждый порт приписывается к конкретной виртуальной сети. Это делается с помощью специальной программы, входящей в комплект коммутатора. Возможна также группировка на основе MAC-адресов.

Для создания системы, построенной на виртуальных ЛВС, сетевому администратору, прежде всего, нужно решить, сколько всего будет виртуальных сетей, какие компьютеры будут в них входить и как они будут называться. Зачастую виртуальные ЛВС называют в соответствии с цветами радуги, поскольку тогда сразу становятся понятнее и нагляднее цветные диаграммы, показывающие принадлежность пользователей виртуальным сетям. Скажем, пользователи «красной» сети будут изображены красным цветом, «синей» – синим, и т.д. Таким образом, на одном ри-

сунке можно отобразить физическую и логическую структуры одновременно.

В качестве примера рассмотрим четыре ЛВС, изображенные на рис. 9.10. Здесь шесть машин входят в виртуальную сеть **С** (Серая), а еще пять машин в виртуальную сеть **Б** (белая). Четыре физических сети объединены двумя мостами, М1 и М2. На рис. 9.11 показаны те же самые станции тех же самых виртуальных сетей, только здесь используются коммутаторы К1 и К2, к каждому порту которых подключено по одному компьютеру.

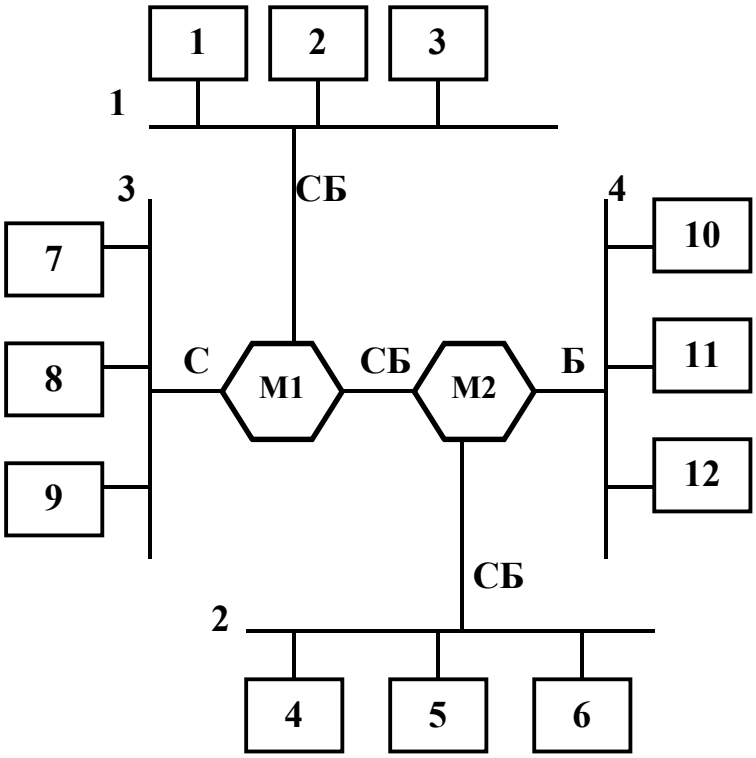


Рис. 9.10. Структуризация сети с помощью мостов

Чтобы виртуальные сети функционировали корректно, необходимо наличие конфигурационных таблиц в мостах или коммутаторах. Эти таблицы сообщают о том, через какие порты (каналы) производится доступ к тем или иным виртуальным сетям. Когда кадр прибывает, например, из серой виртуальной ЛВС, его нужно разослать на все порты, помеченные буквой **С**. Порт может быть помечен сразу несколькими буквами, то есть он может обслуживать несколько виртуальных ЛВС. Это видно на рис. 9.10.

Пусть у машины 1 имеется кадр для широковещательной передачи. Мост М1 принимает его и замечает, что он пришел с машины с пометкой **С**. Поэтому его необходимо ретранслировать

на все порты (кроме того, с которого пришел кадр), принадлежащих «серой» виртуальной сети. У М1 есть только два порта, кроме входящего, и оба помечены как **С**, поэтому кадр передается на оба из них.

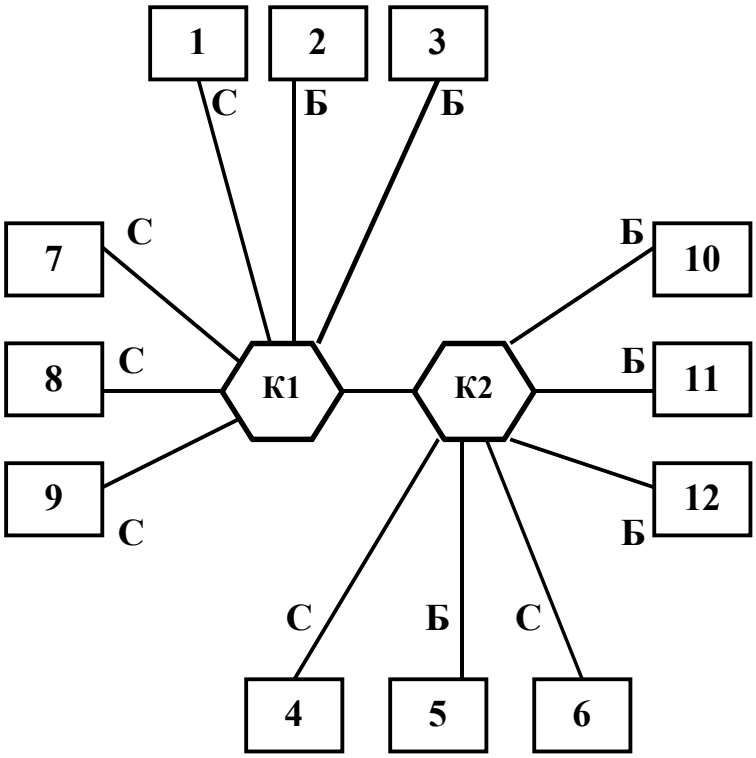


Рис. 9.11. Структуризация сети с помощью коммутаторов

С мостом М2 история несколько другая. Здесь мост знает, что в ЛВС 4 нет машин типа **С**, поэтому туда кадры не передаются вообще. Ретрансляция производится только в ЛВС 2. Если какой-нибудь пользователь ЛВС 4 перейдет на работу в другой отдел (без перемещения компьютера), а там будет сеть **С**, то таблицы моста М2 необходимо будет обновить и переобозначить порт **СБ** вместо **Б**. Если машина 5 уходит в серую сеть, то порт к ЛВС 2 надо будет переобозначить вместо **СБ** на **С**.

Допустим теперь, что все машины ЛВС 2 и ЛВС 4 стали серыми. Тогда не только порты М2, соединенные с ЛВС 2 и ЛВС 4, получат обозначение **С**, но и порт М1, соединенный с М2, превратится в **С**, поскольку «белые» кадры, приходящие на М1, больше не будут нуждаться в ретрансляции на мост М2. На рис. 9.11 изображена та же ситуация, только здесь все порты, соединенные с определенной машиной, отмечены только одним цветом, поскольку каждый компьютер может принадлежать только одной виртуальной ЛВС.

Мосты и коммутаторы узнают «цвет» приходящего кадра с помощью одного из следующих методов:

1. Каждому порту присваивается цвет.
2. Каждому MAC-адресу присваивается цвет.
3. Все IP-адреса соответствуют определенному цвету.

В первом методе каждый порт маркируется цветом какой-либо виртуальной ЛВС. Однако это работает только в том случае, если все машины порта принадлежат одной виртуальной сети. На рис. 9.10 этим свойством обладает порт ЛВС 3 моста M1, а порт ЛВС 1 уже не может применять метод маркировки портов.

При использовании второго метода мост или коммутатор имеет таблицу, в которой представлены 48-битные MAC-адреса и названия виртуальных сетей всех станций, соединенных с устройством. В этом случае можно смешивать виртуальные сети внутри физической сети, как это происходит с ЛВС 1 на рис. 9.10. Когда прибывает кадр, мосту или коммутатору необходимо лишь извлечь адрес MAC-уровня и найти его в таблице (это позволит понять, в какой виртуальной сети находится станция, с которой был отправлен кадр).

Третий метод заключается в том, что мост (коммутатор) просматривает поля данных кадров, чтобы с помощью IP-адреса идентифицировать конкретную машину. Такая стратегия особенно полезна, когда существенная часть станций представляет собой ноутбуки, которые могут подключаться в одном из нескольких мест. Поскольку у каждой из стыковочных станций есть свой MAC-адрес, то просто информация о том, какая стыковочная станция использовалась, ничего не скажет о том, в какой из виртуальных сетей находится сам ноутбук.

Контрольные вопросы к главе 9

1. Перечислите основные протоколы локальных сетей. Для каких целей введены стандарты на протоколы?
2. Опишите принципы основных протоколов локальных сетей.
3. Для чего необходима структуризация локальных сетей?
4. Чем отличается физическая структуризация от логической?
5. Какими коммуникационными устройствами осуществляется структуризация локальных сетей? Дайте основные характеристики таких устройств.
6. Что такое виртуальные локальные сети?

ГЛАВА 10

ТЕХНОЛОГИИ ГЛОБАЛЬНЫХ СЕТЕЙ

10.1. Основные понятия и определения

Глобальные сети (WAN), которые также называют территориальными компьютерными сетями, служат для того, чтобы предоставлять свои сервисы большому количеству конечных абонентов, разбросанных по большой территории – в пределах области, региона, страны, континента или всего земного шара. Типичными абонентами глобальной компьютерной сети являются локальные сети предприятий, расположенные в разных городах и странах, которым нужно обмениваться данными между собой. Услугами глобальных сетей пользуются также и отдельные компьютеры.

Глобальные сети обычно создаются крупными телекоммуникационными компаниями для оказания платных услуг абонентам. *Оператор сети* (network operator) – это та компания, которая поддерживает нормальную работу сети. *Поставщик услуг*, часто называемый также *провайдером* (service provider), – та компания, которая оказывает платные услуги абонентам сети. Владелец, оператор и поставщик услуг могут объединяться в одну компанию. Кроме вычислительных глобальных сетей существуют и другие виды территориальных сетей передачи информации. В первую очередь это телефонные и телеграфные сети, работающие на протяжении многих десятков лет, а также телексная сеть.

Ввиду большой стоимости глобальных сетей существует долговременная тенденция создания единой глобальной сети, которая может передавать данные любых типов: компьютерные данные, телефонные разговоры, факсы, телеграммы, телевизионное изображение и т.д. На сегодня существенного прогресса в этой области не достигнуто, хотя технологии для создания таких сетей начали разрабатываться достаточно давно. Первая технология

для интеграции телекоммуникационных услуг ISDN стала развиваться с начала 70-х годов. Пока каждый тип сети существует отдельно и наиболее тесная их интеграция достигнута в области использования общих первичных сетей – сетей PDH и SDH, с помощью которых сегодня создаются постоянные каналы в сетях с коммутацией абонентов. Тем не менее, каждая из технологий, как компьютерных сетей, так и телефонных, старается сегодня передавать «чужой» для нее трафик с максимальной эффективностью.

В идеале глобальная вычислительная сеть должна передавать данные абонентов любых типов. Для этого глобальная сеть должна предоставлять комплекс услуг: передачу пакетов локальных сетей, передачу пакетов компьютеров, обмен факсами, передачу трафика офисных АТС, выход в городские, междугородные и международные телефонные сети, обмен видеоизображениями и другие. Основные типы потенциальных потребителей услуг глобальной компьютерной сети изображены на рис. 10.1.

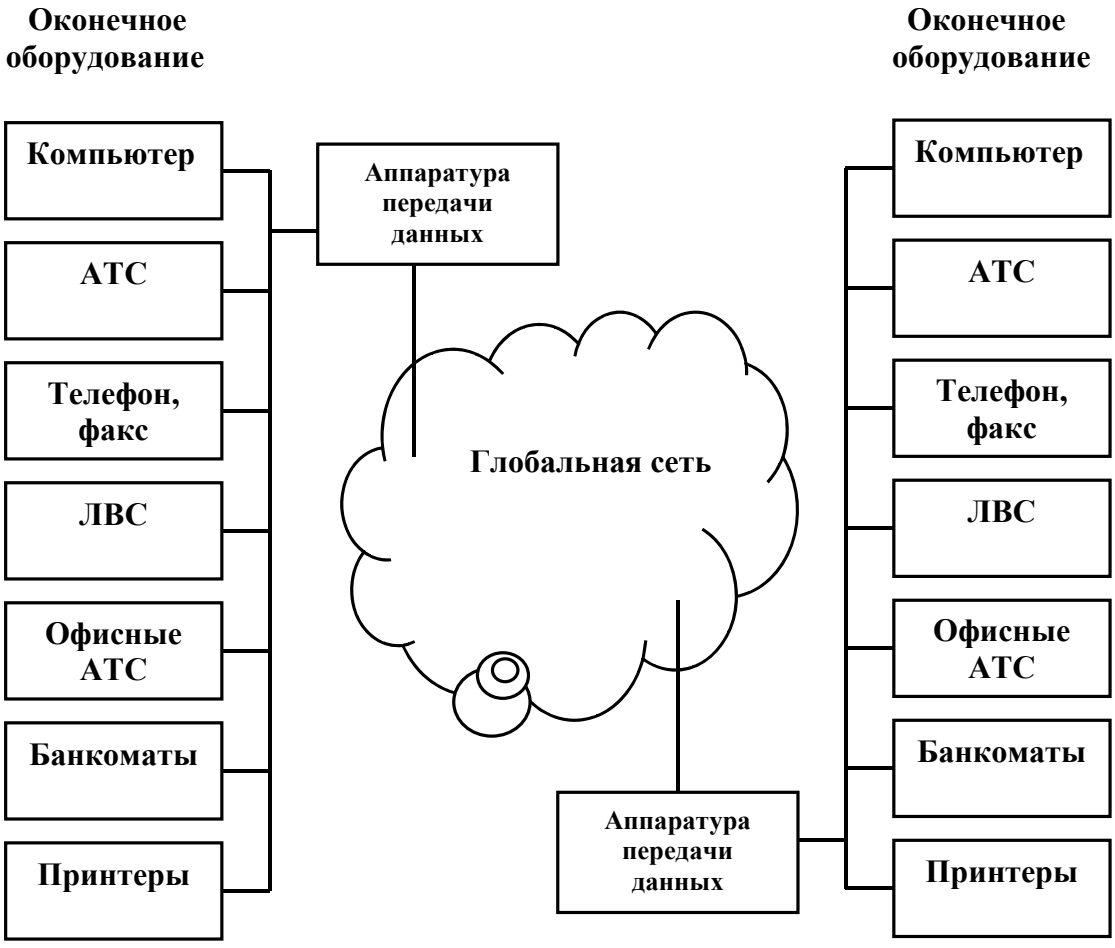


Рис. 10.1. Потребители услуг глобальных сетей

Из рассмотренного списка услуг, которые глобальная сеть предоставляет конечным пользователям, видно, что в основном она используется как транзитный транспортный механизм, предоставляющий только услуги трех нижних уровней модели OSI. Действительно, при построении корпоративной сети, сами данные хранятся и вырабатываются в компьютерах, принадлежащих локальным сетям предприятия, а глобальная сеть их только переносит из одной локальной сети в другую.

Однако в последнее время функции глобальной сети, относящиеся к верхним уровням стека протоколов, стали играть заметную роль. Это связано в первую очередь с популярностью информации, предоставляемой сетью Internet. Информационные услуги Internet оказали влияние на традиционные способы доступа к разделяемым ресурсам, на протяжении многих лет применявшиеся в локальных сетях. Все больше корпоративной информации распространяется с помощью Web-службы. Появился специальный термин intranet, который применяется в тех случаях, когда технологии Internet переносятся в корпоративную сеть. К технологиям intranet относят не только службу Web, но и использование Internet как глобальной транспортной сети, соединяющей локальные сети предприятия, а также все информационные технологии верхних уровней, появившиеся первоначально в Internet и поставленные на службу корпоративной сети. В результате глобальные и локальные сети постепенно сближаются за счет взаимопроникновения технологий разных уровней – от транспортных до прикладных.

Типичный пример структуры глобальной компьютерной сети приведен на рис. 10.2. Здесь используются следующие обозначения: S (switch) – коммутаторы, К – компьютеры, R (router) – маршрутизаторы, MUX (multiplexor) – мультиплексор, UNI (User-Network Interface) – интерфейс пользователь – сеть, NNI (Network-Network Interface) – интерфейс сеть – сеть. Кроме того, офисная АТС обозначена аббревиатурой PBX, а маленькими черными квадратиками – аппаратура передачи данных (Data Circuit Terminating Equipment, DCE).

Сеть строится на основе некоммутируемых (выделенных) каналов связи, которые соединяют коммутаторы глобальной сети между собой. Коммутаторы называют также *центрами коммута-*

ции пакетов (ЦКП). Коммутаторы устанавливаются в тех географических пунктах, в которых требуется ответвление или слияние потоков данных конечных абонентов или магистральных каналов, переносящих данные многих абонентов. Абоненты сети подключаются к коммутаторам в общем случае также с помощью выделенных каналов связи. Эти каналы связи имеют более низкую пропускную способность, чем магистральные каналы, объединяющие коммутаторы, иначе сеть бы не справилась с потоками данных своих многочисленных пользователей.

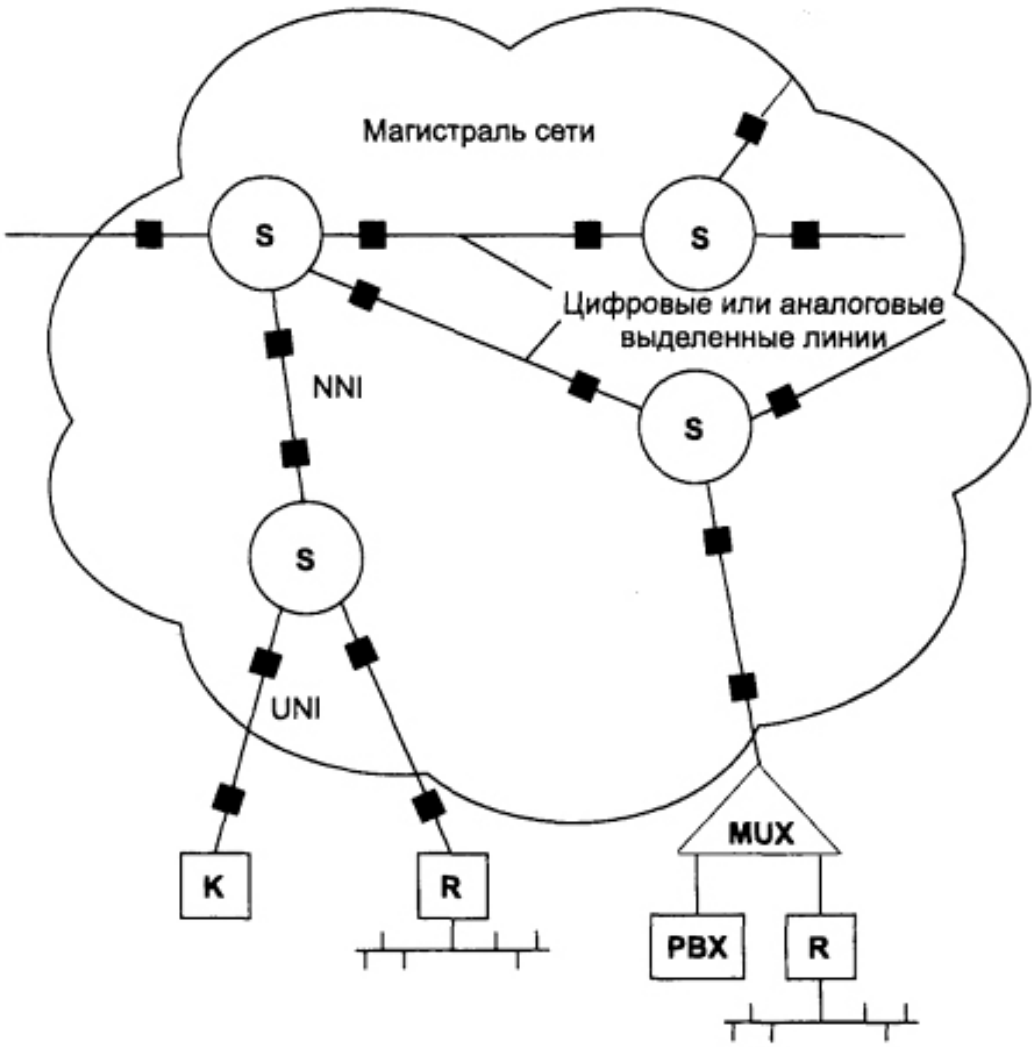


Рис. 10.2. Структура глобальной сети

Для подключения конечных пользователей допускается использование коммутируемых каналов, то есть каналов телефонных сетей, хотя в таком случае качество транспортных услуг обычно ухудшается. Принципиально замена выделенного канала на коммутируемый ничего не меняет, но вносятся дополнитель-

ные задержки, отказы и разрывы канала по вине сети с коммутацией каналов, которая в таком случае становится промежуточным звеном между пользователем и сетью с коммутацией пакетов. Кроме того, в аналоговых телефонных сетях канал обычно имеет низкое качество из-за высокого уровня шумов. Применение коммутируемых каналов на магистральных связях коммутатор-коммутатор также возможно, но по тем же причинам весьма нежелательно.

Локальная сеть отделена от глобальной маршрутизатором или удаленным мостом, поэтому для глобальной сети она представлена единым устройством – портом маршрутизатора или моста. При передаче данных через глобальную сеть *мосты* и *маршрутизаторы* работают в соответствии с той же логикой, что и при соединении локальных сетей. *Мультиплексоры «голос-данные»* предназначены для совмещения в рамках одной территориальной сети компьютерного и голосового трафиков. Так как рассматриваемая глобальная сеть передает данные в виде пакетов, то мультиплексоры «голос-данные», работающие на сети данного типа, упаковывают голосовую информацию в кадры или пакеты территориальной сети и передают их ближайшему коммутатору точно так же, как и любой конечный узел глобальной сети, то есть мост или маршрутизатор. Если глобальная сеть поддерживает приоритезацию трафика, то кадрам голосового трафика мультиплексор присваивает наивысший приоритет, чтобы коммутаторы обрабатывали и продвигали их в первую очередь. Приемный узел на другом конце глобальной сети также должен быть мультиплексором «голос-данные». Голосовые данные направляются офисной АТС, а компьютерные данные поступают через маршрутизатор в локальную сеть. Часто модуль мультиплексора «голос-данные» встраивается в маршрутизатор.

Так как конечные узлы глобальной сети должны передавать данные по каналу связи определенного стандарта, то каждое конечное устройство (DTE) требуется оснастить устройством типа DCE, которое обеспечивает необходимый протокол физического уровня данного канала.

10.2. Организация удаленного доступа

Приведенная на рис. 10.2 глобальная вычислительная сеть работает в наиболее подходящем для компьютерного трафика режиме – коммутации пакетов. Оптимальность этого режима для связи локальных сетей доказывают не только данные о суммарном трафике, передаваемом сетью в единицу времени, но и стоимость услуг такой территориальной сети. Обычно при равенстве предоставляемой скорости доступа сеть с коммутацией пакетов оказывается в 2–3 раза дешевле, чем сеть с коммутацией каналов, то есть публичная телефонная сеть. Поэтому при создании корпоративной сети, имеющей удаленные офисы, необходимо стремиться к построению или использованию услуг территориальной сети с территориально распределенными коммутаторами пакетов. Однако часто такая вычислительная глобальная сеть по разным причинам оказывается недоступной в том или ином географическом пункте. Поэтому при построении корпоративной сети можно дополнить недостающие компоненты услугами и оборудованием, арендуемыми у владельцев первичной или телефонной сети. В зависимости от того, какие компоненты приходится брать в аренду, принято различать корпоративные сети, построенные с использованием:

– выделенных каналов;
– коммутации каналов;
– коммутации пакетов.

Выделенный канал – это канал с фиксированной полосой пропускания или фиксированной пропускной способностью, постоянно соединяющий двух абонентов. Абонентами могут быть как отдельные устройства (компьютеры или терминалы), так и целые сети. Выделенные каналы делятся на аналоговые и цифровые, в зависимости от того, какого типа коммутационная аппаратура применена для постоянной коммутации абонентов. На аналоговых выделенных линиях для аппаратуры передачи данных физический и канальный протоколы жестко не определены. Отсутствие физического протокола приводит к тому, что пропускная способность аналоговых каналов зависит от пропускной способности модемов, которые использует пользователь канала. Мо-

дем собственно и устанавливает нужный ему протокол физического уровня для канала. На цифровых выделенных линиях протокол физического уровня зафиксирован – он задан стандартом G.703. Выделенные каналы можно получить у телекоммуникационных компаний, которые владеют каналами дальней связи (таких, например, как «РОСТЕЛЕКОМ»), или от телефонных компаний, которые обычно сдают в аренду каналы в пределах города или региона. Выделенные каналы очень активно применялись совсем в недалеком прошлом и применяются сегодня, особенно при построении ответственных магистральных связей между крупными локальными сетями. Однако при большом количестве географически удаленных точек и интенсивном смешанном трафике между ними использование этой службы приводит к высоким затратам за счет большого количества арендуемых каналов. Сегодня существует большой выбор выделенных каналов – от аналоговых каналов тональной частоты с полосой пропускания 3,1 кГц до цифровых каналов технологии SDH с пропускной способностью 155 и 622 Мбит/с.

Выделенные аналоговые каналы предоставляются пользователю с 4-проводным или 2-проводным окончанием. На каналах с 4-проводным окончанием организация полнодуплексной связи, естественно, выполняется более простыми способами. Для передачи данных по выделенным аналоговым линиям используются модемы, работающие на основе методов аналоговой модуляции сигнала. В отношении режима работы модемы делятся на три группы:

– модемы, поддерживающие только асинхронный режим работы;

– модемы, поддерживающие асинхронный и синхронный режимы работы;

– модемы, поддерживающие только синхронный режим работы.

Модемы, работающие *только в асинхронном режиме*, обычно поддерживают низкую скорость передачи данных – до 1200 бит/с. Дуплексный режим на 2-проводном окончании обеспечивается частотным разделением канала. Асинхронные модемы представляют наиболее дешевый вид модемов, так как им не требуются высокоточные схемы синхронизации сигналов на кварце-

вых генераторах. Кроме того, асинхронный режим работы неприхотлив к качеству линии.

Модемы, работающие *только в синхронном режиме*, могут подключаться только к 4-проводному окончанию и имеют гораздо более высокие скорости передачи (2400 бит/с – 168 Кбит/с). Синхронные модемы используют для выделения сигнала высокоточные схемы синхронизации и поэтому обычно значительно дороже асинхронных модемов. Кроме того, синхронный режим работы предъявляет высокие требования к качеству линии.

Модемы, *работающие в асинхронном и синхронном режимах*, являются наиболее универсальными устройствами. Чаще всего они могут работать как по выделенным, так и по коммутируемым каналам, обеспечивая дуплексный режим работы. На выделенных каналах они поддерживают в основном 2-проводное окончание и гораздо реже – 4-проводное. Для асинхронно-синхронных модемов разработан ряд стандартов, обеспечивающих скорость передачи до 33,6 Кбит/с.

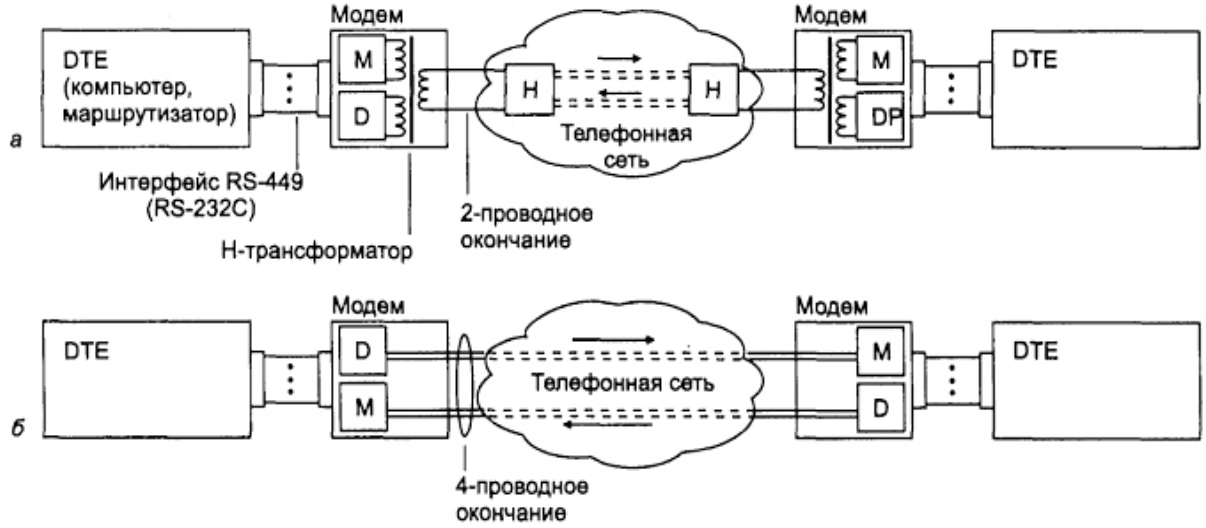


Рис. 10.3. Схема соединения узлов по выделенной линии

Модемы различаются не только поддерживаемыми протоколами, но и определенной ориентацией на область применения. Различают профессиональные модемы, которые предназначены для работы в модемных пулах корпоративных сетей, и модемы для применения в небольших офисах или на дому. Профессиональные модемы отличаются высокой надежностью, способностью устойчиво работать в непрерывном режиме и поддержкой

средств удаленного централизованного управления. Обычно система управления модемными стойками поставляется отдельно и оправдывает себя в условиях большого предприятия.

Типовая структура соединения двух компьютеров или локальных сетей через маршрутизатор с помощью выделенной аналоговой линии приведена на рис. 10.3. В случае 2-проводного окончания (см. рис. 10.3, *а*) для обеспечения дуплексного режима модем использует трансформаторную развязку. Телефонная сеть благодаря своей схеме развязки обеспечивает разъединение потоков данных, циркулирующих в разных направлениях. При наличии 4-проводного окончания (см. рис. 10.3, *б*) схема модема упрощается.

Коммутация каналов

Для построения глобальных связей в корпоративной сети в режиме коммутации каналов используются сети двух типов – традиционные аналоговые телефонные сети и цифровые сети с интеграцией услуг ISDN. Достоинством сетей с коммутацией каналов является их распространенность, что особенно характерно для аналоговых телефонных сетей. Известным недостатком аналоговых телефонных сетей является низкое качество составного канала. Телефонные сети, полностью построенные на цифровых коммутаторах, и сети ISDN свободны от многих недостатков традиционных аналоговых телефонных сетей. Они предоставляют пользователям высококачественные линии связи. Однако даже при качественных каналах связи, которые могут обеспечить сети с коммутацией каналов, для построения корпоративных глобальных связей эти сети могут оказаться экономически неэффективными. Так как в таких сетях пользователи платят не за объем переданного трафика, а за время соединения, то при трафике с большими пульсациями и, соответственно, большими паузами между пакетами оплата идет во многом не за передачу, а за ее отсутствие. Это прямое следствие плохой приспособленности метода коммутации каналов для соединения компьютеров. Тем не менее, при подключении массовых абонентов к корпоративной сети телефонная сеть оказывается единственным подходящим видом глобальной службы из соображений доступности.

К сожалению, эти сети малопригодны для построения магистралей корпоративных сетей. Со средней пропускной способностью 9600 бит/с коммутируемые аналоговые линии, оснащенные модемами, подходят только для пользователя с минимальными требованиями к времени реакции системы. Максимальная на сегодня пропускная способность в 56 Кбит/с достигается только в том случае, если все коммутаторы в сети на пути следования данных являются цифровыми, да и то такая скорость обеспечивается только в направлении «сеть – пользователь». Чаще всего такие линии используются для индивидуального удаленного доступа к сети или же как резервные линии связи небольших офисов с центральным отделением предприятия. Доступ по телефонной сети имеет англоязычное название *«dial-up access»*. Тем не менее, при недостатке средств коммутируемые аналоговые линии обеспечивают связь локальных сетей между собой. Это выгодный режим соединения, если количество передаваемых данных невелико и данные не требуют частого обновления. В этом случае две сети могут соединяться по аналоговой телефонной сети, например, раз в сутки, передавать в течение нескольких минут данные, а затем разрывать соединение.

В телефонных коммутаторах аналоговых телефонных сетей могут использоваться два принципа коммутации – аналоговый, основанный на частотном разделении канала (FDM), и цифровой, основанный на разделении канала во времени (TDM).

Коммутация пакетов

В 80-е годы для надежного объединения локальных сетей в корпоративную сеть использовалась практически одна технология глобальных сетей с коммутацией пакетов – X.25. Сегодня выбор стал гораздо шире, помимо сетей X.25 он включает такие технологии, как frame relay и ATM. Кроме этих технологий, разработанных специально для глобальных компьютерных сетей, можно воспользоваться услугами территориальных сетей TCP/IP. Более подробно эти технологии будут рассмотрены ниже.

Целесообразно делить территориальные сети, используемые для построения корпоративной сети, на две большие категории: магистральные сети и сети доступа.

Магистральные территориальные сети (backbone wide-area networks) используются для образования одноранговых связей между крупными локальными сетями, принадлежащими большим подразделениям предприятия. Магистральные территориальные сети должны обеспечивать высокую пропускную способность, так как на магистрали объединяются потоки большого количества подсетей. Кроме того, магистральные сети должны быть постоянно доступны, то есть обеспечивать очень высокий коэффициент готовности. Обычно в качестве магистральных сетей используются цифровые выделенные каналы со скоростями от 2 до 622 Мбит/с. При наличии выделенных каналов для обеспечения высокой готовности магистрали используется смешанная избыточная топология связей.

Под *сетями доступа* понимаются территориальные сети, необходимые для связи небольших локальных сетей и отдельных удаленных компьютеров с центральной локальной сетью предприятия. В качестве отдельных удаленных узлов могут также выступать банкоматы или кассовые аппараты, требующие доступа к центральной базе данных для получения информации. Банкоматы или кассовые аппараты обычно рассчитаны на взаимодействие с центральным компьютером по сети X.25, которая в свое время специально разрабатывалась как сеть для удаленного доступа неинтеллектуального терминального оборудования к центральному компьютеру.

К сетям доступа предъявляются требования, существенно отличающиеся от требований к магистральным сетям. Так как точек удаленного доступа у предприятия может быть очень много, одним из основных требований является наличие разветвленной инфраструктуры доступа. Кроме того, стоимость удаленного доступа должна быть умеренной, чтобы экономически оправдать затраты на подключение десятков или сотен удаленных абонентов. При этом требования к пропускной способности у отдельного компьютера или локальной сети, состоящей из двух-трех клиентов, обычно укладываются в диапазон нескольких десятков килобит в секунду. В качестве сетей доступа обычно применяются телефонные аналоговые сети, сети ISDN и реже – сети frame relay. При подключении локальных сетей филиалов также используются выделенные каналы со скоростями от 19,2 до 64 Кбит/с.

Программные и аппаратные средства, которые обеспечивают подключение компьютеров или локальных сетей удаленных пользователей к корпоративной сети, называются *средствами удаленного доступа*. Обычно на клиентской стороне эти средства представлены модемом и соответствующим программным обеспечением. Организацию массового удаленного доступа со стороны центральной локальной сети обеспечивает *сервер удаленного доступа* (Remote Access Server, *RAS*). Сервер удаленного доступа представляет собой программно-аппаратный комплекс, который совмещает функции маршрутизатора, моста и шлюза. Серверы удаленного доступа обычно имеют достаточно много низкоскоростных портов для подключения пользователей через аналоговые телефонные сети или ISDN. Очевидно, что для экономии модемов можно не ставить на каждый компьютер центральной сети отдельный модем, а организовать общий пул *модемов* и сделать его разделяемым ресурсом как для звонков из локальной сети, так и для звонков извне. Разделяемый для пользователей локальный пул модемов создается с помощью так называемого *коммуникационного сервера* (Communication Server). Коммуникационный сервер – это обычный компьютер или специализированное устройство, предоставляющее пользователям прозрачный доступ к последовательным портам ввода-вывода, к которым подключены разделяемые модемы.

Сервер удаленного доступа обслуживает удаленных пользователей, предоставляя им доступ к ресурсам локальной сети извне. Именно это является основной задачей систем удаленного доступа. С этой точки зрения удаленный доступ можно определить как эффективный способ разделения ресурсов централизованных серверов между удаленными клиентами. В качестве удаленных пользователей могут выступать как отдельные компьютеры, так и небольшие локальные сети (офисы) филиалов предприятия.

Общая схема удаленного доступа представлена на рисунке 10.4. Модемы обозначены буквой M, а маршрутизаторы буквой R.

Однако если удаленные компьютеры или офисы находятся в других городах или странах, то описанная выше схема доступа становится дорогой. Качественный скачок в расширении возможностей удаленного доступа произошел в связи со стремительным ростом популярности и распространенности Internet.

Транспортные услуги Internet дешевле, чем услуги междугородных и международных телефонных сетей, а их качество быстро улучшается. Поэтому стала возможной двухступенчатая связь удаленных пользователей со своей корпоративной сетью. Сначала удаленный пользователь через телефонный канал связывается с местным поставщиком услуг Интернет, а затем через Интернет соединяется со своей корпоративной сетью.

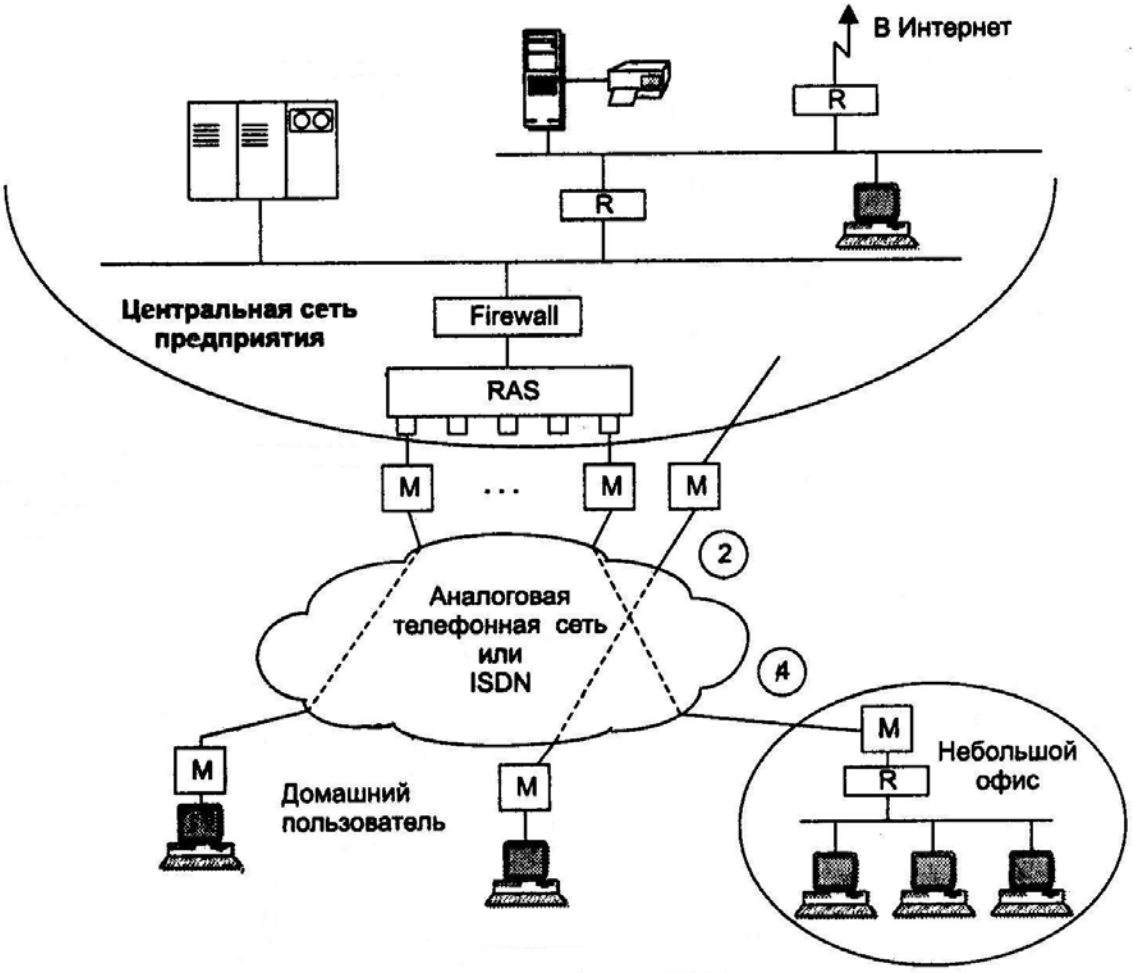


Рис. 10.4. Схема удаленного доступа

10.3. Сети и технологии X.25

Сетями X.25 называются сети, доступ к которым производится в соответствии с рекомендациями Международного консультативного комитета по телефонии и телеграфии (МККТТ), первый вариант которой появился в 1976 г. Эта рекомендация опи-

сывает интерфейс доступа пользователя в сеть передачи данных (СПД), а также интерфейс взаимодействия с удаленным пользователем через СПД. Передача данных в сети X.25 производится по протоколам, описанным в рекомендации X.25. Главным достоинством протокола X.25 явилось то, что он носил международный характер. По существу, это был первый шаг к стандартизации сетевых служб. Протокол X.25 разрабатывался во времена, когда каналы и аппаратура передачи данных были медленными и ненадежными, поэтому протокол предусматривает широкий спектр средств обнаружения и исправления ошибок на канальном уровне. В силу этого по сети передается большое количество служебных пакетов, что приводит к некоторому снижению эффективности сети.

Несмотря на появление новых интегральных технологий сетей связи, рассчитанных на высокоскоростные каналы связи, сети X.25 все еще являются наиболее распространенными СПД. Это объясняется тем, что именно сети X.25 с наибольшим основанием можно сравнить с телефонными сетями. Установив соединение компьютера с ближайшим узлом сети X.25, можно связаться с любым из многих тысяч пользователей сетей X.25 по всему миру (для этого надо лишь знать его сетевой адрес), точно так же, как, подняв трубку телефонного аппарата, подключенного к ближайшей АТС, можно соединиться практически с любым абонентом. Технология X.25 особенно актуальна для России и других стран, где пока отсутствует развитая инфраструктура высокоскоростных первичных каналов связи.

На основе технологий X.25 построено большинство эксплуатируемых в настоящее время СПД с коммутацией пакетов, предназначенных для организации и обеспечения надежной передачи данных в условиях разветвленных территориальных сетей на базе низко- и среднескоростных каналов. При этом за счет повторной передачи искаженных кадров между каждой парой соседних узлов сети обеспечивается достоверная и упорядоченная передача данных. Однако в сети с каналами низкого качества из-за повторных передач возникают нерегламентированные и непостоянные задержки передаваемых данных, поэтому передача трафика, чувствительного к задержкам (например, оцифрованного голоса), по сетям X.25 с удовлетворительным качеством невозможна.

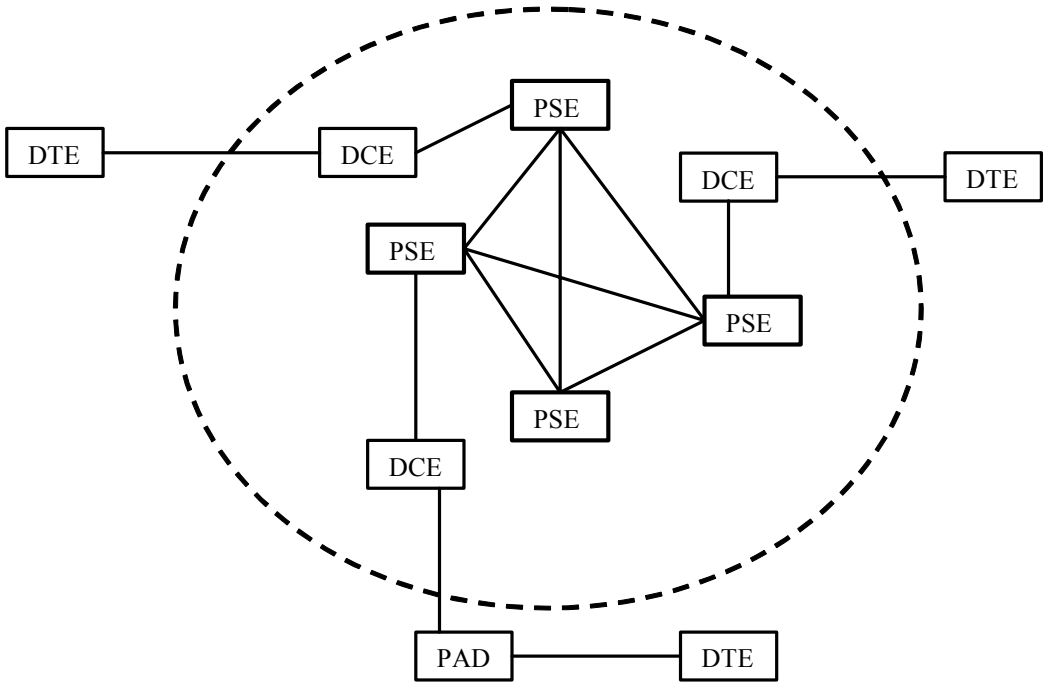


Рис. 10.5. Схема соединения объектов сети X.25

Спецификация X.25 определяет двухточечное взаимодействие между конечным оборудованием пользователей (DTE – data terminal equipment; терминалы, компьютеры) и телекоммуникационным оборудованием (DCE – data circuit-terminal equipment). Устройства DTE подключают к устройствам DCE (модемы), которые соединены с «коммутаторами переключения пакетов» (PSE) и другими DCE внутри сети с коммутацией пакетов PSN и, наконец, с другим устройством DTE. Взаимоотношения между объектами сети X.25 показаны на рис. 10.5. DTE может быть терминалом, который не полностью реализует все функциональные возможности X.25. Такие DTE подключают к DCE через трансляционное устройство, называемое пакетный ассемблер/дизассемблер (PAD).

Рекомендация X.25 описывает три уровня протоколов: физический, канальный и сетевой. Они реализуют функции соответственно физического, канального, сетевого и частично транспортного уровней модели взаимодействия открытых систем OSI (Рис. 10.6).

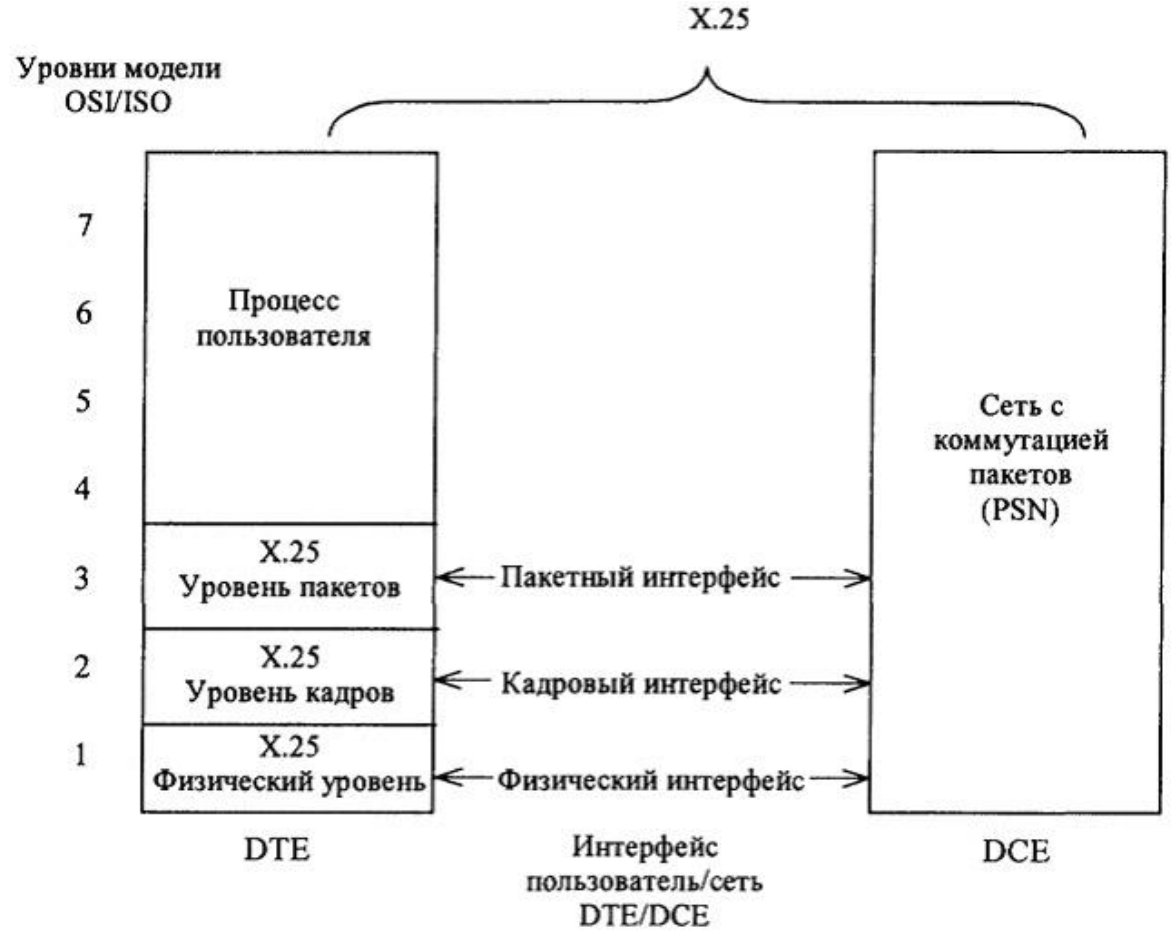


Рис. 10.6. Соответсвие стека протоколов X.25 модели OSI

Физический уровень, широко представленный в оборудовании массового спроса, описывает уровни сигналов и логику взаимодействия на уровне физического интерфейса.

Канальный уровень, также широко представленный в оборудовании (например, в модемах), отвечает за эффективную и надежную передачу данных в соединении «точка – точка», т. е. между соседними узлами сети X.25. Уровень реализован протоколом Link Access Procedure, Balanced (LAPB), определяющим кадрирование пакетов для звена DTE/DCE. На этом уровне осуществляется защита от ошибок, управление потоком данных и, кроме того, обеспечивается получение оптимального по скорости передачи режима в зависимости от протяженности канала между двумя точками (времени задержки в канале) и качества канала (вероятности искажения информации при передаче).

Для реализации указанных выше функций поток информации разбивается на кадры (frame), каждый из которых представляет

собой организованную определенным образом последовательность битов. Кадр обрамляется «флагами» (уникальными последовательностями битов, являющимися разделителем между кадрами), и состоит из служебных полей (поля адреса, поля управления с циклическим номером кадра, поля проверочной последовательности кадра) и информационного поля для информационных кадров. Длину кадра можно менять при настройке параметров протокола к физическим характеристикам линии связи. Чем короче кадр, тем меньше вероятность его искажения при передаче. С другой стороны, если линия хорошего качества, то информацию лучше передавать более длинными кадрами, обеспечивающими уменьшение процента избыточной информации (флаги, служебные поля кадра).

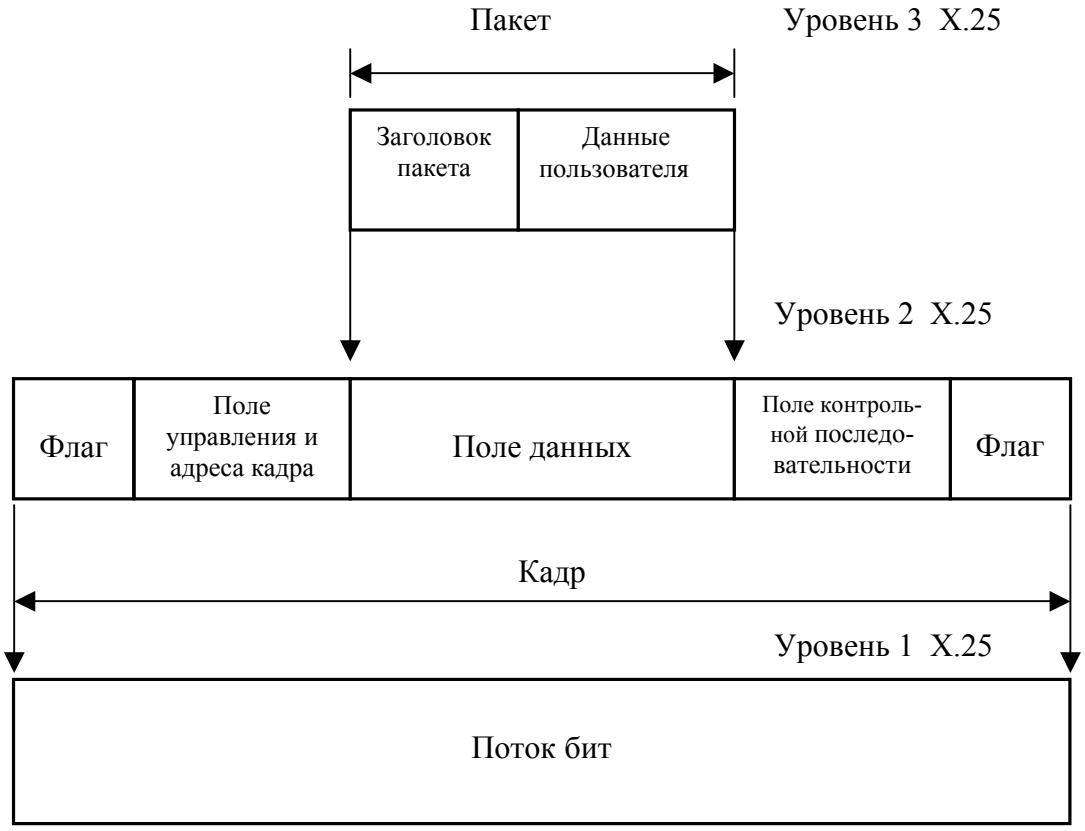


Рис. 10.7. Блоки данных X.25

Наконец, *на сетевом уровне*, определяющем специфику сетей X.25, производится маршрутизация пакетов и доведение информации от «точки входа» в сеть до «точки выхода» из нее. На этом уровне информация разбивается на порции, называемые пакетами. Уровень описывает форматы пакетов и процедуры обмена

пакетами между равноправными объектами этого уровня. Структура пакета во многом аналогична структуре кадра. При передаче пакет помещается в поле данных информационного кадра (кадра канального уровня).

Блок данных X.25 состоит из последовательности полей, показанной на рис. 10.7. Поля X.25 уровня 3 образуют пакет X.25 и состоят из заголовка и данных пользователя. Поля X.25 уровня 2 включают в себя поле управления и адреса кадра, встроенный пакет уровня 3 (поле данных) и проверочную последовательность блока данных (FCS).

В сетях X.25 реализуется метод «коммутации пакетов», в соответствии с которым перед передачей информации от одного абонента к другому между ними сначала устанавливается виртуальное (логическое) соединение, т. е. происходит обмен пакетами «запрос вызова» – «вызов принят», после чего производится обмен информацией. Чтобы начать связь, один компьютер обращается к другому с запросом о сеансе связи. Вызванный компьютер может принять или отклонить связь. Если вызов принят, то обе системы могут начать передачу информации. Любая сторона может в любой момент прекратить связь.

Сквозная передача между устройствами DTE выполняется через двунаправленную связь, называемую виртуальной цепью. Виртуальные цепи позволяют осуществлять связь между различными элементами сети через любое число промежуточных узлов. После организации виртуальной цепи DTE отсылает пакет на другой конец связи через DCE, используя соответствующую виртуальную цепь. DCE просматривает номер виртуальной цепи для определения маршрута этого пакета через сеть X.25. Протокол сетевого уровня X.25 осуществляет мультиплексную передачу между всеми DTE, которые обслуживает устройство DCE, расположенное в сети со стороны пункта назначения, в результате чего пакет доставляется к DTE пункта назначения. Виртуальные соединения могут быть как постоянными, так и коммутируемыми, когда соединение устанавливается под каждый сеанс обмена информацией.

Доступ пользователей к сети X.25 осуществляется в одном из двух режимов – в пакетном или в монопольном. Доступ с персонального компьютера (ПК) в сеть в *пакетном режиме* реализует-

ся путем установления в ПК специальной платы, обеспечивающей обмен данными в соответствии со стандартом X.25. Подключение ЛВС через сеть X.25 осуществляется с помощью сетевых плат, или для этого могут использоваться мосты – маршрутизаторы удаленного доступа, включенные в виде отдаленных устройств и поддерживающие протокол X.25. Преимущество таких устройств по сравнению со встроенными в компьютер платами (помимо большей производительности) состоит в том, что они не требуют установки специального программного обеспечения, а сопрягаются с ЛВС по стандартному интерфейсу локальной сети, что позволяет реализовать более гибкие и универсальные решения. Подключение пользовательского оборудования к сети в пакетном режиме удобно, когда требуется многопользовательский доступ к этому оборудованию через сеть.

Подключение к сети X.25 в *монопольном режиме* производится по стандартам X. 3, X.28, X.29, которые определяют функционирование специальных устройств доступа в сеть (PAD). Эти устройства используются для доступа в сеть абонентов в асинхронном режиме обмена информацией, т.е. через последовательный порт компьютера (непосредственно или с применением модемов).

Поля адресации в пакетах запроса на установление соединения содержат адреса DTE источника и пункта назначения. Их используют для организации виртуальных цепей. Адреса (называемые также International Data Numbers, или IDN) имеют разную длину, которая может составлять до 14 десятичных знаков. Четвертый байт в пакете запроса на установление соединения определяет длину адресов DTE источника и назначения. Формат адреса представлен на рис. 10.8.

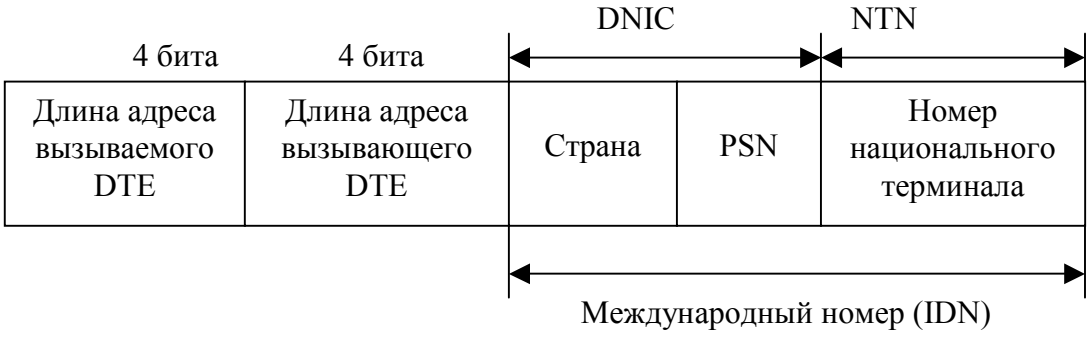


Рис. 10.8. Формат адреса сети X.25

Адресация в сетях X.25 осуществляется в соответствии с рекомендацией МККТТ X.121, согласно которой полный сетевой адрес имеет следующий вид (записывается как единое число без пробелов и служебных символов):

CCCCXXXXYYYYZZ

Первые четыре цифры *IDN (CCCC)* называются код идентификации сети (DNIC – Data Network Identification Code). Он поделен на три части. Первая цифра определяет код региона (1 – Океания, 2 – Европа, 3 – Северная Америка, 4 – Азия, 5 – Австралия, 6 – Африка, 7 – Южная Америка). Две следующие цифры определяют страну, где находится сеть PSN (для стран СНГ это 50). Четвертая цифра определяет код национальной сети (Для России, например: 0 – ROSPAC, 1 – SPRINT, 3 – MMTELNET, 4 – INFOTEL, 6 – ROSNET).

Последовательность цифр XXXXYYYYZZ называются номером национального терминала (NTN-national terminal number), используемого для идентификации определенного DTE в сети (внутрисетевой адрес). Здесь обычно: XXXX – номер узла, YYYY – номер линии на узле, ZZ – подадрес абонента.

Метод коммутации пакетов, лежащий в основе сетей X.25, определяет их основные преимущества. На сегодняшний день накоплен большой опыт использования сетей X.25, который показывает, что они эффективны для широкого круга задач передачи данных: обмен сообщениями, обращение большого количества пользователей к удаленной базе данных, связь локальных сетей, объединение удаленных кассовых аппаратов и банкоматов и пр.

Немаловажным достоинством сетей X.25 является то, что по ним можно передавать данные по каналам телефонной сети общего пользования, как выделенным, так и коммутируемым с максимальной для этих каналов скоростью и достоверностью. Кроме того, сети X.25 предоставляют возможность связи через обычные асинхронные COM-порты. Таким образом, практически любое приложение, допускающее обращение к удаленным ресурсам через COM-порт, может быть легко интегрировано в сеть X.25.

Для объединения локальных сетей в узлах, имеющих подключение к сети X.25, используют методы инкапсуляции (упаковки) пакетов информации из локальной сети в пакеты X.25. Стандарт-

ный механизм инкапсуляции позволяет передавать различные протоколы локальных сетей (IP, IPX и др.) и реализован практически во всех современных маршрутизаторах. Таким образом, сети X.25 предлагают универсальный транспортный механизм для передачи информации между приложениями. При объединении локальных сетей через X.25 отдельные фрагменты корпоративной сети можно изолировать друг от друга, что облегчает решение проблемы безопасности и разграничения доступа, которые возникают в сложных информационных структурах. Во многих случаях отпадает необходимость использования сложных механизмов маршрутизации, так как эту функцию может выполнять сеть X.25.

Сегодня в мире насчитывают десятки глобальных сетей X.25 общего пользования, узлы которых расположены практически во всех крупных деловых, промышленных и административных центрах. В России услуги X.25 предлагает ряд компаний, таких, как Infotel, Роснет и др. Для того чтобы подключиться к любому ресурсу сети X.25, пользователю достаточно иметь компьютер с последовательным асинхронным портом и модем.

С точки зрения безопасности передачи информации, сети X.25 имеют ряд достоинств. С помощью сети можно эффективно решить проблему несанкционированного доступа. В случае же, если необходима полная конфиденциальность, когда неприемлем даже небольшой риск перехвата информации, необходимо использовать средства шифрования, в том числе и в реальном времени. В настоящее время для сетей X.25 разработаны средства шифрования, позволяющие работать на достаточно высоких скоростях (до 64 Кбит/с). Такое оборудование производят ряд зарубежных компаний (например, Siemens), а также имеются и российские разработки, созданные под эгидой ФАПСИ.

Метод коммутации пакетов, лежащий в основе сетей X.25, определяет основные преимущества таких сетей:

1. Сети X.25 позволяют в режиме реального времени разделять один и тот же физический канал между несколькими абонентами. Благодаря этому во многих случаях оказывается экономически выгоднее для передачи данных пользоваться сетью X.25, производя оплату за каждый байт переданной информации, а не оплачивать время использования телефонной линии. Метод разделения физического канала между абонентами в сетях X.25 на-

зывают еще логическим или статистическим уплотнением (в отличие от временного разделения канала). При статистическом разделении канала нет строго регламентированной степени загрузки канала каждым абонентом в определенный момент времени. Имеется большой опыт эффективного использования сетей X.25 для широкого спектра задач передачи данных, когда трафик в сети не является равномерным во времени: обмен сообщениями между пользователями, обращение большого числа пользователей к удаленной базе данных или к удаленному хосту электронной почты, связь локальных сетей, объединение удаленных кассовых аппаратов или банкоматов.

2. Сети X.25 позволяют передавать оптимальным образом данные по выделенным и коммутируемым каналам телефонной сети общего пользования. Критериями оптимизации являются максимально возможные на этих каналах скорость и достоверность передачи данных.

3. В сетях X.25 имеется механизм альтернативной маршрутизации, с помощью которого, помимо основного маршрута, задается ряд альтернативных (резервных) маршрутов, за счет чего значительно увеличивается надежность работы сети. Однако это означает, что между любыми двумя точками подключения пользователя к сети должно быть, по крайней мере, два различных маршрута.

При всех достоинствах сетевой технологии X.25 у нее есть и свои довольно серьезные ограничения. В настоящее время принято считать, что сети X.25 медленны, дороги и вообще устарели. Практически не существует сетей X.25, использующих скорости, превышающие 128 Кбит/с. Связано это с тем, в частности, что протокол X.25 включает в себя мощные средства коррекции ошибок, обеспечивая передачу данных без искажений даже на линиях плохого качества. Понятно, что за надежность связи приходится платить, как правило, именно быстродействием оборудования сети и сравнительно большими, хотя и предсказуемыми, задержками распространения информации.

Сети с коммутацией пакетов X.25 не обеспечивают качественную передачу критичного к задержкам трафика (голоса и видеоинформации), так как в них отсутствуют механизмы обеспечения приоритетов каких-либо видов данных.

10.4. Сети и технологии ISDN

Сети ISDN (Integrated Services Digital Network – цифровая сеть с интеграцией услуг) относятся к классу сетей, в которых основным режимом коммутации является принцип коммутации каналов, а данные обрабатываются в цифровой форме. Сеть ISDN можно рассматривать как глобальный коммутатор. Основной поток информации (голос и данные) в ISDN несут B-каналы (bearer channel – основной, несущий канал). Эти каналы коммутируются между парой абонентов с помощью информации, передаваемой по дополнительному D-каналу (Delta channel). После коммутации (установления соединения) каждый B-канал представляет собой две «трубы», пропускающие во встречных направлениях битовые потоки со скоростью 64 Кбит/с. Для цифровой телефонии пропускной способности этих «труб» достаточно для качественной передачи речи. Служебный канал также двунаправленный, его пропускная способность может быть 16 или 64 Кбит/с в зависимости от типа сервиса. Выделение служебного канала позволяет выполнять сервисные функции во время работы текущего соединения, не нарушая его (в обычной телефонии такое невозможно). В качестве сигнала вызова по D-каналу посылается пакет, который содержит идентификаторы вызывающего и вызываемого абонентов и признак сервиса (голос/данные). На установление соединения требуется 2 – 4 секунды. В отличие от аналоговой телефонии, по одной абонентской линии ISDN может передаваться информация для нескольких устройств, поскольку цифровая структура позволяет легко решать задачу маршрутизации.

Режим коммутации пакетов в сети ISDN используется для передачи только сообщения протокола сигнализации. Сети изначально предназначены для передачи как данных, так и голоса. В сетях ISDN используется цифровая технология, получающая все большее распространение, так как:

– цифровые устройства, используемые в ISDN, производятся на основе интегральных схем высокой интеграции;

– по сравнению с аналоговыми устройствами они отличаются большой надежностью и устойчивостью в работе и, кроме того, в производстве и эксплуатации, как правило, дешевле;

– цифровую технологию можно использовать для передачи любой информации по одному каналу (акустических сигналов, телевизионных видеоданных, факсимильных данных);

– цифровые методы преодолевают многие из ограничений передачи и хранения, которые присущи аналоговым технологиям.

В сетях ISDN при передаче аналогового сигнала осуществляется преобразование его в последовательность цифровых значений, а при приеме – обратное преобразование. Например, при разговоре по телефону акустические сигналы преобразуются в электрические. Однако непосредственная передача аналогового электрического сигнала по телефонной линии связи сопряжена с рядом недостатков: искажение сигнала вследствие его нелинейности, которая увеличивается усилителями, затухание сигнала при передаче через среду, подверженность влиянию шумов в канале и др. В ISDN эти недостатки преодолимы. Здесь форма аналогового сигнала представляется в виде цифровых значений, представляющих соответствующие значения амплитуды. Цифровые сигналы также подвержены ослаблению и шумам при их прохождении через канал, однако на приемном пункте необходимо отмечать лишь наличие или отсутствие двоичного цифрового импульса, а не его абсолютное значение, которое важно в случае аналогового сигнала. Следовательно, цифровые сигналы принимаются надежнее, их можно полностью восстановить, прежде чем они из-за затухания станут ниже порогового значения.

Резкое возрастание роли ISDN-сетей объясняется тем, что они обеспечивают интегрированный доступ к речевым и неречевым услугам, имеют сложившуюся инфраструктуру, являются цифровыми сетями, основанными на использовании цифровых каналов 64 Кбит/с, обладают достаточной гибкостью. Популярность ISDN-сети возрастает, поскольку по определению она является мультисервисной (обеспечивает услуги по предоставлению связи, доставке информации, а также дополнительные услуги), ориентированной на приложения. Технология ISDN стабильно развивается, а сеть на ее основе имеет необходимые интерфейсы с другими сетями. Кроме того, имеется большой набор терминального оборудования для ISDN-сетей.

Сети ISDN, связанные между собой, распространены по всему миру. Абонент ISDN получает интерфейс, к которому может под-

ключаться оборудование различных классов. Через линии ISDN могут соединяться и удаленные части корпоративных сетей, обеспечивая значительно большую скорость передачи данных, чем теоретический предел (56 Кбит/с) традиционных телефонных коммуникаций. При этом цена коммутируемых цифровых линий ISDN в большинстве случаев оказывается ниже цены выделенных линий. Передача данных возможна в разных вариантах: между удаленными друг от друга локальными сетями, между индивидуальным удаленным абонентом и локальной сетью, между индивидуальными абонентами. Через линии ISDN возможна передача данных с помощью технологий и протоколов глобальных сетей (X.25, Frame Relay) а также организация туннелей для соединения локальных сетей с протоколами IP и IPX.

Основными средствами доступа к сети ISDN являются маршрутизаторы или мосты локальных сетей, оконечные сетевые устройства доступа для оптических и медных линий связи, мультиплексоры (для сбора и передачи информации от удаленных абонентов), системы для проведения видеоконференций, мини – УАТС (управленческие автоматические телефонные станции). Цифровые УАТС с функциями ISDN позволяют: более полно использовать каналы связи для передачи данных и речи, выйти абоненту в сеть ISDN с различных устройств (телефона, факса, компьютера), одновременно передавать речь и данные, подключать мосты или маршрутизаторы для взаимодействия удаленных ЛВС.

Архитектура сети ISDN предусматривает следующие виды служб:

– некоммутируемые средства (выделенные цифровые каналы);
– коммутируемая телефонная сеть общего назначения;
– сеть передачи данных с коммутацией каналов;
– сеть передачи данных с коммутацией пакетов;
– сеть передачи данных с трансляцией кадров;
– средства контроля и управления работой сети.

Технология ISDN разрабатывалась как основа всемирной телекоммуникационной сети, позволяющих связывать как телефонных абонентов, так и абонентов других глобальных сетей. Основное назначение сети – передача телефонного трафика. Поэтому за основу адресации узлов был взят формат международного телефонного плана, расширенный для поддержки большего

числа абонентов и использования адресов других сетей. Формат адреса ISDN состоит из 55 десятичных цифр.

Сети и технологии ISDN предоставляют пользователям следующие основные услуги: передача данных со скоростью 64 Кбит/с, передача речи в цифровом виде, телетекст, факс, видеосвязь. Таким образом, сети ISDN, основной целью разработки которых было объединение в одной сети трафиков цифровых телефонных сетей и компьютерных данных, в настоящее время широко используются для решения задач по передаче информации в следующих областях: телефония, передача данных, объединение ЛВС, доступ к глобальным компьютерным сетям, интеграция различных видов трафика, передача трафика, чувствительного к задержкам (звук, видео).

10.5. Сети и технологии PDH и SDH

Существуют два поколения технологий цифровых первичных сетей – технология плезиохронной («плезио» означает «почти», то есть почти синхронной) цифровой иерархии (Plesiochronic Digital Hierarchy, PDH) и более поздняя технология – синхронная цифровая иерархия (Synchronous Digital Hierarchy, SDH). В Америке технологии SDH соответствует стандарт SONET. Цифровая аппаратура мультиплексирования и коммутации была разработана в конце 60-х годов компанией AT&T для решения проблемы связи крупных коммутаторов телефонных сетей между собой.

Физический уровень технологии PDH поддерживает различные виды кабелей: витую пару, коаксиальный кабель и волоконно-оптический кабель. Основным вариантом абонентского доступа к каналам T1/E1 является кабель из двух витых пар с разъемами RJ-48. Две пары требуются для организации дуплексного режима передачи данных со скоростью 1,544/2,048 Мбит/с.

Одним из основных недостатков технологии PDH является сложность операций мультиплексирования и демультиплексирования пользовательских данных. Сам термин «плезиохронный», используемый для этой технологии, говорит о причине такого явления – отсутствии полной синхронности потоков данных при объединении низкоскоростных каналов в более высокоскоростные.

Другим существенным недостатком технологии PDH является отсутствие развитых встроенных процедур контроля и управления сетью. Нет в технологии и процедур поддержки отказоустойчивости, которые очень полезны для первичных сетей, на основе которых строятся ответственные междугородные и международные сети.

Третий недостаток состоит в слишком низких по современным понятиям скоростях иерархии PDH. Волоконно-оптические кабели позволяют передавать данные со скоростями в несколько гигабит в секунду по одному волокну, что обеспечивает консолидацию в одном кабеле десятков тысяч пользовательских каналов, но это свойство технология PDH не реализует – ее иерархия скоростей заканчивается уровнем 139 Мбит/с.

Все эти недостатки устранены в новой технологии первичных цифровых сетей, получившей название синхронной цифровой иерархии. В сетях стандарта SDH реализуется технология синхронных волоконно-оптических сетей. Это высокоскоростные сети цифровой связи, которые строятся на базе оптоволоконных кабельных линий или цифровых радиорелейных линий. Основу инфраструктуры современных высокоскоростных телекоммуникационных сетей (магистральных, региональных или городских) составляют цифровые линии и узлы сети стандарта SDH.

Сети и технологии SDH отличаются высоким уровнем стандартизации (что позволяет в одной сети использовать оборудование разных фирм-производителей), высокой надежностью (централизованное управление сетью обеспечивает полный мониторинг состояния узлов), наличием полного программного контроля (отслеживание и регистрация аварийных ситуаций, управление конфигурацией сети осуществляется программными средствами с единой консоли управления), возможностью оперативного предоставления услуг по требованию, сравнительно простой схемой развития сети. Благодаря этим преимуществам технология SDH стала основной при построении цифровых транспортных сетей самого различного масштаба. Топология всей SDH-сети формируется из отдельных базовых топологий типа «кольцо», «линейная цепь», «звезда», «точка-точка», которые используются в качестве сегментов сети. Чаще применяется радиально-кольцевая

архитектура SDH-сети, построенная на базе кольцевой и линейной топологий.

В России наибольшую активность в использовании SDH-технологии проявляет АО «Ростелеком». Это АО ежегодно строит 5-6 тыс. км магистральных цифровых линий на основе волоконно-оптических кабелей (ВОЛС) и цифровых радиорелейных линий. В 1994 году построена и эксплуатируется высокоскоростная цифровая оптоволоконная магистральная линия стандарта SDH между Москвой и Санкт-Петербургом протяженностью 690 км.

10.6. Сети и технологии Frame Relay

Сетью *Frame Relay* (в дальнейшем – **FR**) называется сеть коммутации кадров. Сети frame relay – сравнительно новые сети, которые гораздо лучше подходят для передачи пульсирующего трафика локальных сетей по сравнению с сетями X.25. Это преимущество проявляется только тогда, когда каналы связи приближаются по качеству к каналам локальных сетей, а для глобальных каналов такое качество обычно достижимо только при использовании волоконно-оптических кабелей. Преимущество сетей FR заключается в их низкой протокольной избыточности и дейтаграммном режиме работы, что обеспечивает высокую пропускную способность и небольшие задержки кадров. Надежную передачу кадров технология FR не обеспечивает. Сети FR специально разрабатывались как общественные сети для соединения частных локальных сетей. Они обеспечивают скорость передачи данных до 2 Мбит/с. Особенностью технологии FR является гарантированная поддержка основных показателей качества транспортного обслуживания локальных сетей – средней скорости передачи данных по виртуальному каналу при допустимых пульсациях трафика. Кроме технологии frame relay гарантии качества обслуживания на сегодня может предоставить только технология ATM.

Протокол FR – это интерфейс доступа к сетям быстрой коммутации пакетов. Он позволяет эффективно передавать крайне *неравномерно распределенный во времени трафик*. Отличительные особенности протокола FR: *малое время задержки при передаче информации через сеть, высокие скорости передачи, «высо-*

кая степень связности», эффективное использование полосы пропускания.

Для оценки FR-сетей (как и ATM-сетей) важным фактором является не столько высокая «физическая» скорость передачи данных (т. е. скорость «физических» каналов), *сколько реализация методов статистического уплотнения информации*, обеспечивающих существенное повышение информационной скорости передачи в условиях дефицита физической пропускной способности канала, а также наличие интерфейсов для эффективного подключения к сети различных типов оконечных пользовательских устройств.

Протокол FR выполняет функции первого, частично второго и третьего уровней модели OSI. Он позволяет устанавливать соединение между взаимодействующими узлами сети, аналогично соединению по X.25. Внутри каждого физического канала может быть создана совокупность логических каналов, что и объясняет «высокую степень связности», обеспечиваемую протоколом FR.

Сети FR могут выступать альтернативой сетей X.25. Например, ЛВС могут подключаться к сети непосредственно по интерфейсу FR, и тогда FR-сеть выполняет те же функции по обеспечению взаимодействия удаленных ЛВС, что и сеть X.25. В других случаях сеть FR выступает в качестве высокоскоростной магистрали для объединения ряда сетей X.25. Такое решение легко реализуется, так как большинство современных устройств центров коммутации пакетов сетей X.25 оборудованы портами FR.

В отличие от сетей X.25, где на сетевом уровне обеспечивается гарантированная передача пакетов (в случае искажения при передаче какого-либо пакета происходит его повторная передача), кадр FR не содержит переменных нумераций передаваемых и подтверждаемых кадров. При межузловом обмене информацией в сетях FR ошибочные кадры просто «выбрасываются», их повторная передача средствами FR не происходит. Для обеспечения гарантированной и упорядоченной передачи кадров необходимо использовать либо протоколы более высокого уровня (например, протокол TCP/IP), либо дополнение к протоколу FR.

Кадр FR-сети имеет минимальную избыточность, т.е. доля служебной информации в кадре по отношению к передаваемым данным пользователя минимальна. Это способствует сокраще-

нию времени на передачу фиксированного объема информации. Кроме того, в сети FR может производиться маршрутизация своими средствами (без задействования механизмов маршрутизации по X.25 или по протоколу IP), что значительно увеличивает скорость маршрутизации. Однако такой эффект достигается только при использовании каналов, качество которых соответствует требованиям технологии FR. В противном случае сравнительно много кадров будут передаваться с ошибкой, и потребуется повторная передача кадров, обеспечиваемая дополнительными средствами. Это снизит информационную скорость передачи информации, и более эффективной в этом случае станет сеть X.25.

Эффективность технологии FR достигается также использованием специфических механизмов, управляющих загрузкой сети. Эти механизмы обеспечивают практически гарантированное время доставки кадров через сеть и одновременно дают возможность сети адаптироваться к крайне неравномерным во времени типам трафика (например, к трафику ЛВС).

Стремительному развитию технологии FR и повышению ее эффективности способствует ряд факторов, в частности улучшение качества каналов связи, использование современного многофункционального каналообразующего оборудования. К новому классу такого оборудования относятся мультимедийные пакетные коммутаторы (МПК), совмещающие несколько функций:

– статистическое уплотнение каналов передачи данных, при котором фиксированные промежутки времени в уплотняемом канале не предоставляются отдельно каждому каналу, как это имеет место при использовании метода временного уплотнения. Информация каждого канала разбивается на отдельные блоки, к блоку прибавляются заголовок и хвост, что образует единицу передачи информации – кадр, с помощью которого могут передаваться все виды трафика. Основные преимущества такого уплотнения: динамическое распределение пропускной способности уплотненного канала связи в зависимости от активности в каналах передачи данных, возможность предоставления пропускной способности по требованию, возможность установки приоритетов для различных видов трафика;

– коммутация и передача различных видов трафика;

– управление потоком информации и установка приоритетов;

– поддержка функций телефонных станций.

К функциям АТС, выполняемым МПК, относятся оцифровка и коммутация голоса, передача факсимильных сообщений. Для технологии FR характерным является возможное увеличение задержки при передаче голоса по сравнению с обычной телефонной сетью. Устранить это явление можно путем установления более высокого приоритета для голосового трафика и применения фрагментации кадров.

Распространению технологии FR способствует также наличие стандартов, обеспечивающих совместимость сетей FR с другими сетями. Например, имеется стандарт IETF 1294 для преобразования пакетов TCP/IP в кадры FR. Есть стандарты, обеспечивающие совместимость FR с самыми высокопроизводительными и современными сетями – сетями ATM. При «входе» в сеть ATM длинные кадры FR разбиваются на короткие, размещаемые внутри ATM-ячеек, а при «выходе» из сети ATM из ячеек ATM-сети извлекаются фрагменты кадров FR, и из них собираются полные кадры FR. В настоящее время за рубежом, особенно в США, наблюдается стремительное развитие сетей FR.

Наиболее распространенные способы доступа к сетям FR:

– использование выделенных линий;

– через сети X.25 по обычным коммутируемым телефонным линиям;

– через ISDN для передачи данных и голоса.

В России большинство сетей передачи данных общего пользования также предоставляют пользователям FR-сервис. Основная проблема с реализацией магистральной сети FR заключается в том, что те магистральные междугородные каналы, которые построены на базе телефонных линий (линий тональной частоты), не обеспечивают необходимое для сети FR качество передачи. Для построения сетей FR самые широкие возможности могут предоставить решения, которые основаны на базе оптоволоконных или спутниковых каналов связи.

Технология FR и в будущем сохранит свои преимущества и актуальность, поскольку она обеспечивает идеальный доступ к высокоскоростной магистральной ATM-сети по низкоскоростным каналам связи. Полезная пропускная способность прикладных протоколов при работе через сети FR зависит от качества ка-

налов и методов восстановления пакетов на уровнях стека, расположенного над протоколом FR. Поэтому сети FR следует применять только на магистральных каналах с волоконно-оптическим кабелем высокого качества.

На величины задержек сеть FR гарантий не дает, что является основной причиной, сдерживающей применение этих сетей для передачи голоса. Тем не менее, многие производители оборудования для сетей FR поддерживают передачу голоса, что обеспечивается присвоением кадрам, переносящим замеры голоса, приоритетов. Магистральные коммутаторы FR должны обслуживать приоритетные кадры в первую очередь. Кроме того, желательно, чтобы сеть FR, передающая кадры с замерами голоса, была недогруженной. При этом в коммутаторах не возникают очереди кадров, и средние задержки в очередях близки к нулевым. Для качественной передачи голоса необходимо также соблюдение еще одного условия – передавать замеры голоса только в кадрах небольших размеров, иначе на качество будут влиять задержки упаковки замеров в кадр, так называемые задержки пакетизации.

10.7. Сети и технологии ATM

Технология ATM (Asynchronous Transfer Mode – режим асинхронной передачи) является одной из самых перспективных технологий построения высокоскоростных сетей. Она была разработана и специфицирована при проектировании ISDN отделом коммуникаций Международного союза по электросвязи. Технология ATM специально ориентирована на работу с информацией различного типа:

– речевым трафиком, традиционно обслуживаемым телефонными сетями;

– трафиком данных, который обычно передается по компьютерным сетям;

– трафиком мультимедиа, сочетающим в себе статические изображения, аудио- и видеоинформацию.

Основные особенности ATM-технологии:

1. ATM – это асинхронная технология, так как пакеты не-

большого размера, называемые ячейками (cells), передаются по сети, не занимая конкретных временных интервалов.

2. Технология АТМ ориентирована на предварительное (перед передачей информации) установление соединения между двумя взаимодействующими пунктами. После установления соединения АТМ-ячейки маршрутизируют сами себя, поскольку каждая ячейка имеет поля, идентифицирующие соединение, к которому она относится.

3. По технологии АТМ допускается совместная передача различных видов сигналов, включая речь, данные, видеосигналы. Достигаемая при этом скорость передачи (от 155 Мбит/с до 2,2 Гбит/с) может быть обеспечена одному пользователю, рабочей группе или всей сети. В АТМ-ячейке не предусматриваются позиции для определенных видов передаваемой информации, поэтому пропускная способность канала регулируется путем выделения полосы пропускания потребителю.

4. Поскольку передаваемая информация разбивается на ячейки фиксированного размера (53 байта), алгоритмы их коммутации реализованы аппаратно, что позволяет устранить задержки, неизбежные при программной реализации коммутации ячеек.

5. АТМ-технология обладает способностью к наращиваемости, т.е. к увеличению размера сети путем каскадного соединения нескольких АТМ-коммутаторов.

6. Построение АТМ-сетей и реализация соответствующих технологий возможны на основе оптоволоконных линий связи, коаксиальных кабелей, неэкранированной витой пары. Однако в качестве стандарта на физические каналы для АТМ выбран стандарт на оптоволоконные каналы связи синхронной цифровой иерархии SDH. Технология мультиплексирования и коммутации, разработанная для SDH, стала АТМ-технологией.

7. АТМ-технологии могут быть реализованы в АТМ-сетях практически любой топологии, но оконечное оборудование пользователей подключается к коммутаторам АТМ индивидуальными линиями по схеме «звезда».

Главное отличие *АТМ-технологии* от других телекоммуникационных технологий заключается в высокой скорости передачи информации (в перспективе – до 10 Гбит/с), причем привязка к какой-либо одной скорости отсутствует. Важным является и то

обстоятельство, что АТМ-сети совмещают функции глобальных и локальных сетей, обеспечивая идеальные условия для «прозрачной» транспортировки различных видов трафика и доступа к услугам и службам взаимодействующих с сетью АТМ-сетей.

АТМ-технология допускает использование как постоянных (PVC), так и коммутируемых виртуальных каналов (SVC). *Постоянные каналы PVC* представляют собой соединение (после предварительной настройки) между взаимодействующими пользователями сети, которое существует постоянно. Устройства, связываемые постоянным виртуальным каналом, должны вести довольно громоздкие таблицы маршрутизации, отслеживающие все соединения в сети. Следовательно, рабочие станции, соединенные PVC, должны иметь таблицы маршрутизации всех остальных станций сети, что нерационально и может вызывать задержки в передаче.

Коммутируемые виртуальные каналы (SVC) позволяют устранить необходимость ведения сложных таблиц маршрутизации и таким образом повысить эффективность функционирования сети. Здесь соединение устанавливается динамически, при этом используются АТМ-маршрутизаторы. В отличие от традиционных маршрутизаторов, которые требуют физического подключения сетевого сегмента к каждому из своих портов, в АТМ-маршрутизаторах используется не физическая архитектура с ориентацией на соединения, а виртуальная сетевая архитектура, ориентированная на протоколы. Такие маршрутизаторы необходимы и удобны для создания виртуальной сети, для которой характерной является возможность переключения пользователей, находящихся в любой точке сети, с одного сегмента на другой с сохранением виртуального адреса рабочей группы, что упрощает администратору сети задачу учета изменений списка пользователей.

АТМ-технология способна обрабатывать трафики четырех классов, представленных в таблице 10.1.

Класс А – синхронный трафик с постоянной скоростью передачи и с предварительным установлением соединения. Протокол, обслуживающий трафик этого класса, предназначен для обеспечения потребностей в сетевых услугах при передаче информации с постоянной скоростью. Таким образом, адресат получает поток

данных с той постоянной скоростью, с какой ее передает отправитель. Службу этого класса можно использовать для передачи аудио- и видеоданных вместо обычной телекоммуникационной связи с коммутацией цепей (т.е. вместо аналогового канала).

Таблица 10.1.

Класс служб	Требования к параметрам потоков данных						Тип сообщения
	Синхронизация		Скорость передачи		Установление соединения		
	да	нет	постоянная	переменная	да	нет	
A	+	–	+	–	+	–	Видеоинформация
B	+	–	–	+	+	–	Аудио- и видеоинформация
C	–	+	–	+	+	–	Цифровые данные
D	–	+	–	+	–	+	Цифровые данные

Класс B – синхронный трафик с переменной скоростью передачи и с предварительным установлением соединения (например, сжатая речь, видеоинформация). Здесь, как и в случае трафика класса A, необходимы синхронизация аппаратуры отправителя и получателя и предварительное установление связи между ними, но допускается переменная скорость передачи. Информация передается через фиксированные промежутки времени, но ее объем в течение сеанса передачи может изменяться. Если объем передаваемой информации превышает фиксированный размер одной ячейки, эта информация разбивается на несколько ячеек, сборка которых осуществляется в пункте назначения. Кроме того, эта служба предусматривает передачу уплотненной (сжатой) аудио- и видеоинформации и может использоваться, например, в видеоконференциях, где при ограниченных задержках изменяющаяся скорость передачи данных считается допустимой.

Класс C – асинхронный трафик с переменной скоростью передачи и с предварительным установлением соединения. Здесь синхронизации аппаратуры отправителями получателя не требуется. Такой способ передачи необходим в сетях с коммутацией пакетов (сети X.25, Интернет). Служба класса C ориентирована на создание соединения, но не поддерживает временные соотношения. Служба этого класса требует создания двухточечного соединения между отправителем и получателем. Пользователь-отправитель передает информацию в сеть в виде пакетов переменного размера, которые получает целевое программное обеспечение пользователя АТМ. Поступающие к целевому пользователю пакеты могут приходить с отличной от исходной скоростью. Эта служба обеспечивает обмен данными подобно обычным компьютерным сетям. Трафик класса C, видимо, станет основным для передачи информации в глобальных сетях.

Класс D – асинхронный трафик с переменной скоростью передачи и без установления соединения. Протокол, управляющий доставкой трафика класса D, разработан для обеспечения многобитовой коммутации данных без установления соединения. В этом протоколе предусматривается использование кадров переменной длины: с помощью передатчика каждый кадр делится на сегменты фиксированного размера, которые помещаются в АТМ-ячейки; приемник собирает сегменты в исходный кадр, завершая, таким образом процесс, который называется сегментацией и сборкой. Каждый передаваемый пакет содержит полные адреса отправителя и получателя. Пакеты могут адресоваться как одному получателю, так и нескольким одновременно (многоадресная рассылка).

Режим асинхронной передачи основан на концепции двух оконечных пунктов сети (АС – абонентских систем, терминалов), осуществляющих связь друг с другом через совокупность промежуточных коммутаторов. При этом используются интерфейсы двух типов: интерфейс пользователя с сетью (UNI) и интерфейс между сетями (NNI). UNI соединяет устройство оконечного пользователя с АТМ-коммутатором, а NNI представляет собой канал связи между двумя АТМ-коммутаторами сети (рис. 10.9).

Соединение между двумя оконечными пунктами сети возникает с того момента, когда один из них передает через UNI запрос

в сеть. Этот запрос через цепочку АТМ-коммутаторов отправляется в пункт назначения для интерпретации. Если узел-адресат принимает запрос на соединение, то в АТМ-сети между двумя пунктами организуется виртуальный канал.

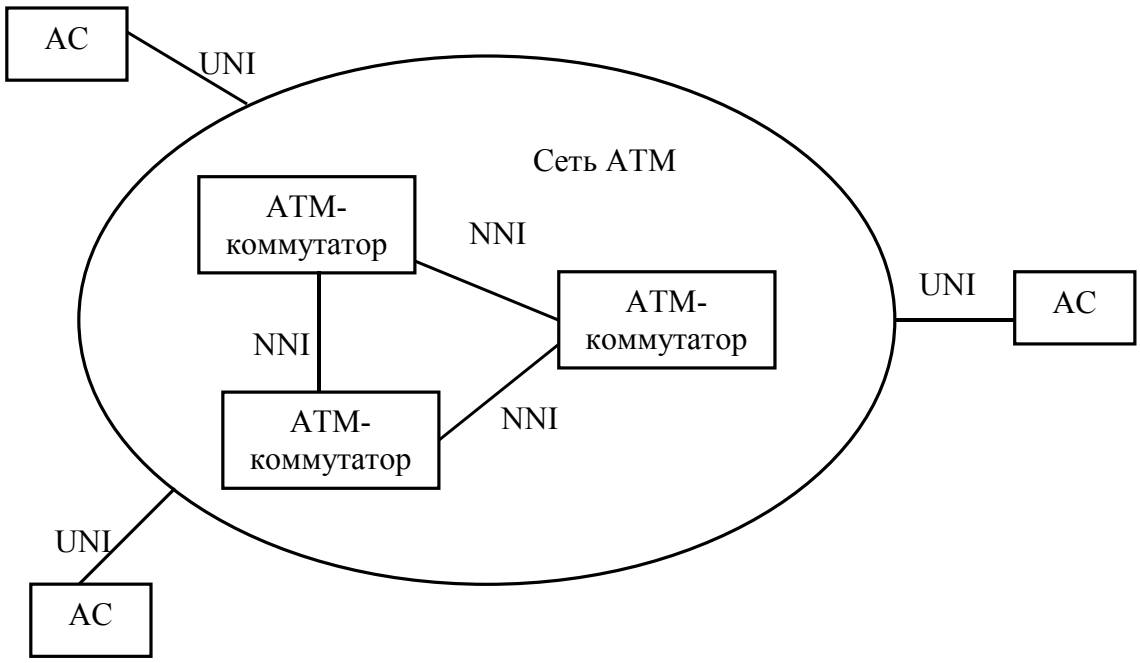


Рис. 10.9. Структура сети АТМ

Движущей силой развития технологии АТМ является ее эффективность в обслуживании низкоскоростных приложений и возможность работы на сравнительно низких скоростях (от 2 Мбит/с). Говорить о «конкуренции» сетей FR и АТМ неправомочно, так как в настоящее время FR является основным интерфейсом доступа к сетям АТМ, позволяющим обеспечивать передачу по сети АТМ разнородного трафика, динамически распределяя полосу пропускания.

Совмещение разнородных телекоммуникационных сетей, построенных на базе различных технологий (X.25, FR, IP и др.), для предоставления пользователям всего спектра услуг в настоящее время возможно только при использовании технологии АТМ.

Технология АТМ реализует коммутацию, ориентированную на аппаратуру, программные средства которой обеспечивают безукоризненное выполнение соединений с неограниченной полосой пропускания для передачи данных, видео- и голосовых сообщений. Технология пакетной коммутации АТМ применяет короткие пакеты фиксированной длины, называемые ячейками (cell). Ячей-

ка АТМ имеет размер 53 байт, пять из которых составляют заголовок, оставшиеся 48 – собственно информацию (рис. 10.10).

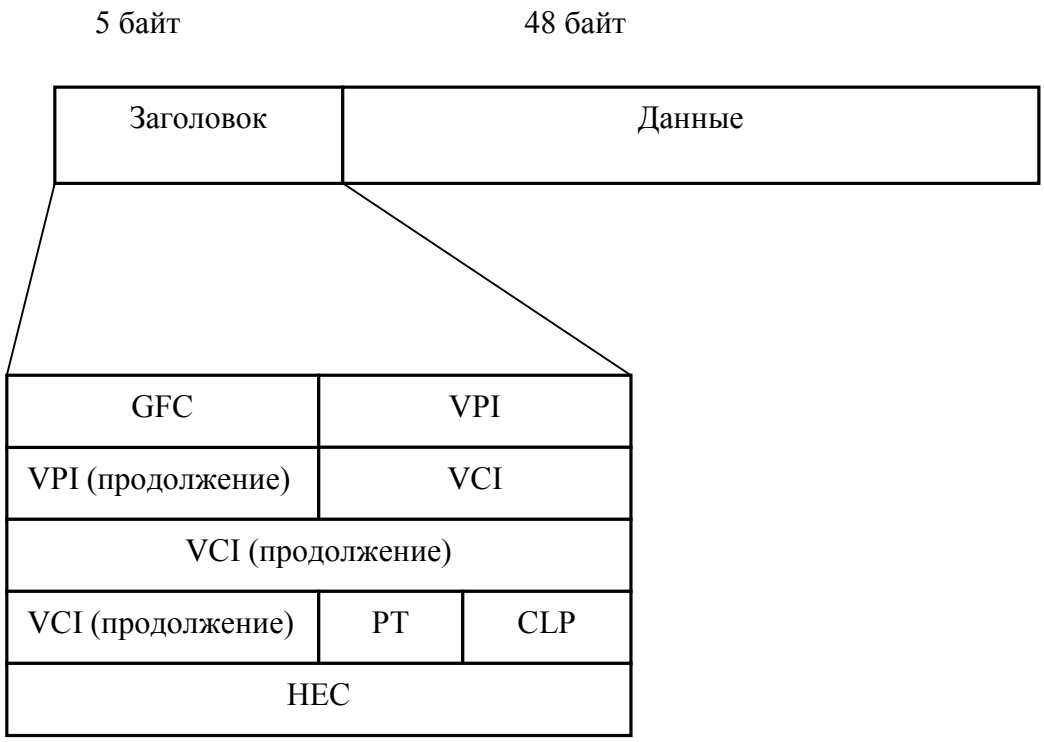


Рис. 10.10. Структура ячейки АТМ

Так как ячейки имеют фиксированную длину, конструкция АТМ-коммутатора более проста, задержки при обработке данных сокращены, дисперсия задержек снижена, что существенно для таких чувствительных к задержкам видам коммуникационного обслуживания, как передача голосовых сообщений и видео.

Поле *управление потоком* (GFC – Generic Flow Control) длиной 4 бит используют только при взаимодействии конечного узла и первого коммутатора сети АТМ.

Поле *идентификатор виртуального пути* (VPI – Virtual Path Identifier) длиной 12 бит используют для группирования виртуальных каналов с целью маршрутизации.

Поле *идентификатор виртуального канала* (VCI – Virtual Channel Identifier) – 16-разрядное, идентифицирует конкретный виртуальный канал в виртуальном пути.

Поле *тип информационного наполнения* (PT – Payload Type) длиной 3 бит, идентифицирует тип данных, содержащихся в поле информационного наполнения. Кроме того, 1 бит этого поля используется для указания перегрузки в сети.

Однобитовое поле *приоритет потери ячейки* (CLP – Cell Loss Priority) позволяет оборудованию ATM определить, какие ячейки нужно отбрасывать в первую очередь при возникновении перегрузки. Ячейки с CLP = 1 являются для сети низкоприоритетными, а ячейки с CLP = 0 – высокоприоритетными.

Поле *контроля ошибок заголовка* (HEC – Header Error Check) содержит значение кода обнаружения и коррекции ошибок.

Поле *данных* ячейки содержит 48 октетов (384 бит) данных пользователя и/или дополнительной управляющей информации.

В заголовке ATM виртуальный канал обозначен комбинацией двух полей – VPI (идентификатор виртуального пути) и VCI (идентификатор виртуального канала). Виртуальный путь используют в случаях, когда два пользователя ATM имеют свои собственные коммутаторы на каждом конце пути и, следовательно, могут организовывать и поддерживать свои виртуальные соединения. Виртуальный путь напоминает канал, содержащий множество кабелей, по каждому из которых может быть организовано виртуальное соединение.

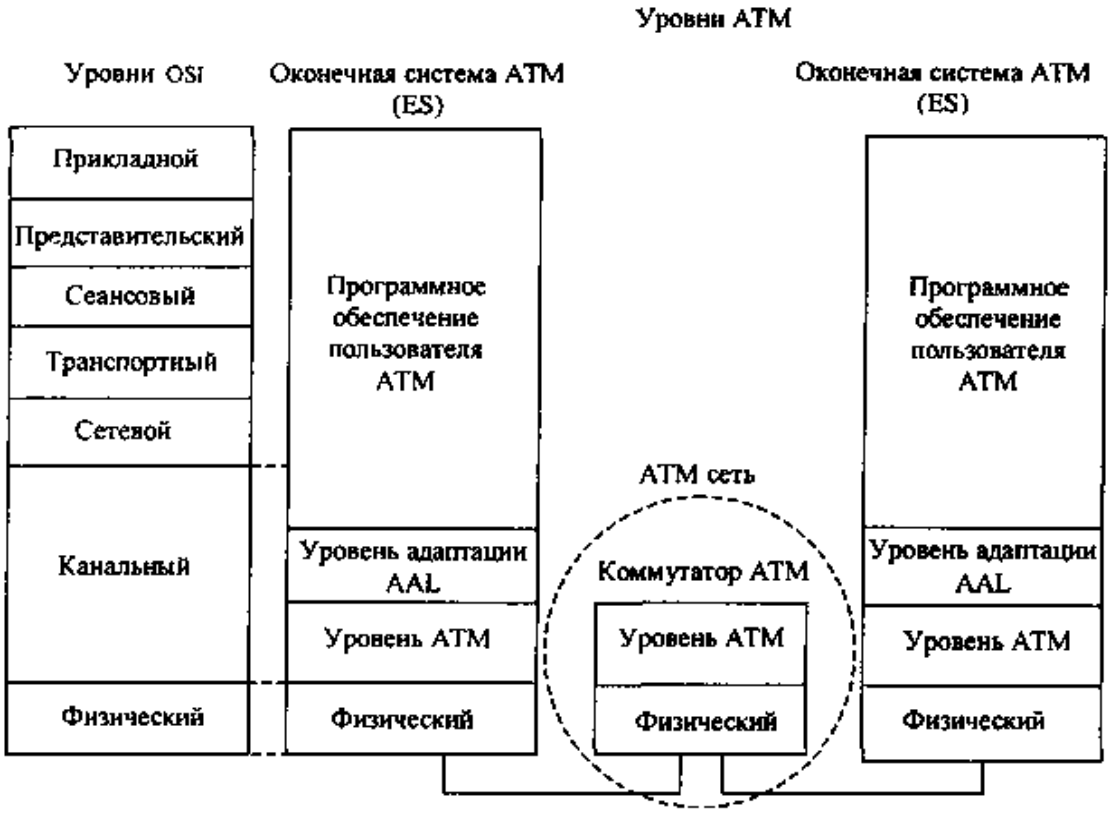


Рис. 10.11. Соответствие уровней ATM модели OSI

Разработчики архитектуры ATM разделили операции, выполняемые в сети устройствами ATM, на три функциональных уровня (рис. 10.11).

Физический уровень отправляет и принимает информацию в виде электрических или оптических сигналов, передаваемых по физическому пути передачи данных. Эта функция физических коммуникаций предусматривает преобразование ячеек в непрерывный поток битов или кадров и обратно, а также предполагает использование различных видов (физического) кодирования и декодирования данных, содержащихся в каждой из ячеек.

Основной функцией *уровня ATM* является коммутация ячеек. На этом уровне устройство ATM принимает ячейки, поступающие по пути передачи данных, определяет путь дальнейшей пересылки, по которому эти ячейки следует ретранслировать, и форматирует заголовок каждой отправляемой ячейки.

Уровень адаптации ATM (AAL) предлагает интерфейс между сетью ATM и пользовательским программным обеспечением ATM, обычно реализуемым в подсистеме сетевого ПО. AAL применяется только в оконечных устройствах, но не в коммутаторах ATM. В оконечном устройстве, играющем роль отправителя, AAL принимает битовый поток от пользовательского программного обеспечения ATM и структурирует его в виде ячеек, подходящих для транспортировки по сети ATM. В принимающем оконечном устройстве ATM соответствующий уровень AAL получает ячейки из сети, воссоздает исходный битовый поток и передает его принимающему пользовательскому ПО.

Для обеспечения совместимости традиционных протоколов и оборудования локальных сетей с технологией ATM была разработана спецификация, называемая LANE (LAN Emulation – эмуляция локальных сетей). Эта спецификация обеспечивает совместную работу сетей Ethernet и ATM на канальном уровне. При этом коммутаторы ATM работают в качестве высокоскоростных коммутаторов магистрали локальной сети, обеспечивая не только скорость, но и гибкость соединений коммутаторов ATM между собой, поддерживающих не только древовидные структуры, но и произвольную топологию связей. В спецификации LANE определен способ преобразования кадров и MAC-адресов технологии Ethernet в ячейки и виртуальные каналы технологии ATM, а так-

же и способ их обратного преобразования. Все действия по преобразованию протоколов выполняют специальные устройства, встраиваемые в обычные коммутаторы Ethernet. Именно поэтому ни коммутаторы ATM, ни рабочие станции сети Ethernet не замечают того, что работа осуществляется с чуждой им технологией. Такая прозрачность была одной из главных целей разработчиков спецификации LANE.

10.8. Сети DWDM

Технология плотного волнового (спектрального) мультиплексирования (Dense Wave Division Multiplexing, DWDM) предназначена для создания оптических магистралей нового поколения, работающих на мультигигабитных и терабитных скоростях. Такой качественный скачок производительности обеспечивает принципиально иной, нежели у SDH, метод мультиплексирования – информация в оптическом волокне передается одновременно большим количеством световых волн. Сети DWDM работают по принципу коммутации каналов, при этом каждая световая волна представляет собой отдельный *спектральный канал.* Каждая волна несет собственную информацию, при этом оборудование DWDM не занимается непосредственно проблемами передачи данных на каждой волне, то есть способом кодирования информации и протоколом ее передачи. Устройства DWDM осуществляют только объединение различных волн в одном световом пучке, а также выделение из пучка каждого спектрального канала. Современное оборудование DWDM позволяет передавать по одному оптическому волокну 32 и более волн разной длины, при этом каждая волна переносит информацию со скоростью 10 Гбит/с. В настоящее время ведутся работы по повышению скорости передачи информации на одной длине волны до 40–80 Гбит/с.

Практический успех технологии DWDM, оборудование которой уже работает на магистралях многих ведущих мировых операторов связи (в том числе, и некоторых российских), во многом определило появление волоконно-оптических усилителей. Эти оптические устройства непосредственно усиливают световые сигналы, исключая необходимость промежуточного преобразо-

вания их в электрическую форму, как это делают регенераторы, применяемые в сетях SDH. Системы электрической регенерации сигналов являются весьма дорогими и, кроме того, протокольно-зависимыми, так как они должны воспринимать определенный вид кодирования сигнала. Оптические усилители, «прозрачно» передающие информацию, позволяют наращивать скорость магистрали без необходимости модернизации усилительных блоков. Протяженность участка между оптическими усилителями может достигать 150 км и более, что обеспечивает экономичность создаваемых магистралей DWDM, в которых длина мультиплексной секции составляет на сегодня 600 – 3000 км при применении от 1 до 7 промежуточных оптических усилителей. Оптические усилители используются не только для увеличения расстояния между мультиплексорами, но и внутри самих мультиплексоров. Если мультиплексирование и кросс-коммутация выполняются исключительно оптическими средствами, без преобразования в электрическую форму, то сигнал при пассивных оптических преобразованиях теряет мощность и его нужно усиливать перед передачей на линию. Новые исследования привели к появлению усилителей, позволяющих нарастить количество одновременно передаваемых длин волн до 80 – 160 и более, то есть обеспечить передачу трафика со скоростями 800 Гбит/с – 1,6 Тбит/с в одном направлении по одному оптическому волокну.

С успехами DWDM связано еще одно перспективное технологическое направление – полностью оптические сети (All-Optical Networks). В таких сетях все операции по мультиплексированию/демультиплексированию, вводу-выводу и кросс-коммутации (маршрутизации) пользовательской информации выполняются без преобразования сигнала из оптической формы в электрическую.

Исключение преобразований в электрическую форму позволяет существенно удешевить сеть, но возможности оптических технологий пока еще недостаточны для создания полностью оптических сетей нужного масштаба, поэтому практическое применение таких сетей ограничено фрагментами, между которыми выполняется электрическая регенерация сигнала. Тем не менее, работы в этом направлении ведутся активно и полностью оптические системы кросскоммутации уже выпускаются.

Ниже перечислены основные преимущества технологии DWDM.

1. Дальнейшее повышение коэффициента использования частотного потенциала оптического волокна и достижение терабитных скоростей.

2. Отличная масштабируемость – повышение суммарной скорости сети за счет добавления новых спектральных каналов без необходимости замены всех магистральных модулей мультиплексоров.

3. Экономическая эффективность за счет отказа от электрической регенерации на участках сети большой протяженности.

4. Независимость от протокола передачи данных – технологическая «прозрачность», позволяющая передавать через магистраль DWDM трафик сетей любого типа.

5. Независимость спектральных каналов друг от друга.

6. Совместимость с технологией SDH – мультиплексоры DWDM оснащаются интерфейсами, способными принимать и передавать данные мультиплексоров SDH.

7. Совместимость с технологиями семейства Ethernet – Gigabit Ethernet.

10.9. Сети IP

Революционный рост популярности Интернета привел к тому, что сегодня практически каждая глобальная сеть должна быть способна передавать трафик протокола IP. А это означает, что сегодня все глобальные сети являются составными сетями IP, а отличия между ними заключаются в лежащих под уровнем IP технологиях. Сети IP изначально были задуманы как экономичные дейтаграммные сети, предоставляющие своим пользователям только услуги типа best effort («доставка по возможности»). Такая сеть старается обработать поступающий трафик как можно быстрее, но при этом никаких гарантий относительно результата усилий не дает. Сервис «с максимальными усилиями» основан на некотором справедливом алгоритме обработки очередей, возникающих при перегрузках сети, когда в течение некоторого времени скорость поступления пакетов в сеть превышает скорость

продвижения этих пакетов. В простейшем случае алгоритм обработки очереди рассматривает пакеты всех потоков как равноправные и продвигает их в порядке поступления. В том случае, когда очередь становится слишком большой (не умещается в буфере), проблема решается простым отбрасыванием вновь поступающих пакетов. В результате классическая составная сеть IP не в состоянии гарантировать своим пользователям качество обслуживания их трафика, если только сеть не работает с очень низким уровнем загрузки, что в большинстве случаев неприемлемо. Процесс же по встраиванию в сети IP механизмов поддержки качества обслуживания пока еще далек от завершения.

Созданию стройной законченной системы поддержки качества обслуживания в рамках протокола IP мешает его дейтаграммная природа. Действительно, неопределенность путей следования пакетов при существовании альтернативных маршрутов равной стоимости не позволяет выполнить точную оценку загруженности каждого ресурса сети, а значит, не позволяет применить в сетях IP методы инжиниринга трафика. Но так как трафик IP сегодня является непременным атрибутом любой сети передачи данных (и некоторых телефонных сетей тоже) и не поддерживать его просто невозможно, то для предоставления качественных услуг большинство крупных глобальных сетей, особенно сетей операторов связи, строится по четырехуровневой схеме (рис. 10.12).

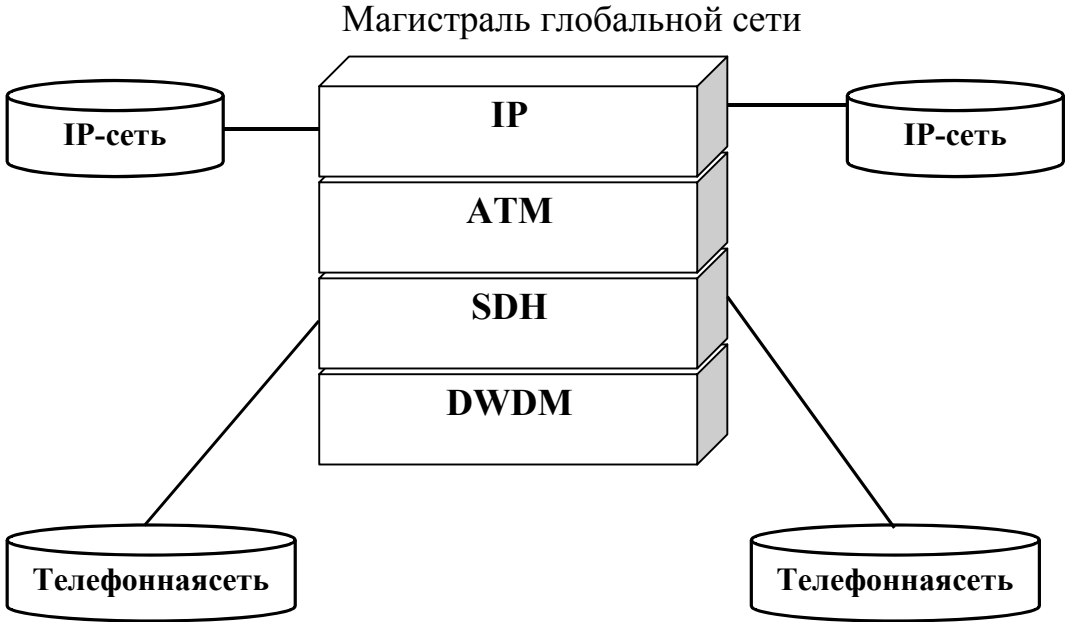


Рис. 10.12.Структура глобальной сети

Два нижних уровня не относятся к собственно пакетным сетям – это уровни первичной сети, с помощью которой оператор сети может достаточно быстро организовать постоянный цифровой канал между точками подключения оборудования вышележащей наложенной сети – пакетной или телефонной. На рисунке первичная сеть представлена двумя уровнями. На нижнем уровне работает наиболее скоростная на сегодняшний день технология DWDM, образующая спектральные скорости 10 Гбит/с и выше. На следующем уровне работает технология SDH, с помощью которой пропускная способность спектральных каналов делится на более мелкие подканалы, связывающие интерфейсы коммутаторов пакетной сети (или телефонных коммутаторов). На рисунке показан наиболее масштабируемый на сегодня вариант построения первичной сети, включающий слои DWDM и SDH. Такое построение сегодня характерно только для наиболее крупных территориальных сетей, покрывающих страны и континенты. Во многих случаях слой DWDM отсутствует, технология SDH тоже применяется не всегда. В самом простом случае первичная сеть для образования постоянных каналов вообще отсутствует, и коммутаторы или маршрутизаторы пакетной сети соединяются непосредственно кабельными или беспроводными линиями связи. Последнее решение хоть и требует меньших начальных затрат, но страдает от недостатка гибкости – чтобы подключить новое устройство, необходимо физически прокладывать новую линию связи.

Третий уровень образован сетью ATM, основным назначением которой является создание инфраструктуры постоянных виртуальных каналов, соединяющих интерфейсы маршрутизаторов IP, работающих на четвертом, верхнем уровне глобальной сети. Для каждого типа трафика образуется отдельный виртуальный канал, обеспечивающий требуемые для трафика параметры качества – среднюю скорость, пульсацию, уровень задержек, уровень потерь. Уровень IP, освобожденный в представленной модели от проблем обеспечения параметров качества, выполняет свои классические функции – образует составную сеть и обеспечивает услуги конечным пользователям, передающим по глобальной сети свой IP-трафик.

Несмотря на сложность многослойной структуры, подобные сети получили большое распространение и для крупных операто-

ров комплексных услуг являются на сегодня фактическим эталоном глобальной сети, с помощью которой можно оказывать комплексные услуги, как IP, так и ATM, классической телефонии и услуги предоставления цифровых каналов в аренду. Тем не менее остаются востребованными и «чистые» сети IP, называемые так из-за того, что под уровнем IP нет другой сети с коммутацией пакетов, такой, как ATM. В такой сети цифровые каналы по-прежнему образуются инфраструктурой двух нижних уровней (DWDM, SDH), а этими каналами непосредственно пользуются интерфейсы маршрутизаторов IP, без какого-либо промежуточного слоя. Некоторые элементы поддержки качества возможны и в такой сети, если на маршрутизаторах активизированы механизмы кондиционирования трафика, контролирующие входящие потоки таким образом, чтобы их интенсивность не превысила заранее оговоренные пределы, а также механизмы управления очередями. Однако маршруты трафика в такой сети выбираются классическими протоколами маршрутизации, а, значит, все пакеты следуют к сетям назначения по кратчайшим маршрутам, то есть не эффективно, поэтому высокого качества обслуживания достичь здесь не удается.

Тем не менее, в тех случаях, когда сеть передает трафик, не чувствительный к задержкам, «чистая» сеть IP может оказаться вполне рациональным решением, к тому же более экономичным и простым в эксплуатации, чем сложная четырехуровневая модель, требующая для своего обслуживания еще и специалистов по технологии ATM. Однако, для того, чтобы маршрутизаторы IP могли использовать цифровые каналы, на этих каналах должен работать какой-либо протокол канального уровня, так как сам канал является устройством физического уровня.

Контрольные вопросы к главе 10

1. Что такое глобальная сеть?
2. Перечислите основных потребителей услуг глобальных сетей.
3. Дайте характеристику режимов передачи данных в глобальных сетях.
4. Опишите основные технологии глобальных сетей.

ГЛАВА 11

КОРПОРАТИВНЫЕ СЕТИ. ЗАЩИТА ИНФОРМАЦИИ В СЕТЯХ

11.1. Общая структура корпоративной сети

Для эффективного управления крупными организациями, имеющими большое количество филиалов или отделов, размещенных в удаленных друг от друга зданиях, строится корпоративная сеть. На основе такой сети формируются информационные связи между локальными сетями центрального офиса, филиалов и подразделений, которые могут находиться на значительном удалении друг от друга (например, в разных городах или странах). Основной функцией любой корпоративной сети является организация оперативного доступа к информации пользователей, где бы они ни находились.

Корпоративная вычислительная сеть – это интегрированная, многомашинная, распределенная система одного предприятия, имеющего территориальную рассредоточенность, состоящая из взаимодействующих локальных сетей структурных подразделений и подсистемы связи для передачи информации.

Корпоративная вычислительная сеть – это сеть на уровне компании (корпорации), в которой используются программные средства на основе протокола TCP/IP и Internet-технологии для решения внутренних задач (Intranet-технологии). Корпоративные сети и информационные системы корпорации основаны на технологии «клиент – сервер». Такие технологии позволяют эффективно решать задачи автоматизации производственной деятель-

ности и управления всей корпорацией, которая может иметь удаленные офисы и филиалы в других городах и даже странах. Корпоративные сети дают возможность предоставлять услуги не только своим сотрудникам, но и внешним пользователям. Использование типовых решений Internet-технологий позволяет относительно дешево построить корпоративную сеть и значительно сократить сроки окупаемости затрат на ее создание, эксплуатацию и модернизацию. Все эти возможности объясняют лавинообразный рост корпоративных сетей, наблюдающийся в последние годы.

Однако, несмотря на все достоинства корпоративных сетей, их эксплуатация ставит ряд достаточно сложных проблем. Одной из главных проблем является обеспечение ее защиты от несанкционированного доступа. Эта задача с каждым годом приобретает все большую актуальность. Умелые действия злоумышленников могут парализовать работу сети и деятельность всей корпорации. Поэтому при проектировании и эксплуатации корпоративных сетей и автоматизированных информационных систем следует особое внимание уделить разработке и внедрению средств обеспечения безопасности. При всей важности и актуальности системы защиты информации на практике этой проблеме уделяется второстепенное значение. Система защиты информации должна способствовать эффективному выполнению основной функции корпоративной сети – оперативному доступу к информации.

Типовая структура корпоративной сети приведена на рис. 11.1.

В общем случае, корпоративная сеть состоит из сети центрального офиса (сеть кампуса), сетей удаленных филиалов (удаленные ЛВС-1, ЛВС-2,…, ЛВС-N), удаленных пользователей (доступ с домашних компьютеров сотрудников, либо малых удаленных офисов) и объединяющей их телекоммуникационной среды. Сеть центрального офиса может состоять из отдельных локальных сетей здания или комплекса зданий (ЛВС-1, ЛВС-2,…, ЛВС-K). В центральной сети находятся основные сервера и хранилища данных корпорации. Как правило, центральные офисы имеют учрежденческие автоматические телефонные станции (АТС).

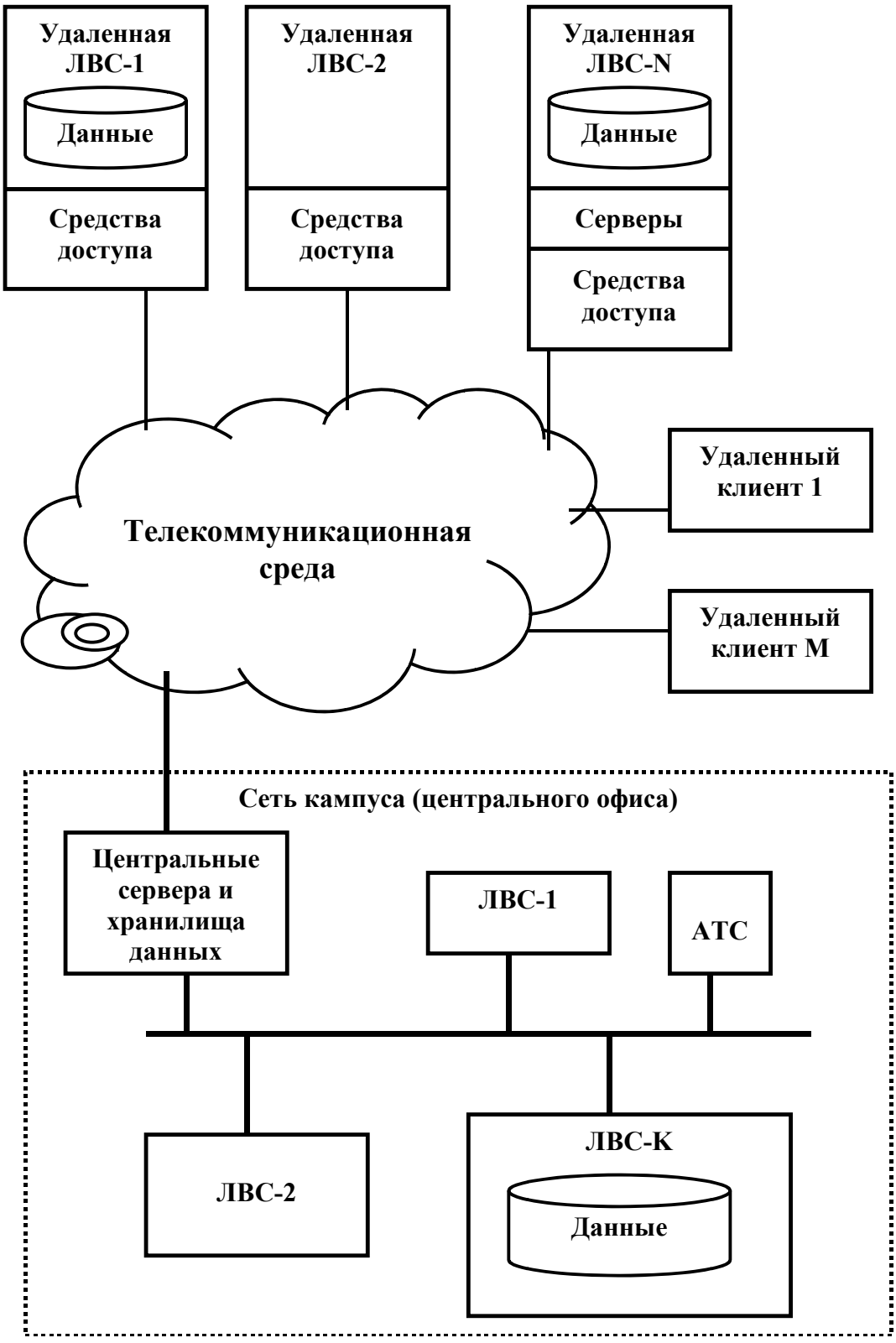


Рис. 11.1.Структура корпоративной сети

Сети удаленных филиалов, в зависимости от размеров, могут иметь свои сервера и хранилища данных, а также средства досту-

па в используемую телекоммуникационную среду для обмена данными с центральным офисом и офисами филиалов. Удаленные персональные компьютеры через телекоммуникационную среду имеют прямую связь с ЛВС центрального офиса, а также ЛВС филиалов. Отдельные удаленные пользователи для выхода в телекоммуникационную среду используют стандартные средства доступа (например, модемы).

Рис. 11.2. Состав корпоративной сети

В качестве промежуточной коммуникационной среды могут быть использованы обычные телефонные сети, выделенные кана-

лы, средства беспроводной связи, а также глобальные, региональные и городские сети (X.25, Frame Relay и др.), позволяющие передавать IP-пакеты. Такие сети являются транспортной средой для передачи информации потребителям. Стек протоколов TCP/IP, благодаря его популярности, фактически стал стандартом для межсетевого взаимодействия. Основным его преимуществом является совместимость. Он позволяет обеспечить совместимость между компьютерами различных типов, а также между локальными и глобальными сетями различных технологий. Кроме того, стек TCP/IP позволяет организовать доступ к информационным ресурсам глобальной сети Интернет.

С точки зрения функционального назначения корпоративная сеть состоит из трех составляющих: технические средства, программное обеспечение, информационные ресурсы (рис. 11.2). Технические средства состоят из рабочих станций пользователей, серверов, хранилищ данных, периферийных устройств, коммуникационного оборудования и линий связи.

Программная часть в свою очередь состоит из общесистемного программного обеспечения и прикладных программных средств, обеспечивающих решение специализированных задач корпорации. В составе системных программных средств можно выделить сетевые операционные системы, системы управления базами данных, стандартные пакеты программ (текстовые процессоры, электронные таблицы и др.), средства телекоммуникаций (средства передачи файлов, браузеры и др.).

Сетевые операционные системы служат для управления работой сети и реализуют принцип сетевой модели «клиент – сервер». Наиболее популярными системами являются Windows NT компании Microsoft и NetWare компании Novell. Система Windows NT для передачи данных использует протоколы TCP/IP или IPX/SPX. Система NetWare позволяет соединять компьютеры в сети типа Ethernet или Token Ring, используя модель «клиент – сервер». Программное обеспечение сервера NetWare выполняется на всех главных компьютерных платформах типа UNIX, DOS, Windows, Macintosh. Для того чтобы компьютер-клиент имел доступ к сети, на нем должно быть установлено программное обеспечение клиента системы NetWare. После этого клиенты могут совместно ис-

пользовать файлы и ресурсы принтеров, а также выполнять ряд различных приложений с помощью сервера.

Информационные ресурсы являются важнейшей и наиболее ценной компонентой, ради которой и строится корпоративная сеть. Корпоративная информация может формироваться из различных источников: ввод с клавиатур рабочих станций, чтение с внешних носителей и периферийных устройств (например, сканеров), генерироваться прикладным программным обеспечением. Кроме того, корпорации могут использовать информационные ресурсы других организаций через сеть Интернет.

Потребителями информационных ресурсов корпоративных сетей могут быть не только свои сотрудники (внутренние пользователи), но и внешние пользователи (физические лица и организации). Под понятием «пользователь корпоративной сети» понимаются зарегистрированные в установленном порядке физические лица или организации, наделенные определенными полномочиями доступа к информации в сети. В рамках своих полномочий пользователи могут осуществлять только разрешенные им действия с использованием общесистемного и прикладного программного обеспечения.

Среди всех пользователей следует выделить технических специалистов, занимающихся обеспечением функционирования корпоративной сети. Администраторы системы занимаются сопровождением системного программного обеспечения, обеспечивают работоспособность сети и контроль за ходом обработки информации. Защитой сети занимаются администраторы безопасности. Разработкой прикладного программного обеспечения занимаются программисты. Указанная категория пользователей осуществляет свои функции со своих специализированных рабочих станций. Они могут иметь ограничения по правам доступа к информации, но, как правило, имеют неограниченные возможности по изменению программного обеспечения и процессов обработки информации.

11.2. Основные принципы проектирования информационных систем

Создание и накопление информационных ресурсов корпорации, а также доступ к ним производится с помощью прикладного программного обеспечения и входящих в его состав специализированных автоматизированных информационных систем (ИС). Анализ опыта разработок автоматизированных информационных систем, их внедрения и функционирования позволил определить следующие принципы, которые должны учитываться при их проектировании.

Принцип открытости. Разрабатываемая ИС должна быть совместима со всеми современными стандартами, поддерживать Internet/Intranet технологии, а также иметь возможность наращивания функциональности. Все рабочие места системы должны функционировать в единой корпоративной сети, по которой происходит обмен информацией, образуя единое информационно-коммуникационное пространство.

Принцип идентичности. Разработка новых, совершенствование уже существующих или внедрение получаемых извне автоматизированных информационных систем различного функционального назначения являются в организационном и общем методологическом планах сходными научно-техническими проблемами. Данный принцип основан на наличии значительного количества общих признаков, определяющих характер построения, особенности функционирования и развития ИС различного масштаба и прикладного назначения. Важная прикладная значимость этого принципа заключается в возможности использования при разработке ИС опыта создания и эксплуатации других автоматизированных систем различного назначения, а также в создании потенциальных условий для обеспечения взаимодействия этих систем, а возможно, и их частичной или полной интеграции.

Непрерывность, поэтапность и преемственность разработки и развития. ИС – постоянно развивающиеся системы. Каждое нововведение служит развитием основных системных принципов и уже достигнутого качества. В новых проектных решениях необходим учет ранее накопленного опыта, а также сохранение всех по-

лезных для дальнейшего использования средств и ресурсов (в первую очередь электронные информационные ресурсы, записанные на машиночитаемых носителях, а также имеющиеся в наличии технические средства). На этапе проектирования невозможно предусмотреть весь круг проблем, связанных с развитием системы. Кроме того, реализация всех задач в полном объеме может быть не только нецелесообразна, но и экономически невозможна. Однако проектные решения должны обеспечить возможность последовательной поэтапной разработки подсистем ИС по мере создания условий для расширения ее функциональных характеристик и структуры без остановки эксплуатации. Необходимость постоянного развития и усложнения системы появляется не только в связи с накоплением опыта и информационных ресурсов, но и под влиянием внешней среды, в частности, требований пользователей, изменений функциональной структуры организации, а также быстрой смены поколений технических и программных средств. Таким образом, развитие системы должно быть предусмотрено уже на начальных стадиях ее проектирования. Это относится к составу решаемых задач, развитию архитектуры системы и ее отдельных подсистем, совершенствованию и наращиванию используемых программных, технических, технологических и других средств.

Адаптивность. Составляющие ИС должны обладать свойствами, обеспечивающими их быструю адаптацию к изменениям внешней среды и новым аппаратно-программным средствам. Адаптивность рассматривается как заложенная в проектные решения возможность перестройки системы или отдельных ее составляющих без остановки эксплуатации ИС, в соответствии с изменениями внешних условий. Такие изменениям могут быть связаны с появлением новых функциональных задач и требований к системе, возникшей необходимостью и возможностью замены морально устаревших программно-технических средств. Система должна допускать использование достаточно широкого спектра оборудования, как в серверной части, так и в клиентской, функционировать в различных сетевых средах и при этом обеспечивать высокую степень защиты своих данных от несанкционированного доступа и разрушения.

Адаптивность в условиях динамично развивающихся информационных технологий является одним из наиболее значитель-

ных требований к проектным решениям и программно-техническим средствам ее обеспечения.

Модульный принцип построения программных и технических средств. Предполагает, что состав указанных средств состоит из блоков (модулей) обеспечивающих возможность их замены или изменения с целью совершенствования функционирования ИС или ее адаптации к новым условиям.

Принцип технологичности. Предполагает единство для всей системы технологии создания, обновления, сохранения и использования информационных ресурсов и однократную обработку информационных документов, а также их многократное и многоцелевое использование.

Принцип корпоративности. При проектировании ИС, входящей в состав системы более высокого уровня, должна быть предусмотрена ее аппаратная, программная, организационная, функциональная и информационно-лингвистическая совместимость с другими системами.

Принцип масштабируемости. Это требование для корпоративных систем, гарантирующее сохранность средств, вложенных в разработку и развитие системы. Все предлагаемые программные и аппаратные решения должны обладать высокой степенью масштабируемости во всех измерениях, в частности по количеству пользователей, объему хранимых данных, интенсивности сетевого обмена данными, скорости обработки информации, набору предоставляемых услуг, способам обеспечения доступа и т.д.

Полная нормализация процессов и их мониторинг. Многоцелевое использование информации ИС требует обеспечения высокой достоверности данных в системе. Для этого на различных этапах обработки и ввода информационных документов необходимо использовать различные формы контроля информации. Постоянный мониторинг необходим также для получения качественных и количественных характеристик функционирования ИС.

Регламентация. ИС ориентированы на функционирование в промышленном режиме, обеспечивающем массовую поточную обработку информационных документов. Эта обработка регламентируется стандартами, маршрутными и пооперационными технологиями, нормативами на ресурсные и временные показатели, развитой службой диспетчеризации.

Экономическая целесообразность. Создание ИС должно предусматривать выбор таких проектных решений (в том числе программных, технических и организационно-технологических), которые при условии достижения поставленных целей и задач обеспечивают минимизацию затрат финансовых, материальных и трудовых ресурсов.

Типизация проектных решений. Разработка и развитие ИС и сетей производится с ориентацией на сотрудничество и взаимодействие с другими организациями отрасли, вышестоящими органами управления, региональными органами контроля и отчетности (налоговые инспекции, различные фонды), а также в соответствии с правилами и протоколами международного информационного обмена.

Максимальное использование готовых решений. Для сокращения стоимости и сроков разработки и внедрения ИС, а также уменьшения ошибок проектирования как системы в целом, так и отдельных ее составляющих, рекомендуется максимально использовать готовые решения и средства. В указанном плане при создании новой системы значительный объем работ связан с анализом альтернативных вариантов предлагаемых решений, выбором наиболее соответствующего для объекта автоматизации и его адаптации к новым условиям применения.

Защита и безопасность данных. Разрабатываемая ИС должна иметь различные средства защиты информации, в частности обеспечивать разграничение прав доступа к данным и функциям в зависимости от должностных обязанностей сотрудников, защиту от несанкционированного доступа и разрушения, безопасность при возникновении внештатных ситуаций, иметь средства резервного копирования.

Ориентация на первых лиц объекта автоматизации. Успешное выполнение работ по созданию автоматизированной системы, ее развитию и эксплуатации возможно только при условии их безусловной поддержки первым лицом объекта автоматизации и закреплении приказом по организации непосредственной ответственности за их выполнение за руководителем на уровне не ниже заместителя руководителя. В подразделениях автоматизируемой организации ответственность за выполнение работ (предпроектное обследование, приемку подсистем, их эксплуатацию)

должна возлагаться в первую очередь на руководителей соответствующих подразделений.

Изложенные принципы проектирования носят общий характер. В каждом конкретном случае разработки ИС могут учитываться и другие принципы, характерные и имеющие большое значение для конкретной предметной области использования.

11.3. Стадии и этапы проектирования ИС

Под проектированием ИС понимается детализированная разработка проекта системы, содержащего полный комплект ее организационной, конструкторской, технологической и эксплуатационной документации. Проектирование автоматизированных информационных систем предполагает выполнение ряда стадий и этапов. Начальным этапом в разработке ИС является изучение структуры организации и анализ основных информационных потоков. Важнейшей составляющей этого этапа является анализ существующей аппаратно-программной и телекоммуникационной инфраструктуры, как наиболее важной системообразующей составляющей.

В России действует система стандартов, определяющих содержание, состав исполнителей и порядок выполнения работ на разных этапах проектирования, а также порядок их приемки. Одновременно сложилась определенная практика проектирования, которая в основных ее положениях не противоречит установленным стандартам и нормативам.

Стандарты ГОСТ 34.601–90 «Автоматизированные системы. Стадии создания», введенные в действие с 01.01.1992 г., предусматривают следующие стадии и этапы проектирования.

1. Формирование требований к АС

1.1. Обследование объекта и обоснование необходимости создания АС.

1.2. Формирование требований пользователей к АС.

1.3. Оформление отчета о выполненной работе и заявки на разработку АС (тактико-технического задания).

2. Разработка концепции АС

2.1. Изучение объекта.

2.2. Проведение необходимых научно-исследовательских работ.

2.3. Разработка вариантов концепции АС и выбор варианта концепции АС, удовлетворяющей пользователя.

2.4. Оформление отчета о выполненной работе.

3. Техническое задание

3.1. Разработка и утверждение технического задания на создание АС.

4. Эскизный проект

4.1. Разработка предварительных проектных решений по системе и ее частям.

4.2. Разработка документации на АС и ее части.

5. Технический проект

5.1. Разработка проектных решений по системе и ее частям

5.2. Разработка документации на АС и ее части.

5.3. Разработка и оформление документации на поставку изделий для комплектования АС и/или технических требований (технических заданий) на их разработку.

5.4. Разработка заданий на проектирование в смежных частях проекта объекта автоматизации.

6. Рабочая документация

6.1. Разработка рабочей документации на систему и ее части.

6.2. Разработка или адаптация программ.

7. Ввод в действие

7.1. Подготовка объекта автоматизации к вводу АС в действие.

7.2. Подготовка персонала.

7.3. Комплектация АС поставляемыми изделиями (программными и техническими средствами, программно-техническими комплексами, информационными изделиями).

7.4. Строительно-монтажные работы.
7.5. Пуско-наладочные работы.
7.6. Проведение предварительных испытаний.
7.7. Проведение опытной эксплуатации.
7.8. Проведение приемочных испытаний.

8. Сопровождение

8.1. Выполнение работ в соответствии с гарантийными обязательствами.
8.2. Послегарантийное обслуживание.

В стандарте указывается также, что:

– стадии и этапы, выполняемые организациями – участниками работ по созданию АС, устанавливаются в договорах и техническом задании на основе настоящего стандарта;

– допускается исключать стадию «Эскизный проект» и отдельные этапы работ на всех стадиях, объединять стадии «Технический проект» и «Рабочая документация» в одну стадию «Технорабочий проект». В зависимости от специфики создаваемых АС и условий их создания допускается выполнять отдельные этапы работ до завершения предшествующих стадий, а также параллельное во времени выполнение этапов работ, включение новых этапов.

В приложениях к данному стандарту подробно расписаны:

– содержание работ по стадиям и этапам проектирования;

– перечень видов организаций, участвующих в работах.

Существуют также и другие государственные стандарты, регламентирующие различные аспекты проектирования АС, среди которых следует указать:

ГОСТ 34.602-89 «Техническое задание на создание автоматизированной системы». Введены с 01.01.90 г.;

ГОСТ 34.603-92 «Виды испытаний АС». Введены с 01.01.93 г.

В соответствии с имеющимся в России опытом проектирование ИС различного назначения и сложности, как правило, включает в себя четыре этапа (стадии) выполнения работ: предпроектное обследование объекта автоматизации, концептуальное, эскизное, техническое и рабочее проектирование. В отдельных случаях некоторые стадии проектирования, например, эскизного и

технического проектирования или технического и рабочего проектирования, полностью или частично объединяются. Как следует из примечаний к ГОСТ 34.601-90, такое объединение не противоречит установленным нормам. В самом общем плане содержание работ на разных стадиях может быть сведено к следующему:

1. **При предпроектном обследовании объекта автоматизации** производится сбор и обработка сведений об организации и особенностях функционирования объекта автоматизации, включая данные о его взаимодействии с внешней средой и другими объектами, а также выполнение системного анализа, разработку технико-экономического обоснования целесообразности автоматизации и выработку общих требований на разработку автоматизированной системы.

2. **При концептуальном проектировании** производится разработка *аванпроекта (пилотного проекта)* или программы создания системы, которая включает:

– краткую характеристику исходного состояния объекта автоматизации и среды, в которой он функционирует;

– указание основных целей и перечень задач автоматизации;

– описание укрупненной организационно-функциональной структуры выбранного варианта (или вариантов) построения создаваемой системы;

– технико-экономическое обоснование;

– укрупненное описание и основные требования к средствам информационного и лингвистического обеспечения;

– перечень и общие требования к средствам программно-аппаратного обеспечения и системам телекоммуникаций;

– перечень и укрупненную характеристику этапов создания системы, сроки их выполнения;

– исходную оценку стоимостных показателей выполнения работ;

– техническое задание на систему в целом и/или ее основные составные части (подсистемы, программно-технические комплексы и средства, отдельные задачи и т.д.) В соответствии с ГОСТ 34.601–90 данная работа может быть выделена в отдельную стадию или этап проектирования.

3. **При эскизном проектировании** производится разработка *эскизного проекта*, который содержит принципиальные конструкторские и схемные решения объекта разработки, а также данные, определяющие его назначение и основные параметры (при проектировании программного обеспечения системы эскизный проект должен содержать полную спецификацию разрабатываемых программ).

4. **При техническом проектировании** производится разработка *технического проекта*, содержащего принципиальные электрические схемы и конструкторскую документацию объекта разработки и составных его частей, перечень выбранных готовых средств программного и технического обеспечения (в том числе типов ЭВМ, операционной системы, прикладных программ и т.д.), алгоритмов решения задач для разработки новых средств программного обеспечения и т.п.

5. **При рабочем проектировании**, представляющем собой заключительный этап собственно проектирования, производится окончательное уточнение и детализация результатов предыдущих этапов, создание и испытания опытного и/или опытно-промышленного образца объекта автоматизации, разработка и отработка программных продуктов, технологической и эксплуатационной документации. Результаты этого этапа излагаются в рабочем или технорабочем проекте. В современной практике проектирования автоматизированных информационных систем он является начальным этапом их внедрения в работу организации.

11.4. Необходимость защиты информации в информационных системах и сетях

Появление локальных и глобальных сетей передачи данных предоставило пользователям компьютеров новые возможности оперативного обмена информацией. Развитие новых информационных технологий и всеобщая компьютеризация привели к тому, что информационная безопасность становится не только обязательной, она является одной из характеристик ИС и сетей передачи данных. Существует довольно обширный класс систем об-

работки информации, при разработке которых фактор безопасности играет первостепенную роль (например, банковские информационные системы).

Многочисленные публикации последних лет показывают, что злоупотребления информацией, циркулирующей в ИС или передаваемой по каналам связи, совершенствуются не менее интенсивно, чем меры защиты от них. В настоящее время для обеспечения защиты информации требуется не просто разработка частных механизмов защиты, а реализация системного подхода, включающего комплекс взаимосвязанных мер (использование специальных технических и программных средств, организационных мероприятий, нормативно-правовых актов, морально-этических мер противодействия и т.д.). Поэтому обеспечение информационной безопасности компьютерных систем и сетей является одним из ведущих направлений развития информационных технологий.

Сегодня можно утверждать, что рождается новая современная технология – технология защиты информации в компьютерных информационных системах и сетях передачи данных. Реализация этой технологии требует увеличивающихся расходов и усилий. Однако все это позволит избежать значительно превосходящих потерь и ущерба, которые могут возникнуть при реальном осуществлении угроз информационным системам и сетям.

По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышается зависимость общества от степени безопасности используемых им информационных технологий. Обеспечение безопасности корпоративных сетей предполагает организацию противодействия любому несанкционированному вторжению в процесс их функционирования, а также попыткам модификации, хищения, вывода из строя или разрушения ее компонентов, то есть защиту всех компонентов сети: аппаратных средств, программного обеспечения, данных и персонала.

Актуальность и важность проблемы обеспечения информационной безопасности обусловлена следующими факторами:

– высокие темпы роста парка персональных компьютеров, применяемых в самых разных сферах деятельности, и как следствие, резкое расширение круга пользователей, имеющих непо-

средственный доступ к вычислительным сетям и информационным ресурсам;

– увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью компьютеров и других средств автоматизации;

– бурное развитие аппаратно-программных средств и технологий, не удовлетворяющих современным требованиям безопасности;

– несоответствие бурного развития средств обработки информации и проработки теории информационной безопасности, разработки международных стандартов и правовых норм, обеспечивающих необходимый уровень защиты информации;

– повсеместное распространение сетевых технологий, объединение локальных сетей в глобальные, создание единого информационно-коммуникационного мирового пространства на базе сети Интернет, которая по своей идеологии не обеспечивает достаточной информационной безопасности.

Ежегодно в мире растет количество правонарушений в информационной сфере. Соответственно растет и размер ущерба, нанесенного злоумышленниками.

Об остроте проблемы защиты информации, ярко выраженной тенденции роста неправомерных действий в информационной сфере и вызванного ими ущерба свидетельствуют следующие данные 90-х годов. Ежегодные потери от компьютерной преступности в США в начале 90-х годов оценивались в 100 млрд. долларов, в странах Западной Европы – в 30 млрд. долларов. В середине 90-х годов преступления, совершаемые в информационных корпоративных сетях, увеличились в среднем в два раза, при этом фирмы ежегодно расходовали примерно 6 млрд. долларов на обеспечение безопасности своих информационных сетей. Согласно статистическим данным 1997 г. более 40 % компаний и агентств несли финансовые убытки из-за недостаточного обеспечения безопасности информации.

Одним из беспрецедентных компьютерных преступлений в последние годы стал взлом многослойной защиты компьютерной системы банка «Ситибэнк» (США, Нью-Йорк). Российский гражданин В. Левин с 30 июня по 3 октября 1994 г., находясь в г. Санкт Петербурге и используя обычный персональный компью-

тер и электронную связь, сделал не менее 40 незаконных переводов на общую сумму более 10 млн долларов со счетов различных клиентов «Ситибэнка» на счета действующих с ним в заговоре лиц или контролируемых ими фирм.

В 1995 г. в России было выявлено около 200 электронных преступлений, связанных с изъятием денег при помощи пластиковых карточек и с хищениями путем внедрения в телекоммуникационные сети банков. По данным Главного управления специальных технических мероприятий МВД России (Управления «К») в 2004 году в России было зафиксировано 13 тысяч компьютерных преступлений: от незаконного взлома и доступа к компьютерам (около 2/3 преступлений) до мошенничества в области пластиковых карт и мобильных телефонов (www. internet. ru).

В ноябре 1988 г. сетевой вирус-червь, написанный студентом последнего курса Корнельского университета Р. Моррисом, в течение двух суток инфицировал более 6000 компьютерных систем (включая системы НАСА, Агентства национальной безопасности США, десятков университетов и академических центров) и практически парализовал их работу. Общий ущерб от вируса Морриса был оценен в 96 млн. долларов. В начале 90-х годов сработавшая программа-вирус типа «логической бомбы», на двое суток остановила главный конвейер Волжского автомобильного завода. В 1992 г. в мире было зафиксировано более 300 различных вирусов, а в 1997 г. уже было известно от 10 до 15 тыс. вирусов. При этом каждый месяц в среднем обнаруживалось около 200 новых вирусов. 2000 г. стал годом рождения почтовых вирусов, в частности самого быстро распространяющегося вируса «I Love You». В отдельных странах поражению им подверглось от 30 до 80 % компьютерных сетей. Убытки от его действия оцениваются в 10 млрд. долларов. Сообщается (данные 2001 г.) о свободном хождении в глобальных сетях около 50 тыс. вирусов и ежедневном появлении почти 500 новых.

С 29 марта по 8 апреля 2005 года в Москве прошел международный форум по обеспечению информационной безопасности, на котором присутствовали ведущие эксперты более чем из 50 стран. В программу форума входили три мероприятия: международный симпозиум по кибербезопасности, международная конференция по обеспечению безопасности при использовании ин-

фокоммуникационных систем, заседание исследовательской комиссии Международного союза электросвязи (МСЭ-Т) по информационной безопасности. Особый статус и важность проблем подтверждаются участием в форуме министра информационных технологий и связи РФ, министра внутренних дел РФ, директора МСЭ-Т, директора Европейского агентства по сетевой и информационной безопасности.

Участники форума отметили следующие важные положения:

1. Системы обеспечения безопасности должны рассматриваться как неотъемлемая составная часть информационно-телекоммуникационных систем.

2. Вопросы обеспечения информационной безопасности являются комплексными. Их решение требует объединения усилий и организации согласованных мероприятий со стороны органов государственной власти, силовых структур, научных учреждений, операторских компаний.

3. Для согласованного развития нормативных, юридических, технологических и организационных элементов эффективной инфраструктуры кибербезопасности важным фактором становится международное сотрудничество.

Участники форума выделили следующие основные направления совершенствования информационно-коммуникационных систем и информационной безопасности в России:

1. Образование под руководством Мининформсвязи РФ отраслевого Координационного совета по сетевой и информационной безопасности с целью содействия созданию единой защищенной информационно-телекоммуникационной инфраструктуры России, координации деятельности организаций в области обеспечения сетевой и информационной безопасности.

2. Дальнейшее совершенствование законодательства в сфере обеспечения информационной безопасности, разработка единого правового понятийного аппарата, подходов к правовому регулированию в сфере информационной безопасности, правоприменительной практики.

3. Консолидация усилий операторов связи и правоохранительных органов по оперативному реагированию на действия злоумышленников. Необходимость административного определения базового уровня обеспечения безопасности операторами

связи и принятием его в качестве одного из условий операторской деятельности.

4. Обеспечение дальнейшего развития теории информационной безопасности инфокоммуникационных систем.

5. Подготовка специалистов в области современных информационных технологий и технологий обеспечения информационной безопасности.

11.5. Основные понятия информационной безопасности

Основные термины и определения в области защиты информации даны в ГОСТ Р 50922-96 «Защита информации. Основные термины и определения».

Защита информации – это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий нарушителя на защищаемую информацию.

Под **информационной безопасностью** понимают состояние защищенности обрабатываемых, хранимых и передаваемых данных от незаконного ознакомления, преобразования и уничтожения, а также состояние защищенности информационных ресурсов от воздействий, направленных на нарушение их работоспособности.

Под **безопасностью информационной системы** понимается ее защищенность от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, от попыток несанкционированного получения информации, модификации или физического разрушения ее компонентов. Природа воздействий на ИС может быть самой разнообразной. Это и попытки проникновения злоумышленников, и ошибки персонала, и выход из строя аппаратных и программных средств, стихийные бедствия.

В последние годы понятие «информационная безопасность» распространилось и на такие объекты, как сложные организационно-технические системы, имеющие информационные компоненты (информационную среду), и собственно информационные системы (ИС) и телекоммуникационные сети (ТС). В ИС и ТС

основными объектами защиты выступают информационные ресурсы и информационная инфраструктура, образующие их информационную среду. Другими словами, защищенность информационной системы или корпоративной сети (КС) достигается принятием мер как по обеспечению безопасности (конфиденциальности, целостности и доступности) информации, так и по доступности и целостности компонентов и ресурсов системы (сети), т.е. ее информационной среды как совокупности информационных ресурсов и информационной инфраструктуры. И в этом смысле можно говорить об обеспечении информационной безопасности корпоративной сети.

Информационная безопасность корпоративной сети представляет собой состояние защищенности циркулирующей в ней информации (информационных ресурсов) и информационной инфраструктуры (совокупность информационных систем, локальных сетей и сетей передачи данных), которое обеспечивает устойчивое функционирование сети в условиях действия дестабилизирующих факторов (угроз). Важное отличие проблемы обеспечения информационной безопасности ИС или КС от проблемы защиты информации состоит также в необходимости наряду с задачами защиты информации и информационной инфраструктуры решать и другие дополнительные задачи. Это задачи, связанные с обнаружением и преодолением последствий преднамеренного воздействия злоумышленника на информационную сферу ИС (КС), нарушающих процесс функционирования ИС (КС).

Информационная безопасность компьютерных систем и сетей достигается принятием комплекса мер по обеспечению конфиденциальности, целостности, доступности информационных ресурсов и компонентов системы или сети.

Конфиденциальность информации – это ее свойство быть доступной только ограниченному кругу субъектов информационной системы, в которой циркулирует данная информация (пользователям, процессам, программам). Для остальных субъектов системы информация должна быть неизвестной.

Под **целостностью информации** понимается ее свойство сохранять свою структуру и/или содержание в процессе передачи, использования и хранения. Целостность информации обеспечивается в том случае, если данные в системе не отличаются в се-

мантическом отношении от данных в исходных документах, то есть если не произошло их случайного или преднамеренного искажения или разрушения.

Доступность информации – это свойство системы (сети) обеспечивать своевременный беспрепятственный доступ авторизованных субъектов к интересующей их информации или осуществлять своевременный информационный обмен между ними.

Достоверность информации – свойство, выражаемое в строгой принадлежности информации субъекту, который является ее источником, либо тому субъекту, от которого она принята.

Субъект – это активный компонент системы, который может стать причиной образования потока информации от объекта к субъекту или изменения состояния системы. Объект – пассивный компонент системы, хранящий, принимающий или передающий информацию. Доступ к объекту означает доступ к содержащейся в нем информации.

Под доступом к информации понимается прием, ознакомление с информацией и ее обработка, в частности копирование, модификация или уничтожение. Различают санкционированный и несанкционированный доступ к информации.

Санкционированный доступ к информации – это доступ, не нарушающий установленные правила разграничения доступа. Правила разграничения доступа служат для регламентации права доступа к компонентам системы.

Несанкционированный доступ (НСД) характеризуется нарушением установленных правил разграничения доступа. Пользователь, программа или процесс, осуществляющие несанкционированный доступ к информации, являются нарушителями таких правил разграничения доступа. Несанкционированный доступ является наиболее распространенным видом компьютерных нарушений.

Целостность ресурса или компонента системы – это его свойство быть неизменным в семантическом смысле при функционировании системы в условиях случайных или преднамеренных искажений либо разрушающих воздействий.

Применение при межсетевом взаимодействии открытых каналов передачи данных создает потенциальную угрозу проникновения злоумышленников. Если пассивный нарушитель только про-

сматривает доступные ему сообщения, то активный наряду с прослушиванием может перехватывать, искажать и уничтожать их. Поэтому одной из важных задач обеспечения информационной безопасности при межсетевом взаимодействии является использование методов и средств, позволяющих одной стороне убедиться в подлинности другой стороны.

С допуском к информации и ресурсам системы (сети) связана группа таких понятий, как идентификация, аутентификация, авторизация. С каждым зарегистрированным субъектом системы (сети) связывают некоторую информацию, однозначно идентифицирующую субъект. Эта информация является идентификатором субъекта системы (сети). Субъект, имеющий зарегистрированный идентификатор, считается законным (легальным).

Идентификация субъекта – это процедура распознавания субъекта по его идентификатору (имени), которая выполняется при попытке субъекта войти в систему (сеть). Эта функция выполняется в первую очередь, когда пользователь делает попытку войти в сеть. Он сообщает системе по ее запросу свой идентификатор, и система проверяет в своей базе данных его наличие.

Аутентификация субъекта – это проверка подлинности субъекта с данным идентификатором. Процедура аутентификации устанавливает, является ли субъект именно тем, кем он себя объявил. При проведении аутентификации проверяющая сторона убеждается в подлинности проверяемой стороны, при этом проверяемая сторона тоже активно участвует в процессе обмена информацией. Обычно пользователь подтверждает свою идентификацию, вводя в систему уникальную, не известную другим пользователям информацию о себе (например, пароль или сертификат).

Идентификация и аутентификация – взаимосвязанные процессы распознавания и проверки подлинности субъектов (пользователей). Именно от них зависит решение системы, можно ли разрешить доступ к ресурсам системы конкретному пользователю или процессу. После того как субъект идентифицирован и аутентифицирован, выполняется его авторизация.

При защите каналов передачи данных выполняется *взаимная аутентификация субъектов*, то есть взаимное подтверждение подлинности субъектов, связывающихся между собой по линиям связи. Процедура подтверждения подлинности выполняется

обычно в начале сеанса при установлении соединения абонентов; термин «соединение» указывает на логическую связь (потенциально двустороннюю) между двумя субъектами сети. Цель данной процедуры – обеспечить уверенность, что соединение установлено с законным субъектом и вся информация дойдет до места назначения.

Авторизация субъекта – это процедура предоставления законному субъекту, успешно прошедшему идентификацию и аутентификацию, соответствующих полномочий и доступных ресурсов системы (сети).

Под **угрозой безопасности** для системы (сети) понимаются возможные воздействия, которые прямо или косвенно могут нанести ущерб ее безопасности.

Ущерб безопасности подразумевает нарушение состояния защищенности информации, содержащейся и обрабатывающейся в системе (сети) или самой системы или сети.

Уязвимость системы (сети) – это любая характеристика компьютерной системы, использование которой может привести к реализации угрозы.

Атака на компьютерную систему (сеть) – это действие, предпринимаемое злоумышленником с целью поиска и использования той или иной уязвимости системы. Таким образом, атака – это реализация угрозы безопасности. Противодействие угрозам безопасности – цель, которую призваны выполнить средства защиты компьютерных систем и сетей.

Политика безопасности – это совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты компьютерной системы (сети) от заданного множества угроз безопасности.

Политика безопасности регламентирует эффективную работу средств защиты корпоративной сети. Она охватывает все особенности процесса обработки информации, определяя поведение системы в различных ситуациях. Политика безопасности реализуется посредством комплексного применения административно-организационных мер, физических мер и программно-аппаратных средств и определяет архитектуру системы защиты. Для конкретной организации политика безопасности должна носить индивидуальный характер и зависеть от конкретной техно-

логии обработки информации и используемых программных и технических средств.

Политика безопасности зависит от способа управления доступом, определяющего порядок доступа к объектам системы. Различают два основных вида политики безопасности: избирательную и полномочную.

Избирательная политика безопасности основана на избирательном способе управления доступом. Он характеризуется задаваемым администратором множеством разрешенных отношений доступа (например, в виде троек <объект, субъект, тип доступа>). Обычно для описания свойств избирательного управления доступом применяют математическую модель на основе матрицы доступа, в которой столбец соответствует объекту системы, а строка – субъекту. На пересечении столбца и строки указывается тип разрешенного доступа субъекта к объекту. Обычно выделяют такие типы, как «доступ на чтение», «доступ на запись», «доступ на исполнение» и т.п.

Полномочная политика безопасности основана на полномочном (мандатном) способе управления доступом. Она заключается в совокупности правил предоставления доступа, базирующихся на множестве атрибутов безопасности субъектов и объектов, например в зависимости от метки конфиденциальности информации и уровня допуска пользователя. Полномочное управление доступом подразумевает, что:

– все субъекты и объекты системы однозначно идентифицированы;

– каждому объекту системы присвоена метка конфиденциальности, определяющая ценность содержащейся в нем информации;

– каждому субъекту системы присвоен некий уровень допуска, определяющий максимальное значение метки конфиденциальности информации объектов, к которым субъект имеет доступ.

Чем важнее объект, тем выше его метка конфиденциальности. Поэтому самыми защищенными оказываются объекты с наиболее высокими значениями метки конфиденциальности.

Основным назначением полномочной политики безопасности являются регулирование доступа субъектов системы к объектам с различными уровнями конфиденциальности, предотвращение

утечки информации с верхних уровней должностной иерархии на нижние, а также блокирование возможных проникновений с нижних уровней на верхние. При этом полномочная политика может функционировать на фоне избирательной, придавая ее требованиям иерархически упорядоченный характер в соответствии с уровнями безопасности.

11.6. Проблемы защиты информации в IP-сетях

11.6.1. Виды атак в IP-сетях

Повсеместное распространение стека протоколов TCP/IP и использование технологий Intranet обнажило слабые стороны IP-сетей. Создавая свое детище, архитекторы стека TCP/IP не видели причин особенно беспокоиться о защите сетей, строящихся на его основе. Они и не предполагали, что когда-нибудь отсутствие эффективных средств защиты станет основным фактором, сдерживающим применение протоколов TCP/IP.

Остановимся на более подробном рассмотрении важных проблем недостаточной информационной безопасности протоколов TCP/IP, IP-сетей и служб Internet. Эти пороки являются «врожденными» практически для всех протоколов стека TCP/IP и служб Internet. Большая часть этих проблем связана с исторической зависимостью Internet от операционной системы UNIX. Сеть ARPANET строилась как сеть, связывающая исследовательские центры, научные, военные и правительственные учреждения, крупные университеты США. Эти структуры использовали операционную систему UNIX в качестве платформы для коммуникаций и решения собственных задач. Поэтому особенности методологии программирования в среде UNIX и ее архитектуры наложили отпечаток на реализацию протоколов обмена TCP/IP и политики безопасности в сети. Из-за открытости и распространенности система UNIX оказалась любимой добычей хакеров. Поэтому не удивительно, что и набор протоколов TCP/ IP имеет «врожденные» недостатки защиты.

На практике IP-сети уязвимы для ряда способов несанкционированного вторжения в процесс обмена данными. По мере развития компьютерных и сетевых технологий список возможных типов сетевых атак на IP-сети постоянно расширяется. На сегодняшний день наиболее распространенными являются следующие варианты атак:

1. **Подслушивание**. Большинство данных передается по компьютерным сетям в незащищенном формате (открытым текстом), что позволяет злоумышленнику, получившему доступ к линиям передачи информации вашей сети, подслушивать или считывать трафик. Подслушивание в компьютерных сетях называется слежением (sniffing). Если не использовать служб, обеспечивающих устойчивое шифрование, то передаваемые по сети данные будут доступны для чтения. Для подслушивания в компьютерных сетях могут использоваться так называемые, снифферы пакетов. Сниффер пакетов представляет собой прикладную программу, перехватывающую все сетевые пакеты, которые передаются через определенный домен. Некоторые сетевые приложения передают данные в текстовом формате (Telnet, FTP, SMTP и т.д.), и с помощью сниффера можно узнать полезную, а иногда и конфиденциальную информацию (например, имена пользователей и пароли).

2. **Парольные атаки**. Хакеры могут проводить парольные атаки с помощью целого ряда методов, таких, как IP-спуфинг и сниффинг пакетов, атака полного перебора (brute force attack), «троянский конь». Перехват паролей и имен пользователей, передаваемых по сети в незашифрованной форме, путем «подслушивания» канала (password sniffing) создает большую опасность, так как пользователи часто применяют один и тот же логин и пароль для множества приложений и систем. Многие пользователи вообще имеют один пароль для доступа ко всем ресурсам и приложениям. Если приложение работает в режиме «клиент – сервер», а аутентификационные данные передаются по сети в читаемом текстовом формате, эту информацию с большой вероятностью можно использовать для доступа к другим корпоративным или внешним ресурсам. Хотя логин и пароль часто можно получить при помощи IP-спуфинга и сниффинга пакетов, хакеры часто пытаются подобрать пароль и логин, используя для этого мно-

гочисленные попытки доступа. Часто для атаки полного перебора используется специальная программа, которая дает возможность получить доступ к ресурсу общего пользования (например, к серверу). В результате хакер допускается к ресурсам на правах обычного пользователя, пароль которого был подобран. Если этот пользователь имеет значительные привилегии доступа, хакер может создать себе «проход» для будущего доступа.

3. **Изменение данных**. Злоумышленник, получивший возможность прочитать ваши данные, сможет сделать и следующий шаг – изменить их. Данные в пакете могут быть изменены, даже когда нарушитель ничего не знает ни об отправителе, ни о получателе. Если пользователь и не нуждается в строгой конфиденциальности передаваемой информации, наверняка он не захочет, чтобы его данные были изменены по пути.

4. **«Угаданный ключ»**. Ключ представляет собой код или число, необходимое для расшифровки защищенной информации. Хотя узнать ключ доступа трудно и требуются большие затраты ресурсов, тем не менее это возможно. Ключ, к которому получает доступ атакующий, называется скомпрометированным. Атакующий использует скомпрометированный ключ для получения доступа к защищенным передаваемым данным без ведома отправителя и получателя. Ключ дает право расшифровывать и изменять данные, а также вычислять другие ключи, которые могут дать атакующему доступ и к другим защищенным соединениям.

5. **Подмена доверенного субъекта**. Большая часть сетей и операционных систем используют IP-адрес компьютера для того, чтобы определять, тот ли это адресат, который нужен. В некоторых случаях возможно некорректное присвоение IP-адреса (подмена IP-адреса отправителя другим адресом) – такой способ атаки называют фальсификацией адреса (IP spoofing). IP-спуфинг происходит, когда хакер, находящийся внутри корпорации или вне ее, выдает себя за санкционированного пользователя. Это можно сделать двумя способами. Во-первых, нарушитель может воспользоваться IP-адресом, находящимся в пределах диапазона санкционированных IP-адресов, или авторизованным внешним адресом, которому разрешается доступ к определенным сетевым ресурсам. Хакер может применять специальные программы, формирующие IP-пакеты таким образом, чтобы они

выглядели как исходящие с разрешенных внутренних адресов корпоративной сети.

После получения доступа к вашей сети с разрешенным адресом атакующий может изменять, перенаправлять или удалять ваши данные. Атаки IP-спуфинга часто являются отправной точкой для других атак. Обычно IP-спуфинг ограничивается вставкой ложной информации или вредоносных команд в обычный поток данных, передаваемых между клиентским и серверным приложением или по каналу связи между одноранговыми устройствами. Для двусторонней связи хакер должен изменить все таблицы маршрутизации, чтобы направить трафик на ложный IP-адрес. Если нарушителю это удается, он получает все пакеты и может отвечать на них так, будто является санкционированным пользователем.

6. **Перехват сеанса**. Для осуществления перехвата сеанса по окончании начальной процедуры аутентификации хакер переключает установленное соединение, скажем, с почтовым сервером, на новый хост, а исходному серверу выдается команда разорвать соединение. В результате ваш «собеседник» оказывается незаметно подмененным. После получения доступа к сети злоумышленник получает большую свободу действий. Он может:

– посылать некорректные данные приложениям и сетевым службам, что приводит к их аварийному завершению или неправильному функционированию;

– наводнить компьютер или всю сеть трафиком, пока не произойдет останов системы в связи с перегрузкой;

– блокировать трафик, что приведет к потере доступа авторизованных пользователей к сетевым ресурсам.

7. **Посредничество**. Атака типа «посредничество» подразумевает активное подслушивание, перехват и управление передаваемыми данными невидимым промежуточным узлом. Когда компьютеры взаимодействуют на низких сетевых уровнях, они не всегда могут определить, с кем именно обмениваются данными.

8. **Посредничество в обмене незашифрованными ключами**. Если атаки предыдущих типов увенчались успехом, их автор может вмешаться в процесс передачи ключей между сторонами и подставить им собственный ключ для дальнейшего использования. Вообще для атаки такого типа хакеру нужен доступ к пакетам, передаваемым по сети. Такой доступ ко всем пакетам, пере-

даваемым от провайдера в любую другую сеть, может, к примеру, получить сотрудник этого провайдера. Для атак этого типа часто используются снифферы пакетов, транспортные протоколы и протоколы маршрутизации. Атаки проводятся с целью кражи информации, перехвата текущей сессии и получения доступа к частным сетевым ресурсам, для анализа трафика и получения информации о сети и ее пользователях, искажения передаваемых данных и ввода несанкционированной информации в сетевые сессии.

9. **«Отказ в обслуживании»**. Атаки типа «отказ в обслуживании» являются наиболее известной формой хакерских атак. Эти атаки не нацелены на получение доступа к вашей сети или к какой-либо информации из нее. Атака делает вашу сеть недоступной для обычного использования за счет превышения допустимых пределов функционирования сети, операционной системы или приложения. В случае использования некоторых серверных приложений (таких как Web- или FTP-сервер) такие атаки могут заключаться в том, чтобы занять все соединения, доступные для этих приложений, и держать их в занятом состоянии, не допуская обслуживания пользователей. В ходе атак могут использоваться обычные Internet-протоколы, например TCP и ICMP. Большинство таких атак опирается на общие слабости системной архитектуры.

Некоторые атаки сводят к нулю производительность сети, переполняя ее нежелательными и ненужными пакетами или сообщая ложную информацию о текущем состоянии сетевых ресурсов. Если атака этого типа проводится одновременно через множество устройств, ее называют распределенной атакой. Среди хакеров подобные атаки считаются тривиальными, потому что для их организации требуется минимум знаний и умений. Тем не менее, именно простота реализации и огромный причиняемый вред от этих атак привлекают к ним пристальное внимание администраторов, отвечающих за сетевую безопасность. Против атак такого типа трудно создать стопроцентную защиту. Их нелегко предотвратить, так как для этого требуется четкая координация действий с провайдером.

10. **Атаки на уровне приложений**. Такие атаки могут проводиться несколькими способами. Самый распространенный из них состоит в использовании слабостей серверного программного обеспечения (Sendmail, HTTP, FTP). В результате хакеры могут

получить доступ к компьютеру от имени пользователя, работающего с приложением (обычно это не простой пользователь, а привилегированный администратор с правами системного доступа). Сведения об атаках на уровне приложений широко публикуются, чтобы дать возможность администраторам предотвратить их с помощью коррекционных модулей (патчей). Однако многие хакеры также имеют доступ к этим сведениям, что позволяет им учиться.

Главная проблема с атаками на уровне приложений состоит в том, что они часто пользуются портами, которым разрешен проход через межсетевой экран. К примеру, хакер, эксплуатирующий известную слабость Web-сервера, часто использует в ходе атаки TCP-порт 80. Поскольку Web-сервер открывает пользователям Web-страницы, межсетевой экран должен предоставлять доступ к этому порту. Межсетевой экран рассматривает такую атаку как стандартный трафик для порта 80. Полностью исключить атаки на уровне приложений невозможно. Хакеры постоянно обнаруживают все новые уязвимые места прикладных программ и публикуют в Internet информацию о них. Поэтому очень важно организовать хорошее системное администрирование сети.

11. **Злоупотребление доверием**. Этот тип действий не является в полном смысле атакой. Такие действия представляют собой злонамеренное использование отношений доверия, существующих в сети. Классическим примером такого злоупотребления является ситуация в периферийной части корпоративной сети. В этом сегменте часто располагаются серверы DNS, SMTP и HTTP. Поскольку все они принадлежат к одному и тому же сегменту, взлом одного из них приводит к взлому и всех остальных, так как эти серверы доверяют другим системам своей сети. В качестве другого примера приведем систему, установленную с внешней стороны межсетевого экрана и имеющую отношения доверия с системой, расположенной с его внутренней стороны. В случае взлома внешней системы хакер может использовать отношения доверия для проникновения в систему, защищенную межсетевым экраном. Риск злоупотребления доверием можно уменьшить за счет более жесткого контроля уровней доверия в пределах сети. Системы, расположенные с внешней стороны межсетевого экрана, не должны пользоваться абсолютным доверием со стороны защищенных экраном систем. Отношения доверия должны огра-

ничиваться определенными протоколами и аутентифицироваться не только по IP-адресам, но и по другим параметрам.

12. **Вирусы и приложения типа «троянский конь».** Рабочие станции конечных пользователей уязвимы для вирусов и «троянских коней». Вирусами называются вредоносные программы, которые внедряются в другие программы для выполнения определенной нежелательной функции на рабочей станции конечного пользователя. В качестве примера можно привести вирус, который прописывается в файле command. com и удаляет другие файлы, а также заражает все найденные им версии command. com. «Троянский конь» представляет собой не программную вставку, а настоящую программу, которая выглядит как полезное приложение, на деле выполняя разрушительную акцию. Примером типичного «троянского коня» является программа, которая кажется обычной игрой для рабочей станции пользователя. Однако пока пользователь играет в эту «игру», вредоносная программа отправляет свою копию по электронной почте каждому абоненту, занесенному в адресную книгу пользователя. Все абоненты получают по почте «игру» и невольно способствуют ее дальнейшему распространению.

Борьба с вирусами и «троянскими конями» ведется с помощью эффективного антивирусного программного обеспечения, работающего на пользовательском или сетевом уровне. Антивирусные средства способны обнаружить большинство вирусов и «троянских коней» и пресечь их распространение. Регулярное получение и использование самой свежей информации о вирусах помогает эффективно бороться с ними. По мере появления очередных вирусов и «троянских коней» необходимо устанавливать новые версии антивирусных средств и приложений;

13. **Сетевая разведка**. Сетевой разведкой называется сбор информации о сети с помощью общедоступных данных и приложений. При подготовке атаки против какой-либо сети хакер, как правило, пытается получить о ней как можно больше информации. Сетевая разведка проводится в форме запросов DNS, эхо-тестирования и сканирования портов. Запросы DNS помогают понять, кто владеет тем или иным доменом и какие адреса этому домену присвоены. Эхо-тестирование адресов, раскрытых с помощью DNS, позволяет увидеть, какие хосты реально работают в

данной среде. Получив список хостов, хакер использует средства сканирования портов, чтобы составить полный список услуг, поддерживаемых этими хостами. И наконец, «разведчик» анализирует характеристики приложений, работающих на хостах. В результате добывается информация, которую можно использовать для реализации атаки.

11.6.2. Причины уязвимости IP-сетей

Все перечисленные выше атаки возможны в силу ряда причин:

1. Аутентификация отправителя осуществляется исключительно по его IP-адресу.

2. Процедура аутентификации выполняется только на стадии установления соединения, и в дальнейшем подлинность принимаемых пакетов не проверяется.

3. Важнейшие данные, имеющие отношение к системе, передаются по сети в незашифрованном виде.

Ряд распространенных служб Internet также характеризуется «врожденными слабостями». К числу таких служб относятся:

– простой протокол передачи электронной почты SMTP;

– программа электронной почты Sendmail;

– служба сетевых имен DNS;

– служба эмуляции удаленного терминала Telnet;

– всемирная паутина WWW;

– протокол передачи файлов FTP и др.

Простой протокол передачи электронной почты SMTP позволяет осуществлять почтовую транспортную службу Internet. Одна из проблем безопасности, связанная с этим протоколом, заключается в том, что пользователь не может проверить адрес отправителя в заголовке электронного письма. В результате хакер способен направить во внутреннюю сеть большое количество почтовых сообщений, что приведет к перегрузке и блокированию работы почтового сервера.

Популярная в Internet программа электронной почты Sendmail использует для работы некоторую сетевую информацию – IP-адрес отправителя. Перехватывая сообщения, отправляемые с помощью Sendmail, хакер может употребить эту информацию для нападений, например для спуфинга (подмены адресов).

Протокол передачи файлов FTP обеспечивает передачу текстовых и двоичных файлов, поэтому его часто используют в Internet для организации совместного доступа к информации. Его обычно рассматривают как один из методов работы с удаленными сетями. На FTP-серверах хранятся различные документы, программы другие виды информации. К данным этих файлов на FTP-серверах нельзя обратиться напрямую. Это можно сделать, только переписав их целиком с FTP-сервера на локальный сервер. Некоторые FTP-серверы ограничивают доступ пользователей к своим архивам данных с помощью пароля, другие же предоставляют свободный доступ (так называемый анонимный FTP-сервер). При использовании опции анонимного FTP для своего сервера пользователь должен быть уверен, что на нем хранятся только файлы, предназначенные для свободного распространения.

Служба сетевых имен DNS представляет собой распределенную базу данных, которая преобразует имена пользователей и хостов в IP-адреса, указываемые в заголовках пакетов, и наоборот. DNS также хранит информацию о структуре сети компании, например о количестве компьютеров с IP-адресами в каждом домене. Одна из проблем DNS заключается в том, что эту базу данных очень трудно «скрыть» от неавторизированных пользователей. В результате DNS часто используется хакерами как источник информации об именах доверенных хостов.

Служба эмуляции удаленного терминала Telnet употребляется для подключения к удаленным системам, присоединенным к сети. Она применяет базовые возможности эмуляции терминала. При использовании этого сервиса Internet пользователи должны регистрироваться на сервере Telnet, вводя свои имя и пароль. После аутентификации пользователя его рабочая станция функционирует в режиме «тупого» терминала, подключенного к внешнему хосту. С этого терминала пользователь может вводить команды, которые обеспечивают ему доступ к файлам и запуск программ. Подключившись к серверу Telnet, хакер может сконфигурировать его программу таким образом, чтобы она записывала имена и пароли пользователей.

Всемирная паутина WWW – это система, основанная на сетевых приложениях, которые позволяют пользователям просматри-

вать содержимое различных серверов в Internet или Intranet сетях. Самое полезное свойство WWW – использование гипертекстовых документов, в которые встроены ссылки на другие документы и Web-узлы, что дает посетителям сайтов возможность легко переходить от одного узла к другому. Однако это же свойство является и наиболее слабым местом системы WWW, поскольку ссылки на Web-узлы, хранящиеся в гипертекстовых документах, содержат информацию о том, как осуществляется доступ к соответствующим узлам. Используя эту информацию, хакеры могут разрушить Web-узел или получить доступ к хранящейся в нем конфиденциальной информации.

Рассмотрим основные причины уязвимости сети Internet. Это позволит лучше понять уязвимость сетей и отдельных компьютеров, имеющих доступ к Internet:

1. Сеть Internet разрабатывалась как открытая и децентрализованная сеть с изначальным отсутствием политики безопасности. При этом основные усилия были направлены на достижение удобства обмена информацией в Internet. Кроме того, многие сети спроектированы без механизмов контроля доступа со стороны Internet.

2. Для Internet характерны большая протяженность линий связи и уязвимость основных служб. Сервисные программы базового набора протоколов TCP/IP сети Internet не гарантируют безопасности.

3. Модель «клиент – сервер», на которой основана работа в Internet, не лишена определенных слабостей и лазеек в продуктах отдельных производителей. Данная модель объединяет разнообразное программное и аппаратное обеспечение, в котором могут быть «дыры» для проникновения злоумышленников.

4. При создании Web-страниц ряд компаний использует собственный дизайн, который может не соответствовать требованиям обеспечения определенного класса безопасности для Web-узла компании и связанной с ним локальной или корпоративной сети.

5. Информация о существующих и используемых средствах защиты доступна пользователям. Кроме того, возможна утечка технологий безопасности высокого уровня из секретных источников при вскрытии представленных в сети Web-узлов и сетей организаций, занимающихся разработкой этих технологий.

6. Существует возможность наблюдения за каналами передачи данных, поскольку значительная часть информации передается через Internet в открытой незащищенной форме. В частности, электронная почта, пароли и вложенные в письма файлы могут быть легко перехвачены злоумышленником при помощи доступных программ.

7. Средства управления доступом сложно конфигурировать, настраивать и контролировать. Это приводит к неправильной конфигурации средств защиты и, как следствие, к несанкционированному доступу.

8. Существенную роль играет и человеческий фактор. Отдельные пользователи, не отличающиеся высокими моральными принципами, могут за соответствующую плату предоставить злоумышленникам доступ в сеть своей фирмы. Имеются пользователи-дилетанты, которые, не обладая необходимыми знаниями, считают, что средства защиты им вообще не нужны, или неправильно конфигурируют эти средства.

9. Для обслуживания работы в Internet используется большое число сервисов, информационных служб и сетевых протоколов. Знание правильности и тонкостей использования хотя бы большинства этих сервисов, служб и протоколов одному человеку в лице администратора сети практически недоступно.

10. Специалисты по защите информации в Internet готовятся пока в недостаточном объеме и часто в роли администраторов сети работают люди, не имеющие глубокой профессиональной подготовки.

11. Для работы в Internet характерна кажущаяся анонимность. Существует потенциальная возможность обойти средства обнаружения отправителя той или иной информации либо посетителя того или иного Web-узла с помощью использования виртуальных IP-адресов и промежуточных пересыльщиков электронной почты.

Возникает естественный вопрос: сколько потенциально уязвимых мест может быть у сетей, подключенных к Internet? Специалисты компании Internet Security Systems считают, что в любой сети, основанной на протоколе TCP/IP, существует около 135 потенциальных каналов для несанкционированного доступа.

Первые средства защиты передаваемых данных появились практически сразу после того, как уязвимость IP-сетей дала о се-

бе знать на практике. Характерными примерами разработок в этой области могут служить PGP/Web-of-Trust для шифрования сообщений электронной почты, SSL для защиты Web-трафика, SSH (Secure SHell) для защиты сеансов Telnet и процедур передачи файлов. Общим недостатком подобных широко распространенных решений является их «привязанность» к определенному типу приложений, а значит, неспособность удовлетворить тем разнообразным требованиям к системам сетевой защиты, которые предъявляют крупные корпорации или Internet-провайдеры.

Самый радикальный способ преодолеть указанное ограничение сводится к тому, чтобы строить систему защиты не для отдельных классов приложений (пусть и весьма популярных), а для сети в целом. Применительно к IP-сетям это означает, что системы защиты должны действовать на сетевом уровне модели OSI. Преимущество такого выбора заключается в том очевидном факте, что в IP-сетях именно данный уровень отличается наибольшей гомогенностью: независимо от вышележащих протоколов, физической среды передачи и технологии канального уровня транспортировка данных по сети не может быть произведена в обход протокола IP. Поэтому реализация защиты сети на третьем уровне автоматически гарантирует как минимум такую же степень защиты всех сетевых приложений. При этом не требуется какая-либо модификация последних. Для пользователей процедуры защиты окажутся столь же прозрачными, как и сам протокол IP.

Слабые стороны стека протоколов TCP/IP первоначально предполагалось восполнить в шестой версии протокола IP. В 1993 году в составе консорциума IETF была создана рабочая группа IP Security Working Group, занявшаяся разработкой архитектуры и протоколов для шифрования данных, передаваемых по сетям IPv6. Однако по мере продвижения в этом направлении становилось все очевиднее, что разработки, изначально ориентированные на IP шестой версии, могут пригодиться и в более традиционной среде IPv4. В результате на свет появился набор протоколов IPSec, основанных на современных технологиях шифрования и электронной цифровой подписи данных. Поскольку архитектура протоколов IPSec совместима с протоколом IPv4, ее поддержку достаточно обеспечить на обоих концах соединения.

11.7. Модель информационной безопасности

Процесс формирования глобального информационного общества привел не только к качественному изменению способов хранения и обработки информации, но и сделал ее одним из ценнейших товаров. В настоящее время информация представляет собой стратегический ресурс, лежащий в основе национального богатства государств с развитыми информационными технологиями. Именно «интеллектуалоемкость» информационных технологий позволяет странам, не обладающим достаточными природными ресурсами, поставлять на мировой рынок информационные услуги, продукты, технологии. С другой стороны, развитие компьютерных сетей и информационных технологий вызвало резкое увеличение нарушений авторских прав владельцев информации и все возрастающий размах информационного пиратства. В связи с этим проблема обеспечения информационной безопасности и защита информационных систем и сетей от несанкционированного доступа приобрела в настоящее время особую актуальность и становится одной из самых острых в современной информатике.

В соответствии со статьей 20 Федерального закона «Об информации, информатизации и защите информации» целями защиты в области информационных процессов являются:

– предотвращение утечки, хищения, утраты, искажения, подделки информации;

– предотвращение угроз безопасности личности, общества, государства;

– предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;

– предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;

– защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;

– сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;

– обеспечение прав субъектов в информационных процессах при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Понятие информационной безопасности в российской юридической терминологии не является до сих пор устоявшимся по причине отсутствия единого методологического основания, на базе которого могут быть определены его сущность, степень необходимости использования и границы применения. С методологической точки зрения при анализе проблем информационной безопасности необходимо выявить субъекты информационных отношений и их интересы, связанные с использованием информационных систем, определить задачи по защите информации, основные угрозы безопасности и возможные средства защиты от них. Таким образом, необходима многомерная модель информационной безопасности. В литературе по защите информации описаны различные варианты моделей, с разной степенью точности отражающие все многообразие форм воздействия на информацию.

Проблемы информационной безопасности существенно зависят от типа информационных систем и сферы их применения. В локальных системах малого масштаба систему защиты построить гораздо проще, чем в системах распределенного типа. Это объясняется особенностями информационных систем распределенного типа, основными из которых являются:

– территориальная разнесенность компонентов системы и как следствие наличие обмена информацией между ними;

– широкий спектр способов представления, хранения и передачи информации;

– интеграция данных различного назначения, принадлежащих разным субъектам, в единых базах данных и наоборот, размещение необходимых некоторым субъектам данных в различных узлах сети;

– использование режимов распределенной обработки данных;

– одновременное участие в процессах обработки информации большого количества пользователей с разными правами доступа и обслуживающего персонала различных категорий;

– использование разнородных программно-технических средств обработки и систем телекоммуникаций.

Структурная модель информационной безопасности систем распределенного типа представима в виде схемы, изображенной на рисунке 11.3.

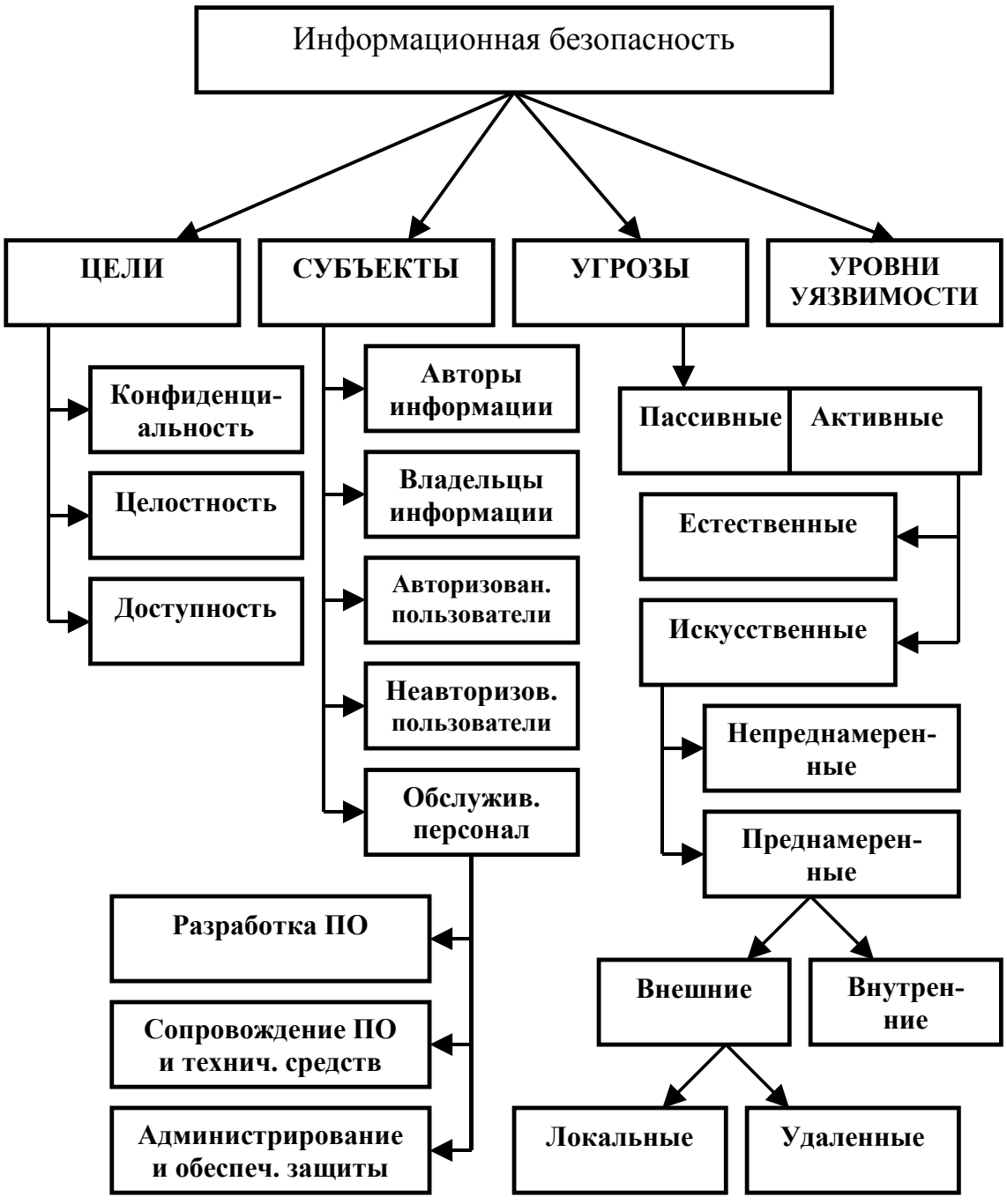


Рис. 11.3. Структурная модель информационной безопасности

Решение проблемы безопасности в информационных системах распределенного типа заключается в анализе следующих основных компонент:

1. Определение основных целей защиты информации.
2. Выявление субъектов информационных процессов.
3. Классификация основных возможных угроз безопасности.
4. Определение уровней уязвимости.

Обеспечение безопасности информации состоит в достижении трех взаимосвязанных целей: конфиденциальность, целостность и доступность.

Задача по обеспечению конфиденциальности состоит в защите информации в процессе ее создания, хранения, обработки и обмена от ознакомления с ней лицами, не имеющими права доступа к ней (неавторизованные пользователи). Кроме того, каждый авторизованный пользователь системы должен иметь доступ только к той части информации, на которую он имеет разрешение.

Задача по обеспечению целостности состоит в защите от преднамеренного или непреднамеренного изменения информации и алгоритмов ее обработки лицами, не имеющими на то права. Наиболее эффективными средствами обеспечения целостности информации являются аутентификация (проверка подлинности по содержанию, источнику, времени создания и т.п.) и идентификация (проверки подлинности сторон в процессе информационного обмена).

Обеспечение доступности состоит в предоставлении пользователям всей имеющейся в системе информации в соответствии с установленными им правами доступа.

Основными субъектами в информационных процессах являются: авторы информационных ресурсов, владельцы информации, авторизованные пользователи, неавторизованные лица (лица, пытающиеся получить самовольный доступ к информации – «хакеры»), отдельные сотрудники или коллективы, участвующие в разработке и обеспечении работоспособности программно-технических средств и средств защиты, администраторы системы (сети и баз данных), а также персонал, занимающийся наполнением системы информацией. Системы защиты должны обеспечивать авторские права владельцам информации и предоставлять доступ к информации пользователям в соответствии с их права-

ми. Кроме того, возможны каналы утечки информации, заложенные разработчиками информационной системы и известные только им.

Персонал, занимающийся сопровождением программно-технических средств, администрированием сети, обеспечением защиты и информационным наполнением, также представляет определенную угрозу несанкционированных утечек. В этом случае система защиты должна располагать соответствующими законодательными и нормативно-правовыми актами на уровне государства и организационными мероприятиями на уровне учреждения.

Под угрозой безопасности информационным системам понимается потенциально возможное действие, событие или процесс, которые посредством воздействия на информацию и другие компоненты системы может нанести ущерб интересам субъектов. Прежде всего, по результатам воздействия угрозы бывают пассивные и активные.

Пассивные угрозы направлены в основном на несанкционированное использование информационных ресурсов сети, не оказывая при этом влияния на ее функционирование. Например, несанкционированный доступ к базам данных, прослушивание каналов связи и т.д.

Активные угрозы имеют целью нарушение нормального функционирования ИС путем целенаправленного воздействия на ее компоненты. К активным угрозам относятся, например, вывод из строя компьютера или его операционной системы, искажение сведений в базах данных, разрушение программного обеспечения, нарушение работы линий связи и т.д. Источником активных угроз могут быть действия взломщиков, вредоносные программы и т.п.

Угрозы безопасности на первом уровне классификации могут быть разделены на естественные и искусственные.

Естественные угрозы – это угрозы, вызванные воздействием на информационные системы и сети объективных физических процессов или стихийных природных явлений, не зависящих от человека. Естественными угрозами безопасности являются, например, стихийные бедствия, аварии, внезапные отключения электропитания, поломки технических средств и другие не зависящие от человека воздействия. Эти угрозы совершенно не под-

даются прогнозированию, и поэтому меры их парирования должны применяться всегда. Стихийные источники, составляющие потенциальные угрозы информационной безопасности, как правило, являются внешними по отношению к рассматриваемому объекту, и под ними понимаются, прежде всего, природные катаклизмы. Эти угрозы опасны для всех элементов корпоративной сети и могут привести к нарушениям нормальной работы, разрушению системы защиты, уничтожению информации, разрушению аппаратно-программных средств и линий связи.

Искусственные угрозы вызваны действиями человека (антропогенные) и подразделяются на непреднамеренные (случайные) и преднамеренные. Данная группа угроз самая обширная. Она представляет наибольший интерес с точки зрения организации защиты, так как действия субъекта всегда можно оценить, спрогнозировать и принять адекватные меры. Методы противодействия этим угрозам управляемы и в основном зависят от организаторов защиты информации.

Непреднамеренные угрозы связаны с людьми, непосредственно работающими с компьютерной системой (действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, но без злого умысла). Они вызваны случайными действиями пользователей, ошибками операторов, программистов, управленческого персонала, сотрудников архивной службы и службы безопасности и ведут к искажению или уничтожению информации, нарушению функционирования, управления и безопасности системы.

Основными непреднамеренными угрозами являются следующие:

– неквалифицированные действия обслуживающего персонала, повлекшие разрушение аппаратно-программных средств и информационных ресурсов;

– неумышленная порча носителей информации, оборудования и каналов связи;

– ошибки, допущенные в процессе проектирования системы;

– заражение рабочих станций вирусами;

– игнорирование персоналом организационно-технологических ограничений, повлекшее разглашение конфиденциальной информации и паролей;

– ввод ошибочной информации.

Преднамеренные искусственные угрозы делятся на внутренние (со стороны персонала организации) и внешние (от посторонних лиц и организаций). По зарубежной и отечественной статистике до 70–80% всех компьютерных преступлений связано с внутренними нарушениями, т.е. осуществляются сотрудниками своей компании. Это обусловлено тем, что свой сотрудник может реально оценить стоимость той или иной информации. Кроме того, некоторые сотрудники обладают привилегиями по доступу к информации в сети и могут их использовать в корыстных интересах.

В свою очередь внешние угрозы подразделяются на локальные (проникновение посторонних лиц в учреждение и доступ их к системе) и удаленные (незаконный доступ к системе через глобальные сети).

Корпоративные сети отличаются тем, что, наряду с обычными (локальными) атаками, осуществляемыми в пределах одной компьютерной системы, к ним применим специфический вид атак, обусловленный распределенностью ресурсов в информационном пространстве. Сетевые (или удаленные) атаки характерны, во-первых тем, что злоумышленник может находиться за тысячи километров от атакуемого объекта и, во-вторых, тем, что нападению может подвергаться не конкретный компьютер, а информация, передающая по сетевым соединениям.

Кроме перечисленных видов угроз для компьютерных сетей характерны следующие виды угроз:

– несанкционированный обмен информацией между пользователями (может привести к получению одним из них не предназначенных ему сведений);

– несанкционированный межсетевой доступ к информационным и техническим ресурсам сети;

– отказ от информации, т.е. непризнание получателем (отправителем) этой информации факта ее получения (отправления), что может привести к различным злоупотреблениям;

– отказ в обслуживании, который может сопровождаться тяжелыми последствиями для пользователя, обратившегося с запросом на предоставление сетевых услуг.

В последние годы все большую угрозу информации в сетях представляют вирусы, которые распространяются по сетям и мо-

гут привести к уничтожению информации и блокированию функционирования всей корпоративной сети.

Способы воздействия угроз на объекты информационной безопасности корпоративных сетей подразделяются на информационно-технические, физические и организационно-правовые.

Информационно-технические способы осуществления угроз включают в себя радиоэлектронные и акустические способы: перехват информации через электромагнитные и акустические поля и излучения; радиоэлектронное подавление линий связи и систем управления; перехват, дешифрирование и навязывание сообщений и команд управления.

Информационные способы включают: несанкционированный доступ к информационным ресурсам; нарушение технологий информационного обмена, сбора, обработки и хранения информации; незаконный сбор и использование информации; манипулирование информацией (дезинформация, скрытие и т.п.); внедрение программ-вирусов, программных и аппаратных закладок; копирование, уничтожение и искажение данных в информационных системах.

К физическим способам относятся: уничтожение или разрушение средств связи и обработки информации, а также носителей информации; хищение носителей информации, программных или аппаратных ключей и средств криптографической защиты информации.

Организационно-правовые способы включают в себя: невыполнение требований законодательства в информационной сфере; неправомерное ограничение доступа граждан и организаций к информации.

11.8. Уязвимость основных функциональных элементов ИС

Наиболее доступными компонентами сетей являются рабочие станции. Именно с них могут быть предприняты наиболее многочисленные попытки совершения несанкционированных действий. С рабочих станций осуществляется управление процессами обработки информации, запуск программ, ввод и корректировка дан-

ных, на дисках рабочих станций могут размещаться важные данные и программы обработки. На видеомониторы и печатающие устройства рабочих станций выводится информация при работе пользователей, выполняющих различные функции и имеющих разные полномочия по доступу к данным и другим ресурсам системы. Именно поэтому рабочие станции должны быть надежно защищены от доступа посторонних лиц и содержать средства разграничения доступа к ресурсам со стороны законных пользователей, имеющих разные полномочия. Кроме того, средства защиты должны предотвращать нарушения нормальной настройки рабочих станций и режимов их функционирования, вызванные непреднамеренными действиями неопытных пользователей.

В особой защите нуждаются такие привлекательные для злоумышленников элементы сетей как серверы, мосты, маршрутизаторы и другое активное коммуникационное оборудование. Серверы привлекательны для злоумышленников как концентраторы больших объемов информации, а коммуникационные устройства как элементы, в которых осуществляется преобразование данных при согласовании протоколов обмена в различных участках сети.

Для повышения безопасности серверов и коммуникационного оборудования в первую очередь, как правило, применяется защита физическими средствами и организационными мерами, позволяющими сократить до минимума число лиц, имеющих непосредственный доступ к ним. В то же время на серверы могут быть предприняты массированные целенаправленные атаки с использованием средств удаленного доступа. В этом случае злоумышленники, прежде всего, могут искать возможности повлиять на работу различных подсистем серверов и коммуникационных средств, используя недостатки протоколов обмена и средств разграничения удаленного доступа к ресурсам и системным таблицам. Для атак могут использоваться все возможности и средства, от стандартных (без модификации компонентов) до подключения специальных аппаратных средств в каналы связи и применения специальных программных средств для преодоления системы защиты.

Внедрение аппаратных и программных закладок в серверы и коммуникационное оборудование открывает дополнительные широкие возможности по несанкционированному удаленному доступу. Закладки могут быть внедрены как с удаленных стан-

ций, так и непосредственно в аппаратуру и программы серверов при их ремонте, обслуживании, модернизации, переходе на новые версии программного обеспечения, смене оборудования.

Каналы и средства связи также нуждаются в защите. В силу большой пространственной протяженности линий связи через неконтролируемую или слабо контролируемую территорию практически всегда существует возможность подключения к ним, либо вмешательства в процесс передачи данных.

Уровни уязвимости информационных систем классифицируются в соответствии со схемой, представленной на рис. 11.4.

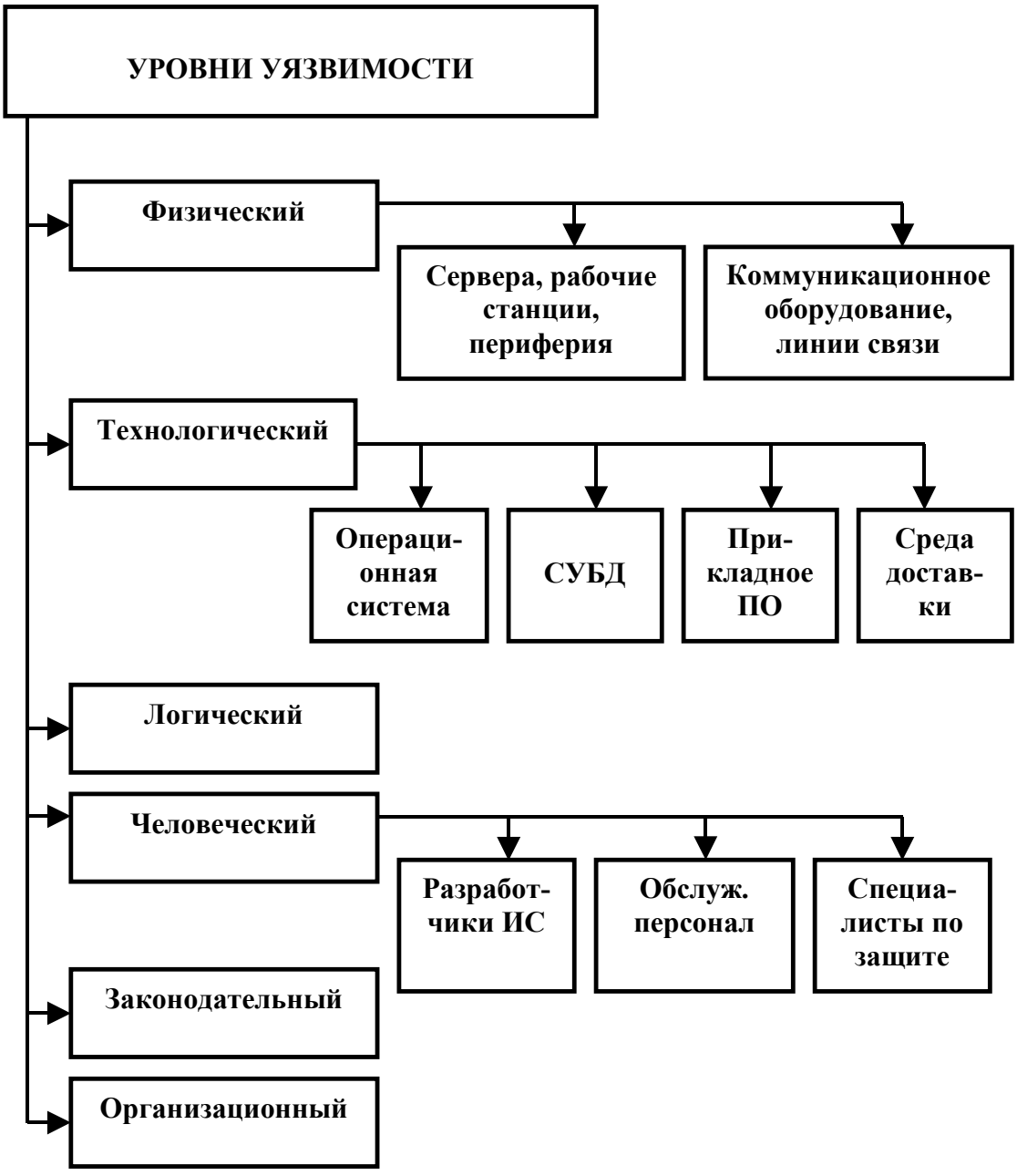


Рис. 11.4.Классификация уровней уязвимости

Физический уровень определяет, насколько эффективно защищены элементы, образующие техническую часть информационной системы: сервера, рабочие станции, периферийные устройства, коммуникационное оборудование и линии связи.

Технологический уровень отражает, насколько эффективно обеспечена защита аппаратно-программных процедур, обеспечивающих требуемую степень безопасности. Это касается выбора операционных систем, систем управления базами данных (СУБД), прикладного программного обеспечения, среды доставки информации.

Логический уровень характеризует адекватность логических основ механизма безопасности и организации хранения и кодирования информации.

Человеческий уровень отражает степень квалификации и ответственности персонала на стадиях проектирования системы и ее эксплуатации (техническое и программное сопровождение, информационное наполнение, контроль за соблюдением требований безопасности).

Законодательный уровень определяет комплекс законодательных и нормативно-правовых актов, регулирующих отношения субъектов в процессах информационного обмена.

Организационный уровень предусматривает комплекс организационных мероприятий, регламентирующий процессы эксплуатации системы.

11.9. Способы и средства защиты информации в сетях

Под защитой информации в компьютерных системах принято понимать создание и поддержание организованной совокупности средств, способов, методов и мероприятий, предназначенных для предупреждения искажения, уничтожения и несанкционированного использования информации, хранимой и обрабатываемой в электронном виде.

Для организации защиты информации в корпоративных сетях важным вопросом является классификация имеющихся способов и средств защиты, которые позволяют воспрепятствовать неза-

конному ее использованию. На рисунке 11.5 схематически показаны наиболее часто используемые способы защиты информации в компьютерных сетях и средства, которыми они могут быть реализованы.

Рис. 11.5.Способы и средства защиты информации

Препятствие – способ физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.д.).

Управление доступом – способ защиты информации за счет регулирования использования всех ресурсов системы (технических, программных, временных и др.). Эти методы должны противостоять всем возможным путям несанкционированного доступа к информации. Управление доступом включает следующие функции защиты:

– идентификацию пользователей, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора);

– установление подлинности объекта или субъекта по предъявленному им идентификатору;

– проверку полномочий;

– разрешение и создание условий работы в пределах установленного регламента;

– регистрацию (протоколирование) обращений к защищаемым ресурсам;

– реагирование (сигнализация, отключение, задержка работ, отказ в запросе и т.п.) при попытках несанкционированных действий.

Маскировка информации, как правило, осуществляется путем ее криптографического закрытия. Механизмы шифрования все шире применяются как при обработке, так и при хранении информации на магнитных носителях. При передаче информации по каналам связи большой протяженности этот метод является единственно надежным.

Противодействие вирусам (или атакам различных вредоносных программ) предполагает комплекс разнообразных мер организационного характера и использование антивирусных программ. Цели принимаемых мер – это уменьшение вероятности инфицирования ИС, выявление фактов заражения системы; уменьшение последствий информационных инфекций, локализация или уничтожение вирусов; восстановление информации в ИС.

Регламентация заключается в реализации системы организационных мероприятий, определяющих все стороны процесса обработки информации.

Принуждение – способ защиты, при котором пользователи и персонал ИС вынуждены соблюдать определенные правила работы с информацией (обработки, передачи и использования защищаемой информации) под угрозой материальной, административной или уголовной ответственности.

Побуждение – способ защиты, побуждающий пользователей и персонал ИС не нарушать установленные порядки за счет соблюдения сложившихся моральных и этических норм.

Средства защиты информации, хранимой и обрабатываемой в электронном виде, разделяют на три самостоятельные группы: технические, программные и социально-правовые. В свою очередь вся совокупность технических средств подразделяется на аппаратные и физические. Социально-правовые средства включают в себя организационные, законодательные и морально-этические.

Физические средства включают различные инженерные устройства и сооружения, препятствующие физическому проникновению злоумышленников на объекты защиты и осуществляющие защиту персонала (личные средства безопасности), материальных средств и финансов, информации от противоправных действий. Примеры физических средств: замки на дверях, решетки на окнах, средства электронной охранной сигнализации и т.п.

Аппаратные средства – устройства, встраиваемые непосредственно в вычислительную технику, или устройства, которые сопрягаются с ней по стандартному интерфейсу. Такие средства принадлежат к наиболее защищенной части системы. С их помощью могут быть реализованы любые концепции защиты, но стоимость реализации оказывается на порядок выше по сравнению с аналогичными по назначению программными средствами. При наличии выбора предпочтение следует отдавать аппаратным средствам защиты, так как они исключают любое вмешательство в их работу непосредственно из сети. Изучение работы этих средств возможно только при наличии непосредственного физического доступа к ним. Другим преимуществом аппаратных средств является их большая производительность по сравнению с программными средствами защиты (особенно в случае их использования в устройствах криптографической защиты).

Программные средства – это специальные программы и программные комплексы, предназначенные для защиты информации в ИС. Они являются наиболее распространенными средствами, так как с их помощью могут быть реализованы практически все идеи и методы защиты, и, кроме того, по сравнению с аппаратными средствами они имеют невысокую стоимость. С помощью программных методов обеспечения безопасности реализованы почти все межсетевые экраны и большинство средств криптографической защиты. Основным их недостатком является доступ-

ность для хакеров, особенно это касается широко распространенных на рынке средств защиты. По целевому назначению их можно разделить на несколько классов:

– программы идентификации и аутентификации пользователей;

– программы определения прав (полномочий) пользователей (технических устройств);

– программы регистрации работы технических средств и пользователей (ведение так называемого системного журнала);

– программы уничтожения (затирания) информации после решения соответствующих задач или при нарушении пользователем определенных правил обработки информации.

Программные средства защиты информации часто делят на средства, реализуемые в стандартных операционных системах (ОС), и средства защиты в специализированных информационных системах.

Криптографические программы основаны на использовании методов шифрования (кодирования) информации. Данные методы являются достаточно надежными средствами защиты, значительно повышающими безопасность передачи информации в сетях.

Часто в сетях используются *аппаратно-программные средства* защиты. Это средства, основанные на использовании технологических устройств, допускающих некоторую настройку параметров их работы программными методами. Они представляют собой компромисс между предыдущими двумя средствами и совмещают высокую производительность аппаратно реализованных систем и гибкость настройки программных. Типичными представителями такого рода устройств является аппаратно реализованные маршрутизаторы фирмы Cisco, которые допускают их настройку в качестве пакетных фильтров.

Организационные и законодательные средства защиты информации предусматривают создание системы нормативно-правовых документов, регламентирующих порядок разработки, внедрения и эксплуатации ИС, а также ответственность должностных и юридических лиц за нарушение установленных правил, законов, приказов, стандартов и т.п.

Организационные средства осуществляют регламентацию производственной деятельности и использования компьютеров в

сети и взаимоотношений исполнителей на нормативно-правовой основе таким образом, что разглашение, утечка и несанкционированный доступ к конфиденциальной информации становятся невозможными или существенно затрудняются за счет проведения организационных мероприятий. Комплекс этих мер реализуется группой информационной безопасности, но должен находиться под контролем первого руководителя. Организационные меры должны охватывать этапы проектирования, внедрения и эксплуатации информационных систем. Они обеспечивают объединение всех используемых средств защиты в единый механизм.

Законодательные средства защиты определяются законодательными актами страны, которыми регламентируются правила пользования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил. Основной целью законодательных средств является предупреждение и сдерживание потенциальных нарушителей.

Морально-этические средства защиты информации основаны на использовании моральных и этических норм, господствующих в обществе. Они включают всевозможные нормы поведения, которые традиционно сложились ранее, складываются по мере распространения информационных технологий в стране и в мире или специально разрабатываются. Морально-этические нормы могут быть неписаные (например, честность), либо оформленные в некий свод (устав) правил или предписаний. Эти нормы, как правило, не являются законодательно утвержденными, но поскольку их несоблюдение приводит к падению престижа организации, они считаются обязательными для исполнения.

11.10. Защита информации от компьютерных вирусов

С развитием информационных технологий и телекоммуникаций появилась необходимость разработки совершенно новых средств защиты информации, предназначенных для противодействия компьютерным вирусам, способным не только уничтожать или искажать информацию, но и блокировать нормальное функционирование всей корпоративной сети. История компьютерных

вирусов ведет начало с 1984г., когда Фред Коэн (США) написал программу, которая автоматически активизировалась и проводила деструктивные изменения информации при незаконном обращении к другим программам автора. С течением времени было создано большое количество программ, предназначенных для вызова тех или иных «вредных» действий без ведома пользователя компьютера.

Компьютерные вирусы в настоящее время являются одной из наиболее распространенных причин потери информации. Особенную остроту проблеме борьбы с вирусами придало развитие локальных и глобальных компьютерных сетей, объединяющих работу большого количества пользователей. Чем более развита компьютерная инфраструктура организации, чем более однородна операционная среда, чем унифицированнее взаимодействие различных программных и аппаратных компонентов, тем выше угроза быстрого распространения вирусов и тем больший урон в потенциале может быть нанесен. Распространение вируса через компьютерную сеть может носить характер эпидемии, полностью дестабилизировав работу организации. При этом может произойти сбой как отдельных компьютеров, так и всей сети в целом, поскольку вирус может вывести из строя сетевые сервера или обеспечить перегрузку сетевого трафика. Такая эпидемия повлечет за собой потерю информации, необходимой для нормальной работы, и потерю времени на восстановление данных и приведение компьютеров и сети в рабочее состояние.

Несмотря на огромные усилия по разработке антивирусных средств, убытки, приносимые компьютерными вирусами, не падают. При этом следует иметь в виду, что разработка антивирусных средств всегда отстает от появления новых вирусов, а поэтому используемые антивирусные средства не дают полной гарантии защиты от вирусов. В настоящее время кроме вирусов существует несколько видов вредоносных программ.

Компьютерный вирус – это специально написанная, как правило, на языке программирования низкого уровня, небольшая по размерам программа, которая может «приписывать» себя к другим программам и выполнять различные нежелательные для пользователя действия на компьютере. Вирусы могут активизироваться при запуске инфицированной программы. Они также

могут постоянно находиться в памяти и заражать открываемые пользователем файлы или создавать свои файлы.

Черви – это независимые программы, размножающиеся путем копирования самих себя через компьютерную сеть. Эти программы, как правило, содержат деструктивный код (вирус), уничтожающий файлы или запускающий атаки на другие компьютеры сети. Не всегда можно четко определить различия между вирусами и червями. Следует отметить, что самые опасные вирусные атаки последних лет связаны именно с червями.

Троянские кони (троян) – это программы, которые запускаются на компьютере не зависимо от согласия пользователя. Трояны, как и вирусы, несут потенциальную опасность, а также обладают скрытностью и не обнаруживают себя до начала деструктивных действий. Троян может попасть на компьютер через почтовое вложение или загружен с web-сайта. Большинство троянских коней маскируются под какие-нибудь полезные программы, игры, экранные заставки или утилиты. При запуске пользователем такой программы она может имитировать работу, но в фоновом режиме может скопировать свои исполняемые файлы с вредоносным кодом и произвести модифицирование системы. Будучи однажды запущенным на компьютере, троянец либо копирует себя в какое-то «потаенное» место, прописывает себя на запуск в системном реестре, обеспечивая себе получение управления при каждой загрузке системы и ждет своего часа. Существуют троянцы, которые внедряются в исполняемые файлы.

После установки трояна на компьютер злоумышленник получит контроль над ним и может причинить значительный вред: удалить или скопировать файлы, перехватить пароли и отправить их по электронной почте, получить доступ к другим станциям и серверам сети или совершить другие нежелательные для пользователя действия. В последнее время получили широкое распространение троянские программы, обладающие возможностью скрытого удаленного администрирования.

Смешанные коды – это сравнительно новый класс вредоносных программ, сочетающий в себе свойства вирусов, червей и троянов. Такие программы наиболее опасны и поражают станции и серверы сети. Вирусы, распространяющиеся по сети относятся к категории трудных для обнаружения. Один инфицированный

компьютер может заразить сотни других по сети. Даже при наличии антивирусных средств сеть остается уязвимой для атак. Например, если пользователь принесет инфицированный домашний ноутбук и включит его в сеть, то с большой вероятностью может произойти заражение станций сети.

Жизненный цикл вируса включает четыре основных этапа:

– внедрение;

– инкубационный период;

– репродуцирование (саморазмножение);

– деструкция (искажение и/или уничтожение информации).

Наиболее широко распространенными деструктивными функциями вирусов являются:

– изменение данных в файлах;

– уничтожение информации путем форматирования диска или отдельных треков на нем;

– уничтожение каталога файлов или отдельных файлов на диске;

– уничтожение программ и файлов операционной системы, что ведет к нарушению ее работоспособности;

– несанкционированная рассылка электронной почты.

Классификация компьютерных вирусов может быть проведена по различным признакам. Одна из возможных схем классификации приведена на рисунке 11.6.

Возможна следующая классификация вирусов:

– среда обитания;

– особенности алгоритма работы;

– деструктивные возможности.

По среде обитания вирусы можно разделить на типы:

– файловые;

– загрузочные;

– макровирусы;

– сетевые.

Наиболее часто распространенными вирусами являются файловые, которые различными способами внедряются в выполняемые файлы.

Загрузочные вирусы записывают себя в загрузочный сектор диска (*boot-сектор*).

Макровирусы заражают файлы документов, электронные таблицы, презентации ряда популярных офисных приложений.

Рис. 11.6. Классификация компьютерных вирусов

Сетевые вирусы используют для своего распространения протоколы компьютерных сетей. Они считаются наиболее опасными, так как имеют возможность передать свой код на удаленный компьютер. Существуют сетевые вирусы, использующие возможности электронной почты. Они распространяются вместе с письмами в виде вложенных файлов. Вирус получает управление после запуска такого файла. После активизации вирус анализирует адресную книгу почтовой программы и рассылает свои копии по полученным оттуда адресам.

Возможность инфицирования компьютерными вирусами корпоративных сетей становится все более серьезной проблемой. Опасность действия вирусов определяется возможностью частичной или полной потери ценной информации, финансовым затратам, а также потерей времени на восстановление работоспособности сети и информационных систем.

Для повышения эффективности борьбы с вирусами в корпоративной сети необходима централизация управления работой ан-

тивирусной системы. В настоящее время существуют сетевые версии антивирусных средств, а также антивирусные пакеты, устанавливаемые на почтовые сервера.

По особенностям алгоритма работы различаются следующие:

– резидентность;

– использование стелс-алгоритмов;

– самошифрование и полиморфичность;

– использование нестандартных приемов.

Резидентный вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращения операционной системы к объектам заражения и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения компьютера или перезагрузки операционной системы.

Использование стелс-алгоритмов позволяет вирусам полностью или частично скрыть себя в системе.

Самошифрование и полиморфичность (шифрование основного тела вируса) используются для того, чтобы максимально усложнить процедуру детектирования вируса. Полиморфным принято называть такой вид вируса, каждая последующая копия которого отличается от предыдущей. Полиморфный вирус не имеет ни одного постоянного участка кода. Такая особенность крайне затрудняет или вообще делает невозможным обнаружение с помощью вирусных масок, характерных для кода определенного вируса. Эта особенность достигается либо изменением кода вируса, либо его шифрованием.

Многие типы вирусов для маскировки своего присутствия используют различные нестандартные методы.

По деструктивным (вредным) действиям вирусы можно разделить на следующие:

– безвредные, т.е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);

– неопасные, влияние которых ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и другими подобными эффектами;

– опасные вирусы, которые могут привести к серьезным сбоям в работе компьютера;

– очень опасные, в алгоритм работы которых заведомо заложены процедуры, которые могут привести к потере программ, уничтожению данных, утрате необходимой для работы компьютера информации.

При борьбе с вирусами важно своевременно определить их наличие в компьютере. О наличии вредоносного кода на компьютере могут гворить следующие симптомы:

1. Подозрительная активность диска. Трояны устроены таким образом, что они работают с диском тогда, когда пользователь ничего не делает. Поэтому, если наблюдается активность диска, необходимо попытаться определить какая программа выполняется в фоновом режиме.

2. Беспричинное замедление работы компьютера. Вирус может потреблять значительную часть системных ресурсов и замедлять работу приложений.

3. Подозрительно высокий трафик в сети. Вирус может использовать сеть для распространения на другие станции или для передачи информации с вашего компьютера злоумышленнику. Некоторые программы (в том числе антивирусы) обладают функцией автоматического обновления и могут повысить трафик, поэтому при возникновении указанного признака необходимо определить источник активности, проверив все выполняющиеся в системе программы.

4. Изменение размеров и имен файлов. Такие изменения практически трудно заметить, но некоторые антивирусные системы могут предупреждать пользователя об этих изменениях.

К сожалению, технологии создания вредоносных программ постоянно совершенствуются. По статистике компании Trend Micro (http://www.trendmicro.com) в 2004 году компаниям по всему миру приходилось сталкиваться ежемесячно в среднем с 3151900 заражениями. Сегодня теоретически доказана возможность создания червя, который может заразить все узлы Интернета за 15 минут. Классические антивирусные средства основаны на анализе сигнатур (последовательность байт, идентифицирующих вирус) вирусов. Такой подход требует наличия в базах данных антивирусов соответствующих сигнатур, поэтому антивирусные средства всегда отстают от разработок новых вирусов. Кроме то-

го, необходимо время для обновления баз данных по узлам при появлении новой сигнатуры.

В последнее время для антивирусных средств перспективным считается принцип отслеживания отклонений поведения программ и процессов от эталонного. Одной из таких систем является Cisco Security Agent, разработанной компанией Cisco System. Она позволяет объединить в одном решении различные защитные механизмы.

В России наиболее распространенными средствами антивирусной защиты являются продукты и технологии компании «Доктор WEB» (www.doctorweb.com) и «Лаборатория Касперского» (www.kaspersky.ru). На указанных сайтах можно познакомиться с различными средствами защиты рабочих станций и сетей, разработанными компаниями и эффективно применяющимися на практике.

11.11. Методы обеспечения безопасности сетей

11.11.1. Стандартные методы защиты

Выше мы рассмотрели классификацию средств и способов защиты информации. Рассмотрим теперь конкретные методы и средства защиты, используемые в корпоративных сетях. Хронологически их можно разделить на традиционные и специфические сетевые. Традиционные методы и средства зарождались и использовались еще до появления компьютерных сетей и использовались на отдельных компьютерах или многопользовательских системах. Сетевые методы и средства появились только с развитием сетевых технологий. Традиционными можно считать следующие средства защиты.

Парольная защита основана на том, что для использования какого-либо ресурса необходимо задать некоторую комбинацию символов (пароль), открывающий доступ к этому ресурсу. С помощью паролей защищаются файлы, личные или корпоративные архивы, программы и отдельные компьютеры. Недостатки такой

защиты: слабая защищенность коротких паролей, которые с помощью специальных программ на высокопроизводительных компьютерах достаточно быстро раскрываются простым перебором. В сетях пароли используются как самостоятельно, так и в качестве основы для различных методов аутентификации. При выборе пароля необходимо соблюдать ряд основных требований:

– в качестве пароля не может использоваться слово из какого бы то ни было языка;

– длина пароля не может быть менее 8 символов;

– один и тот же пароль не может быть использован для доступа к разным ресурсам;

– старый пароль не должен использоваться повторно;

– пароль должен меняться как можно чаще.

Идентификация представляет собой процедуру распознавания пользователя (процесса) по его имени. Для пользователей сети она может быть реализована программно или аппаратно. Аппаратная реализация основана на применении для идентификации пользователей специальных электронных карт, содержащих идентифицирующую конкретного пользователя информацию (подобно банковским кредитным карточкам). Системы идентификации пользователей, реализуемые аппаратно, являются более надежными, чем парольная защита.

Аутентификация пользователей – это развитие систем парольной защиты и идентификации для использования в сетях. Аутентификация – это процедура проверки подлинности пользователя, аппаратуры или программы для получения доступа к определенной информации или ресурсу. По отношению к пользователю система аутентификации обычно требует указания имени и предъявления пароля или электронной карты.

Криптографические методы защиты основаны на шифровании информации и программ. Шифрование программ обеспечивает гарантию невозможности внесения в них изменений. Криптографическая защита данных осуществляется как при их хранении, так и при передаче по сети, причем хранение данных в зашифрованном виде существенно повышает степень их защищенности. В настоящее время доступны как программная, так и высокопроизводительная аппаратная реализация средств криптографии.

Привязка программ и данных к конкретному компьютеру (сети или ключу). Основная идея метода – включение в данные или в программу конкретных параметров или характеристик конкретного компьютера, которое делает невозможным чтение данных или исполнение программ на другом компьютере. Применительно к сети различные модификации этого метода могут требовать либо выполнения всех операций на конкретном компьютере, либо наличия активного соединения сети с конкретным компьютером. Возможности использования метода «привязки» могут значительно повысить защищенность сети.

Разграничение прав доступа пользователей к ресурсам сети – метод, основанный на использовании таблиц или наборов таблиц, определяющих права пользователей и построенных по правилам «разрешено все, кроме» или «разрешено только». Таблицы по идентификатору или паролю пользователя определяют его права доступа к дискам, разделам диска, конкретным файлам или их группам, операциям записи, чтения или копирования и другим ресурсам сети. Возможность такого разграничения доступа определяется, как правило, возможностями используемой операционной системы и заложены именно в ней. Большинство современных сетевых ОС предусматривают разграничение доступа, но в каждой из них эти возможности реализованы в разном объеме и разными способами.

Использование заложенных в ОС возможностей защиты – это обязательное правило. Однако большинство ОС либо имеют минимальную защиту, либо предоставляют возможности ее реализации дополнительными средствами.

При использовании стандартных вышеперечисленных методов защиты необходимо учитывать, что защищенность всей корпоративной сети определяется ее самым слабым звеном. Поэтому неоднородные сети, в которых используются разнородные операционные системы, а также прикладные программные системы, выполненные на базе различных инструментальных средств и систем управления базами данных, представляют собой повышенную опасность с точки зрения безопасности.

Кроме перечисленных выше методов в корпоративной сети необходимо применять архитектурные методы защиты. Они включают решения, принимаемые на уровне топологии и архи-

тектуры сети и повышающие ее защищенность в целом. Различают решения, принимаемые на уровне топологии и архитектуры внутренней сети (корпоративной, локальной), и решения на уровне промежуточной сети, связывающей внутреннюю сеть с внешней, например, с сетью Internet.

На уровне топологии и архитектуры внутренней сети могут приниматься такие решения:

– физическая изоляция закрытого сегмента внутренней сети, содержащего конфиденциальную информацию, от внешней сети;

– функциональное разделение внутренней сети на подсети, при котором в каждой подсети работают пользователи, объединенные по профессиональным интересам;

– сеансовое (кратковременное) подключение внутренней сети к сегменту сети, подключенному к Internet, с помощью коммутатора и/или переключаемого моста (любое кратковременное соединение с внешней сетью более безопасно, чем постоянное соединение).

Основу обеспечения безопасности корпоративной сети составляют мониторинг и аудит ее состояния. Мониторинг (контроль текущего состояния и параметров работы сети) и аудит (регулярный анализ журналов регистрации для выявления происходящих в сети процессов и активности пользователей) – это обязательные составные части работы сетевого администратора.

11.11.2. Межсетевые экраны

При подключении корпоративной сети к открытым сетям, например к сети Internet, появляются угрозы несанкционированного вторжения в закрытую (внутреннюю) сеть из открытой (внешней), а также угрозы несанкционированного доступа из закрытой сети к ресурсам открытой. Подобный вид угроз характерен также для случая, когда объединяются отдельные сети, ориентированные на обработку конфиденциальной информации разного уровня секретности.

Через Internet или другую открытую внешнюю сеть нарушитель может вторгнуться во внутреннюю сеть предприятия и получить несанкционированный доступ к конфиденциальной информации и техническим ресурсам, получить пароли, адреса серверов,

а подчас и их содержимое, войти в информационную систему предприятия под именем зарегистрированного пользователя и т.д.

Угрозы несанкционированного доступа во внешнюю сеть из внутренней сети актуальны в случае ограничения разрешенного доступа во внешнюю сеть правилами, установленными в организации.

Бороться с рассмотренными угрозами безопасности межсетевого взаимодействия средствами универсальных операционных систем не представляется возможным. Ряд задач по отражению наиболее вероятных угроз для внутренних сетей способны решать межсетевые экраны (брандмауэры, firewall). Вне компьютерной сетевой сферы термином *firewall* называют стену, сделанную из негорючих материалов и препятствующую распространению пожара. В сфере компьютерных сетей межсетевой экран представляет собой барьер, защищающий от фигурального пожара – попыток злоумышленников вторгнуться во внутреннюю сеть. Межсетевой экран (МЭ) призван обеспечить безопасный доступ к внешней сети и ограничить доступ внешних пользователей к внутренней сети.

Межсетевой экран – это программная или программно-аппаратная система межсетевой защиты, позволяющая разделить две (или более) взаимодействующие сети и реализовать набор правил, определяющих условия прохождения пакетов из одной сети в другую.

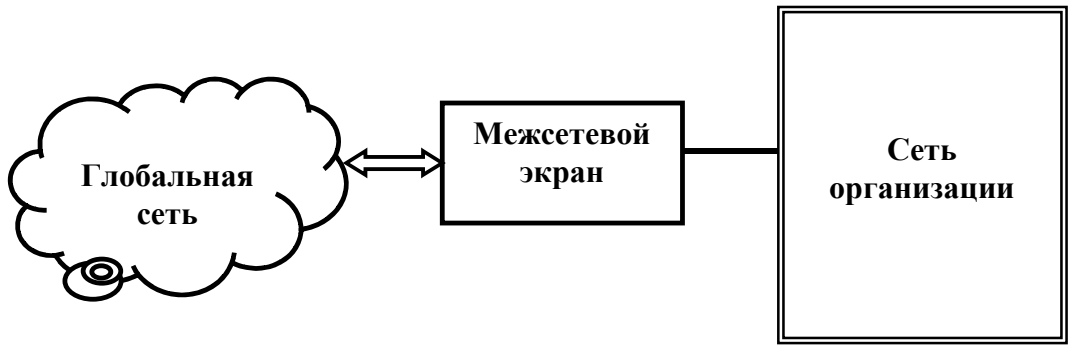


Рис. 11.7. Схема расположения межсетевого экрана

Для противодействия несанкционированному межсетевому доступу он должен располагаться между защищаемой сетью организации, являющейся внутренней, и потенциально враждебной

внешней сетью (рис. 11.7), хотя подобными экранами можно разделить друг от друга и внутренние локальные сети. Если корпоративная сеть состоит из ряда удаленных локальных сетей (ЛВС1, ЛВС2,…), соединенных между собой средствами глобальных сетей, то межсетевые экраны ставятся в каждой локальной сети на границе с глобальной (рис. 11.8).

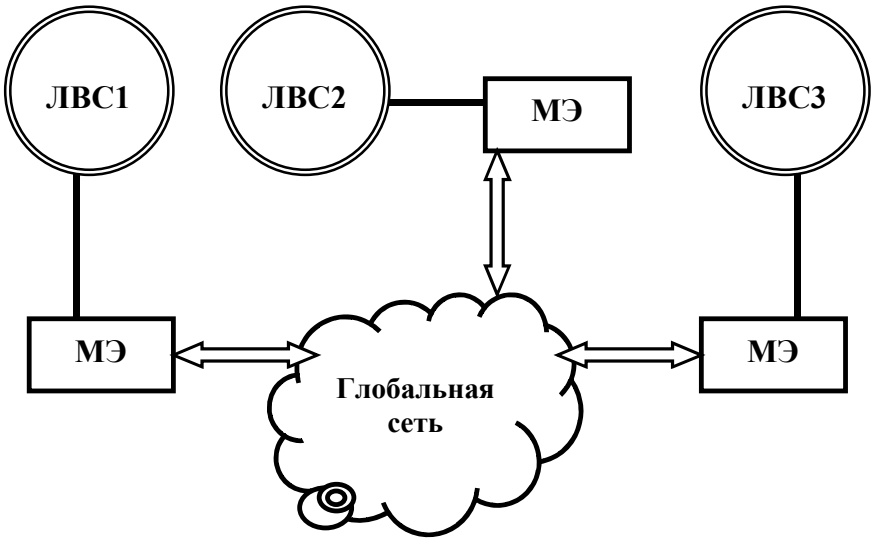


Рис. 11.8. Схема защиты ЛВС корпоративной сети

Главный довод в пользу применения межсетевых экранов состоит в том, что без них внутренняя сеть подвергается опасности со стороны слабо защищенных служб сети Internet. Межсетевой экран пропускает через себя весь трафик, принимая относительно каждого проходящего пакета решение – пропускать его или отбросить. Для того чтобы МЭ мог осуществить это, ему необходимо определить набор правил фильтрации в соответствии с принятой политикой сетевой безопасности.

Политика безопасности включает две составляющие: политика доступа к сетевым сервисам и политика реализации межсетевых экранов. В соответствии с принятой политикой доступа к сетевым сервисам определяется список сервисов Internet, к которым пользователи должны иметь ограниченный доступ.

Межсетевой экран может реализовывать ряд политик доступа к сервисам, однако обычно политика основана на одном из следующих принципов:

– запретить доступ из Internet во внутреннюю сеть и разрешить доступ из внутренней сети в Internet;

– разрешить ограниченный доступ во внутреннюю сеть из Internet, обеспечивая работу только отдельных «авторизированных» систем, например, информационных и почтовых серверов.

В соответствии с политикой реализации межсетевых экранов определяются правила доступа к ресурсам внутренней сети. Эти правила должны базироваться на одном из следующих принципов:

– запрещать все, что не разрешено в явной форме;

– разрешать все, что не запрещено в явной форме.

Эффективность защиты внутренней сети с помощью межсетевых экранов зависит не только от выбранной политики доступа к сетевым сервисам и ресурсам внутренней сети, но и от рациональности выбора и использования основных компонентов межсетевого экрана.

Функциональные требования к межсетевым экранам включают в себя: требования к фильтрации на сетевом, сеансовом и прикладном уровнях модели OSI/ISO; требования по настройке правил фильтрации и администрированию; требования к средствам сетевой аутентификации; требования по внедрению журналов учета и сбору статистики и другие функции.

Межсетевые экраны можно классифицировать по следующим признакам: месту их включения; уровню фильтрации, соответствующему эталонной модели OSI/ISO; требованиям к показателям защищенности.

По первому признаку МЭ подразделяются на внешние и внутренние. Внешние обеспечивают защиту от внешней сети, внутренние разграничивают доступ между сегментами корпоративной сети.

Работа всех межсетевых экранов основана на использовании информации различных уровней эталонной модели OSI и пятиуровневой модели семейства протоколов Internet. Как правило, чем выше уровень, на котором межсетевой экран фильтрует пакеты, тем выше обеспечиваемый им уровень защиты. По уровню фильтрации модели OSI межсетевые экраны разделяют на четыре типа: межсетевые экраны с фильтрацией пакетов (фильтрующие или экранирующие маршрутизаторы); шлюзы сеансового уровня;

шлюзы прикладного уровня; межсетевые экраны экспертного уровня приложений.

Межсетевые экраны с фильтрацией пакетов представляют собой фильтрующие (экранирующие) маршрутизаторы, сконфигурированные таким образом, чтобы фильтровать входящие и исходящие пакеты. Поэтому такие экраны называют иногда пакетными фильтрами. Фильтрация осуществляется анализом IP-адреса источника и приемника, а также портов входящих TCP- и UDP-пакетов и сравнением их с сконфигурированной таблицей правил. Данные системы просты в использовании, дешевы, оказывают минимальное влияние на производительность сетей. Основным их недостатком является уязвимость для замены адресов IP.

Шлюзы сеансового уровня контролируют допустимость сеанса связи. Они следят за подтверждением связи между взаимодействующими процессами, определяя, является ли запрашиваемый сеанс связи допустимым. При фильтрации пакетов шлюз сеансового уровня основывается на информации, содержащейся в заголовках пакетов сеансового уровня протокола TCP.

Шлюзы прикладного уровня проверяют содержимое каждого проходящего через шлюз пакета и могут фильтровать отдельные виды команд или информации в протоколах прикладного уровня, которые им поручено обслуживать. Это более совершенный и надежный тип брандмауэра, использующий программы-посредники прикладного уровня или программы-агенты. Агенты формируются для конкретных служб Internet (HTTP, FTP, Telnet и т.д.) с целью проверки сетевых пакетов на наличие достоверных данных. Однако шлюзы прикладного уровня снижают производительность системы.

Межсетевые экраны экспертного уровня сочетают в себе элементы экранирующих маршрутизаторов и прикладных шлюзов.

Хотя межсетевой экран и является важным и достаточно надежным средством защиты корпоративной сети от несанкционированного доступа, он не может гарантировать полной защиты. Наличие экрана является необходимым, но не достаточным средством обеспечения безопасности сети.

11.11.3. Защищенные виртуальные сети VPN

Для эффективного противодействия сетевым атакам и обеспечения возможности активного и безопасного использования глобальных открытых сетей в начале 90-х годов родилась и активно развивается концепция построения защищенных виртуальных частных сетей VPN (Virtual Private Networks).

В основе концепции лежит достаточно простая идея: если в глобальной сети есть два узла, которые хотят обменяться информацией, то для обеспечения конфиденциальности и целостности передаваемой по открытым сетям информации между ними необходимо построить виртуальный туннель, доступ к которому должен быть чрезвычайно затруднен всем возможным активным и пассивным внешним наблюдателям. Термин «виртуальный» указывает на то, что соединение между двумя узлами сети не является постоянным (жестким) и существует только во время прохождения трафика по сети.

Преимущества таких виртуальных туннелей, заключаются, прежде всего, в значительной экономии финансовых средств. Это объясняется тем, что отпадает необходимость построения или аренды дорогих выделенных каналов связи, а для создания собственных сетей используются дешевые Internet-каналы, надежность и скорость передачи которых в большинстве своем сегодня уже не уступают выделенным линиям.

Защищенной виртуальной сетью VPN называют соединение локальных сетей и отдельных компьютеров через открытую внешнюю среду передачи информации в единую виртуальную корпоративную сеть, обеспечивающую безопасность данных.

Эффективность виртуальной частной сети VPN определяется степенью защищенности информации, циркулирующей по открытым каналам связи. Защита информации в процессе ее передачи по открытым каналам основана на построении защищенных виртуальных каналов связи, называемых туннелями VPN. Туннель VPN представляет собой соединение, проведенное через открытую сеть, по которому передаются криптографически защищенные пакеты сообщений виртуальной сети.

С помощью этой методики пакеты данных передаются через общедоступную сеть как по обычному двухточечному соедине-

нию. Между каждой парой «отправитель-получатель» устанавливается своеобразный туннель – безопасное логическое соединение, позволяющее инкапсулировать данные одного протокола в пакеты другого.

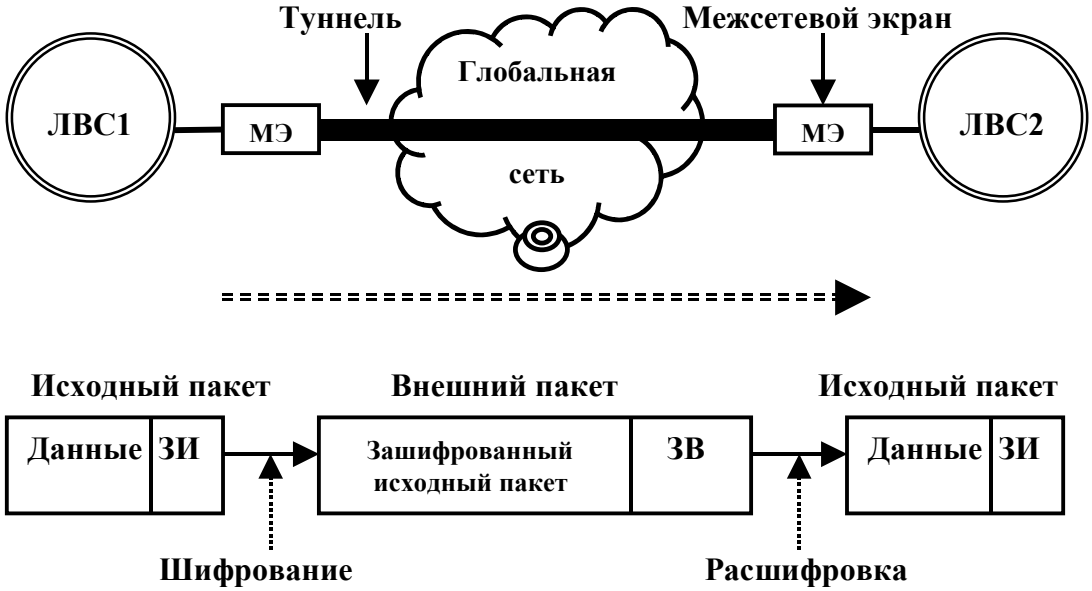


Рис. 11.9 Схема виртуального туннеля

Суть туннелирования состоит в том, чтобы «упаковать» передаваемую порцию данных (вместе со служебными полями) в новый «конверт». Чтобы обеспечить конфиденциальность передаваемых данных, отправитель шифрует исходный пакет вместе с заголовком, упаковывает его в поле данных внешнего пакета с новым открытым IP-заголовком и отправляет по транзитной сети. Схема виртуального туннеля представлена на рисунке 11.9 (где ЗИ – заголовок исходного пакета, ЗВ – заголовок внешнего пакета).

Для транспортировки данных по открытой сети используются открытые поля заголовка внешнего пакета. Для внешних пакетов используются адреса пограничных маршрутизаторов, установленных в начале и конце туннеля, а внутренние адреса конечных узлов содержатся во внутренних исходных пакетах в защищенном виде. По прибытии в конечную точку защищенного канала из внешнего пакета извлекают и расшифровывают внутренний исходный пакет и используют его восстановленный заголовок для дальнейшей передачи по внутренней сети.

Туннелирование может использоваться не только для обеспечения конфиденциальности и целостности всей передаваемой порции данных, но и для организации перехода между сетями с разными протоколами (например, IPv4 и IPv6), а также различными технологиями и системой адресации.

11.11.4. Обеспечение безопасности в беспроводных сетях

Вопрос обеспечения безопасности в беспроводных сетях стоит более остро, чем в проводных. Радиус действия беспроводных сетей типа 802.11 может составлять сотни метров, поэтому злоумышленник, желающий перехватить информацию, может просто приехать на автомобиле к зданию, включить в машине ноутбук с приемопередатчиком и весь трафик, проходящий по локальной сети внутри здания, может быть перехвачен.

При использовании беспроводных сетей могут быть следующие виды рисков:

1. Хищение услуг. Злоумышленник может получить доступ к Интернету.

2. Отказ в услугах. Хакер может стать источником большого количества запросов на подключение к сети, в результате чего затруднить подключение законных пользователей.

3. Хищение или разрушение данных. Злоумышленник, подключившись к сети, может получить доступ к файлам и папкам, а следовательно получить возможность копирования, модификации и удаления.

4. Перехват контроля над сетью. Злоумышленник, используя слабые места в системе безопасности, может внедрить троянского коня или назначить такие права доступа, которые могут привести к незащищенности компьютера от атак из сети Интернет.

Разработкой спецификаций беспроводных сетей занимается группа 802.11x института IEEE. Все технические детали стандарта, в том числе и по обеспечению безопасности, помещаются на web-сайте группы http://www.ieee802.org/11, а также на сайте http://www.wi-fi.org. Стандарт 802.11 описывает протокол безопасности уровня передачи данных под названием **WEP** (Wired Equivalent Privacy – секретность, эквивалентная проводным се-

тям), предназначенный для того, чтобы обезопасить беспроводные ЛВС так же надежно, как и проводные.

При наличии системы безопасности в сети 802.11 каждая станция имеет общий закрытый ключ с базовой станцией. Метод распространения ключей стандартом не оговаривается. Ими можно обменяться заранее по проводной сети. При обмене информацией базовая станция, либо пользовательская машина может случайным образом выбирать ключ и отсылать его противоположной стороне, предварительно зашифровав при помощи открытого ключа этой стороны. После установки ключи могут оставаться неизменными в течение нескольких месяцев или даже лет.

При шифровании при помощи WEP сначала проверяется контрольная сумма полезной нагрузки пакета. Открытый текст, передаваемый алгоритму шифрования, формируется путем добавления контрольной суммы к полезной нагрузке. Полученный открытый текст складывается по модулю 2 с отрезком ключевого потока и результатом этих преобразований является зашифрованный текст. После получения пакета приемник извлекает из него зашифрованные данные (полезную нагрузку) и восстанавливает открытый текст. Сравнивая контрольную сумму полученных данных, можно убедиться в подлинности принятой информации.

Однако протокол имеет ряд недостатков. Во-первых при использовании одинаковых общих ключей для всех пользователей они могут запросто читать весь трафик друг друга. Но даже если всем пользователям раздать разные ключи, WEP все равно может быть взломан. Так как ключи не изменяются в течение больших периодов времени, стандарт WEP рекомендует (но не обязывает) изменять вектор инициализации при передаче каждого.

К сожалению, многие сетевые карты стандарта 802.11 для ноутбуков сбрасывают вектор инициализации в 0, когда ее вставляют в разъем, и увеличивают на единичку с каждым пересылаемым пакетом. Так как сетевые карты вставляются и вынимаются весьма часто, малые числа, выступающие в качестве векторов инициализации, – обычное дело. Если злоумышленнику удастся собрать несколько пакетов, посланных одним и тем же пользователем, с одинаковыми значениями вектора инициализации (который сам по себе посылается открытым текстом вместе с пакетом), то он сможет вычислить сумму по модулю 2 двух блоков откры-

того текста, что дает возможность взломать шифр. Даже если сетевая карта 802.11 будет подбирать значения вектора инициализации для каждого пакета случайным образом, все равно благодаря ограниченной длине вектора (24 разряда) векторы будут повторяться.

Алгоритм взлома протокола WEP был опубликован в 2001 году. Вторая версия протокола (WAP-2.0) предусматривает возможности защиты на сетевом, транспортном и прикладном уровнях, что повышает надежность защиты.

Радиус действия беспроводных систем типа Bluetooth значительно короче, чем сетей 802.11, поэтому злоумышленниек не удастся произвести атаку, оставив ноутбук в припаркованной рядом со зданием машине. Однако проблемы безопасности все равно существуют. Например, если компьютер оборудован беспроводной клавиатурой стандарта Bluetooth и, если не установить систему защиты, то, находясь в соседней комнате, можно без труда прочесть все, что набирается на компьютере. Можно перехватить также все, что передается на беспроводной принтер.

Система защиты Bluetooth обеспечивает безопасность на нескольких уровнях. На физическом уровне для этого применяются скачкообразные изменения частот, но поскольку любое устройство, появляющееся в микросети, должно узнать последовательность скачков частоты, эта последовательность, очевидно, не является секретной. Настоящая защита информации начинает проявляться тогда, когда вновь прибывшее подчиненное устройство пытается запросить канал для связи с управляющим устройством. Предполагается, что оба устройства совместно используют предварительно установленный закрытый ключ. В некоторых случаях он прошивается в обоих устройствах (например, в гарнитуре и мобильном телефоне, продающихся вместе). В других случаях в одном из устройств (например, в гарнитуре) ключ прошит, а в сопряженное устройство (например, мобильный телефон) пользователь должен ввести ключ вручную в виде десятичного числа.

Еще одна проблема безопасности, связанная с Bluetooth, состоит в том, что система идентифицирует только устройства, а не пользователей. Это приводит к тому, что вор, укравший устройство Bluetooth, получит доступ к информации.

Тем не менее, система безопасности в Bluetooth реализована и на верхних уровнях протокола, поэтому даже в случае взлома защиты на уровне передачи данных некоторые шансы еще остаются, особенно если приложение для выполнения транзакции требует ввода PIN-кода вручную с помощью какой-нибудь разновидности клавиатуры.

При настройке беспроводной сети следует соблюдать следующие дополнительные меры безопасности:

1. Избегать соединения беспроводной сети с проводной ЛВС. Беспроводная точка доступа определяет подключение к маршрутизатору в отдельной сети или к интерфейсу брандмауэра.

2. Для реализации беспроводных соединений использовать виртуальные частные сети (VPN).

3. Использовать инструментальные средства сканирования для проверки сети на предмет наличия уязвимых мест в системе безопасности.

4. Регулярно проверять журнал регистрации подключений для контроля всех сетевых подключений.

11.12. Требования к системе обеспечения безопасности сети

Одним из важнейших аспектов функционирования корпоративной сети является обеспечение защиты информации. Необходимо создать такие условия ввода-вывода, хранения, обработки и передачи информации, при которых гарантируется достаточная степень защиты от утечки, модификации и утраты, а также свободный доступ к данным только авторизованных пользователей. Для удовлетворения этих требований формируется *система обеспечения безопасности* корпоративной сети. Она представляет собой совокупность правил, методов и аппаратно-программных средств, создаваемых при ее проектировании, непрерывно совершенствуемых и поддерживаемых в процессе эксплуатации для предупреждения нарушений нормального функционирования при проявлении случайных факторов или умышленных действий, когда возможно нанесение ущерба пользователям путем отказа в

обслуживании, раскрытия или модификации защищаемых процессов, данных или технических средств.

Важным элементом системы безопасности являются национальные и международные правовые акты в области защиты информации. Указом Президента Российской Федерации № 9 от 05.01.1992 г. «О создании Государственной технической комиссии при Президенте Российской Федерации» создан специальный государственный орган, курирующий вопросы защиты информации.

В 1992 г. Гостехкомиссия опубликовала ряд руководящих документов, посвященных вопросам защиты от несанкционированного доступа к информации www.infotecs.ru. Среди них следует отметить следующие:

– «Концепция защиты средств вычислительной техники от несанкционированного доступа к информации»;

– «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»;

– «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

Эти документы регламентируют основные понятия и концепции информационной безопасности на государственном и межгосударственном уровнях, определяют требования и критерии безопасности, образующие шкалу оценивания степени защищенности информационных систем и технологий. Главная задача разработки таких стандартов – создание основы для взаимодействия между производителями, потребителями и экспертами по квалификации продуктов информационных технологий.

Второй из вышеприведенных документов Гостехкомиссии является отечественным аналогом так называемой «Оранжевой книги» – государственного стандарта США «Критерии оценивания безопасности надежных вычислительных систем» (1984г.). Он устанавливает классификацию средств вычислительной техники по уровню защищенности от несанкционированного доступа к информации на базе перечня показателей и совокупности описываемых их требований.

С 01.01.1996 г. введен в действие стандарт ГОСТ Р 50739–95 «Защита от несанкционированного доступа к информации. Средства вычислительной техники. Общие технические требования».

Наиболее значительными стандартами в области защиты информации за рубежом являются: «Критерии безопасности компьютерных систем МО США» (являющиеся развитием «Оранжевой книги»), «Европейские критерии безопасности информационных технологий», «Федеральные критерии безопасности информационных технологий США», «Канадские критерии безопасности компьютерных систем» и, наконец, «Единые критерии оценивания безопасности информационных технологий» («Единые Критерии»).

«Единые Критерии» являются результатом совместных усилий по объединению существующих национальных стандартов в единый согласованный документ и созданию единого международного стандарта оценивания безопасности информационных технологий (ISO 15408: 1999), в том числе корпоративных сетей.

Требования «Единых критериев» охватывают практически все аспекты безопасности ИТ-продуктов и технологий их создания и являются практически всеобъемлющей энциклопедией информационной безопасности, поэтому их можно использовать в качестве справочника безопасности информационных технологий.

Согласно Указу Президента РФ № 1085 от 16.08.2004 г. создана Федеральная служба по техническому и экспортному контролю, которая является преемником Государственной технической комиссии при Президенте России и выполняет «специальные и контрольные функции в области государственной безопасности по вопросам:

1) обеспечения безопасности информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере (далее – безопасность информации в ключевых системах информационной инфраструктуры);

2) обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию

(носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации (далее – техническая защита информации).»

Государственный стандарт ГОСТ Р ИСО/МЭК 15408 «Методы и средства обеспечения безопасности. Критерии безопасности информационных технологий» («Общие критерии») призваны заменить прежние руководящие документы путем интеграции с мировым сообществом. Пока руководствоваться «Общими критериями» могут лишь организации, которые в своих информационных системах не обрабатывают сведения, содержащие государственную тайну.

При практической реализации системы обеспечения безопасности (СОБ) к основным ее функциональным требованиям относятся следующие.

1. **Многоуровневость СОБ**, предусматривающая наличие нескольких рубежей защиты, реализованных в разных точках сети.

2. **Распределенность** средств защиты по разным элементам сети с обеспечением автономного управления каждым из этих средств.

3. **Разнородность** или **разнотипность** применяемых средств защиты. Предпочтение должно отдаваться аппаратным средствам, так как они не поддаются прямому воздействию из внешней сети. Однако на разных уровнях защиты должны использоваться и программные средства.

4. **Уникальность защиты**, являющаяся ее краеугольным камнем. Степень защищенности КВС можно оценить сложностью и, главное, оригинальностью алгоритма защиты, деленному на количество реализаций такого алгоритма и на время его использования. Это означает, что с течением времени любой механизм защиты будет вскрыт, особенно если он многократно тиражирован, т. е. представлен для исследования большому количеству хакеров. Следовательно, предпочтение следует отдать собственному механизму защиты, уникальность которого ослабит интерес со стороны хакеров, поскольку их в гораздо большей степени привлекают массовые, типовые решения.

5. **Непрерывность развития СОБ**, т. е. постоянное наращивание возможностей и модификация системы защиты с течением времени. Развитие должно быть заложено в самом механизме за-

щиты. Разработка СОБ – это не одноразовое действие, а постоянный процесс.

6. **Распределение полномочий**, в соответствии с которым ни один человек персонально не имеет доступ ко всем возможностям системы. Такие возможности открываются только группе уполномоченных лиц. Один из аспектов этого требования заключается в том, что сменный дежурный администратор сети не может обладать теми же полномочиями по конфигурированию системы защиты, которыми обладает администратор по управлению безопасностью сети.

7. **Прозрачность и простота** средств защиты. Это требование трудно реализовать на практике, оно достаточно противоречиво. Для эксплуатации СОБ лучше иметь много простых и понятных средств, чем одно сложное и трудновоспринимаемое средство. Однако для защиты от хакеров предпочтительными могут оказаться сложные и «непрозрачные» решения.

8. **Физическое разделение** серверов и рабочих станций, т. е. организация подсетей рабочих станций и серверов.

9. **Обеспечение предотвращения несанкционированного доступа** к информационным ресурсам корпоративной сети со стороны внутренних и внешних недоброжелателей. Для этого следует снабдить сеть межсетевыми средствами защиты от несанкционированного доступа, исключить коммуникационный сервер доступа к Internet из подсети функциональных серверов.

10. **Организация централизованной службы административного управления сетью**.

11. **Организация централизованной службы управления безопасностью сети**.

Функции указанных выше двух служб не должны быть совмещены в одном лице администратора сети, хотя они и являются службами сетевого управления. Необходимо предусмотреть алгоритм взаимодействия между ними, с тем, чтобы предотвратить принятие прямо противоположных решений, принимаемых администраторами для управления и защиты сети в процессе ее функционирования.

11.13. Принципы построения системы обеспечения безопасности корпоративной сети

Для построения защищенной корпоративной сети принципиально возможен выбор одной из двух концепций:

1. Создание надежной системы обеспечения безопасности (СОБ) корпоративной сети, построенной на базе каналов связи и средств коммутации общего пользования, в которой применяются открытые протоколы Internet.

2. Отказ от средств Internet, создание корпоративной сети на базе специализированной или выделенной сети связи с использованием конкретной сетевой технологии, в частности ATM, FR, ISDN.

Эти концепции представляют полярные взгляды на решение проблемы обеспечения безопасности и, как следствие, имеют определенные недостатки. Первая концепция связана с большими затратами на обеспечение надежной защиты информации при подключении сети к Internet. Вторая предлагает отказаться от услуг Internet и реализуемых в ней технологий, убедительно доказавших свою жизнеспособность и эффективность. Очевидно, что решение проблемы обеспечения безопасности корпоративной сети представляет собой некоторый компромисс между этими концепциями.

Любая система защиты по определению налагает ограничения на работу пользователей сети организационного и технического характера. Разработчикам системы обеспечения безопасности следует учитывать, что сеть создана для выполнения функций пользователей по решению задач корпорации. Поэтому одним из основных принципов создания системы комплексной защиты информации должен стать **принцип максимальной дружественности.** Не следует вводить запреты там, где без них можно обойтись, а если уж и налагать ограничения, то предварительно нужно продумать, как это сделать с минимальными неудобствами для пользователя. Следует учитывать совместимость создаваемой

системы защиты с используемой структурой корпоративной сети и сложившимися традициями фирмы.

Принцип прозрачности также связан с предыдущим. Корпоративной сетью пользуются не только высококлассные программисты. Кроме того, основное назначение корпоративной сети состоит в обеспечении производственных потребностей пользователей, то есть работы с информацией. Поэтому система защиты информации должна работать в «фоновом» режиме, быть «незаметной» и не мешать пользователям в основной работе, но при этом выполнять все возложенные на нее функции.

Принцип превентивности. Необходимо всегда помнить, что последствия реализации угроз безопасности информации могут потребовать значительно больших финансовых, временных и материальных затрат по сравнению с затратами на создание системы комплексной защиты информации.

Принцип оптимальности. Оптимальный выбор соотношения различных методов и способов парирования угроз безопасности информации при принятии решения позволит в значительной степени сократить расходы на создание системы защиты информации.

Принцип адекватности. Принимаемые решения должны быть дифференцированы в зависимости от важности, частоты и вероятности возникновения угроз безопасности информации, степени конфиденциальности самой информации и ее коммерческой стоимости.

Принцип системного подхода к построению системы защиты позволяет заложить комплекс мероприятий по парированию угроз безопасности информации уже на стадии проектирования корпоративной сети, обеспечив оптимальное сочетание организационных и инженерно-технических мер защиты информации. Важность реализации этого принципа основана на том, что оборудование действующей незащищенной корпоративной сети средствами защиты информации сложнее и дороже, чем изначальное проектирование и построение ее в защищенном варианте.

Принцип адаптивности. Система защиты информации должна строиться с учетом возможного изменения конфигурации сети, числа пользователей и степени конфиденциальности и ценности информации. При этом введение каждого нового элемента

сети или изменение действующих условий не должно снижать достигнутого уровня защищенности корпоративной сети в целом.

Принцип доказательности. При создании системы защиты информации необходимы соблюдение организационных мер внутри корпоративной сети, включая применение специальных аппаратно-программных средств идентификации, аутентификации и подтверждения подлинности информации. Реализация данного принципа позволяет сократить расходы на усложнение системы, например, применять цифровую электронную подпись только при работе с удаленными и внешними рабочими местами и терминалами, соединенными с корпоративной сетью по каналам связи.

При модернизации корпоративной сети необходимо позаботиться о модернизации системы информационной безопасности.

Эти принципы должны быть положены в основу при выборе направлений обеспечения безопасности корпоративной сети, функций и мер защиты информации.

При выборе средств защиты информации обязательно встает вопрос о необходимости подтверждения выполнения тех или иных функций конкретным средством защиты. Свидетельством того, что те или иные функции защиты реализованы конкретным средством защиты, является сертификат соответствия – документ, которым независимые эксперты подтверждают готовность средства выполнить возложенные на него задачи.

Система информационной безопасности состоит из нескольких уровней. Первым уровнем является уровень защиты рабочих станций сети.

Второй уровень защиты связан с объединением рабочих станций в локальные сети, установкой выделенных серверов и организацией выхода из локальной сети в Internet. На данном этапе вводятся в действие средства защиты второго уровня – уровня защиты локальной сети:

– средства безопасности сетевых ОС;
– средства разграничения доступа к разделяемым ресурсам;
– средства защиты домена локальной сети;
– серверы аутентификации пользователей;
– межсетевые экраны;
– средства организации VLAN;

– средства обнаружения атак и уязвимостей защиты локальной сети и т.д.

Третий уровень определяется объединением локальных сетей нескольких филиалов компании в общую корпоративную intranet-сеть на базе современных информационных технологий, используя в качестве коммуникационной среды открытые сети, включая Internet.

Построение системы информационной безопасности корпоративной сети далеко не всегда является сугубо технической задачей. Гораздо чаще оно представляет собой задачу организационно-техническую, в которой от решения организационной составляющей во многом зависит состав и сложность реализации составляющей технической. Процесс построения системы информационной безопасности включает следующие этапы:

1. Экспертиза защищенности корпоративной информационной системы.

2. Разработка концепции и политики информационной безопасности компании.

3. Проектирование корпоративной системы в защищенном исполнении.

4. Поставка и ввод в опытную эксплуатацию средств защиты.

5. Сопровождение систем информационной безопасности.

6. Модернизация и развитие систем информационной безопасности.

На первом этапе проводится экспертиза защищенности существующей или планируемой к реализации корпоративной сети, при этом рекомендуется сначала провести четкую классификацию существующих информационных ресурсов компании по степени их конфиденциальности.

На втором этапе формулируется концепция и политика информационной безопасности корпоративной сети.

На третьем этапе можно приступить непосредственно к выбору технических средств, которые в совокупности с организационными мерами позволили бы успешно решать поставленные перед подсистемой информационной безопасности задачи. При проектировании системы информационной безопасности следует также учитывать ряд общих принципов обеспечения защиты информации:

– **Экономическая эффективность**. Стоимость средств защиты должна быть меньше, чем размеры возможного ущерба.

– **Минимум привилегий**. Каждый пользователь должен иметь минимальный набор привилегий, необходимый для работы.

– **Простота**. Защита тем эффективнее, чем легче пользователю с ней работать.

– **Постоянство работы.** При нормальном функционировании защита не должна отключаться. Только в особых случаях сотрудник со специальными полномочиями может отключить систему защиты.

– **Открытость проектирования и функционирования механизмов защиты**. Специалисты, имеющие отношение к системе защиты, должны полностью представлять себе принципы ее функционирования и в случае возникновения затруднительных ситуаций адекватно на них реагировать.

– **Независимость системы защиты от субъектов защиты**. Лица, занимавшиеся разработкой системы защиты, не должны быть в числе тех, кого эта система будет контролировать.

– **Отчетность и подконтрольность**. Система защиты должна предоставлять доказательства корректности своей работы.

– **Ответственность**. Личная ответственность лиц, занимающихся обеспечением безопасности информации.

– **Изоляция и разделение**. Объекты защиты целесообразно разделять на группы таким образом, чтобы нарушение защиты в одной из групп не влияло на безопасность других.

– **Принцип враждебного окружения**. Система защиты должна проектироваться в расчете на враждебное окружение. Разработчики должны исходить из предположения, что пользователи имеют наихудшие намерения, будут совершать серьезные ошибки и искать пути обхода механизмов защиты.

– **Отсутствие излишней информации**. Существование механизмов защиты следует по возможности скрыть от пользователей, работа которых должна контролироваться.

Для некоторых типов компаний этапу ввода системы информационной безопасности в эксплуатацию должен предшествовать этап проведения аттестации на соответствие требованиям, налагаемым российским законодательством на системы защиты отдельных категорий информации. И только после подтверждения

корректности реализации системы безопасности внешним государственным органом систему можно вводить в эксплуатацию.

11.14. Законы информационной безопасности

Компания Microsoft на web-сайте регулярно публикует бюллетени и официальные документы по безопасности. Адрес англоязычного сайта Microsoft Security – http://www.microsoft.com/security. Информационные ресурсы на русском языке размещены на сайте – http://www.microsoft.com/ rus/security.

На основании многолетней практической работы в области безопасности специалистами компании сформирован список рекомендаций, получивший название «Десять непреложных заповедей обеспечения безопасности». Эти заповеди иногда называют законами информационной безопасности, соблюдение которых существенно повысит безопасность как автономных компьютеров, так и корпоративной сети.

Закон 1. Если злоумышленник сможет убедить вас, что его программа должна выполняться на вашем компьютере – это больше не ваш компьютер.

При выполнении программы ей передается полный контроль над компьютером, а значит, она может выполнить любые действия, например установить вирус, удалить или изменить файлы, сделать возможным дистанционное управление и проникновение хакеров в вашу сеть, а также установить различные вредоносные программы.

Закон 2. Если злоумышленник сможет изменить настройки вашей операционной системы – это больше не ваш компьютер.

Если хакер сможет изменить файлы операционной системы, то он может получить права администратора компьютера со всеми вытекающими последствиями.

Закон 3. Если злоумышленник имеет неограниченный физический доступ к вашему компьютеру – это больше не ваш компьютер.

В этом случае злоумышленник может просто украсть ваш компьютер, нанеся вам материальный ущерб. Однако ценность компьютера определяется не только стоимостью аппаратной части, но и ценностью содержащейся в нем информации. Получив физический доступ к вашему компьютеру, злоумышление может отформатировать жесткий диск, скопировать его содержимое, установить клавиатуру с радиопередатчиком и отследить нажатие всех клавиш, включая ваши пароли.

Закон 4. Если вы разрешите злоумышленнику загружать исполняемые программы на ваш web-сайт – это больше не ваш компьютер.

Этот закон представляет собой утверждение, обратное закону 1. В данном случае злоумышленник получит возможность загружать на ваш компьютер вредоносную программу и выполнять ее.

Закон 5. Простые пароли сводят на нет сильную систему защиты.

Если злоумышленник расшифрует ваш пароль, то он зарегистрируется в системе под вашим именем и получит все ваши права и доступ к информации.

Закон 6. Компьютер защищен ровно настолько, насколько администратор добросовестно относится к своим обязанностям.

Каждый компьютер должен обслуживаться администратором, который устанавливает программное обеспечение, конфигурирует операционную систему, устанавливает средства обеспечения безопасности, а также производит другие работы по обеспечению работоспособности. Поэтому к администраторам компьютеров, а тем более всей сети должны предъявляться высокие требования по квалификации, добросовестности по отношению к своим обязанностям, честности.

Закон 7. Зашифрованные данные защищены ровно настолько, насколько защищен ключ шифрования.

Следует иметь в виду, что каким бы хитрым ни был алгоритм кодирования, зашифрованные данные могут находиться

в безопасности до тех пор, пока в безопасности хранится ключ декодирования.

Закон 8. Устаревший антивирусный сканер не намного лучше, чем отсутствие сканера вообще.

Сканер вирусов может обнаружить только те вредоносные программы, информация о которых хранится в его базе данных. Поскольку новые вирусы создаются практически ежедневно, то необходимо регулярно обновлять базу данных антивирусных средств. Следует иметь в виду, что вирусы наносят самые крупные повреждения именно на ранних этапах своей жизни.

Закон 9. Абсолютной анонимности практически не бывает, ни в реальной жизни, ни в Интернете.

Если вы посещаете web-сайт, то его собственник может, в конце концов, определить, кто вы. Имеется множество способов замаскировать источник запросов, но ни один из них не дает полной гарантии остаться неузнанным.

Закон 10. Технологии не являются панацеей от всех бед.

Гарантированные меры безопасности требуют совершенства на таком уровне, которого просто не существует и, фактически, вряд ли может быть достигнут. Любое программное обеспечение имеет ошибки, которые можно использовать со злым умыслом и подорвать систему безопасности. Кроме того, большое влияние оказывает человеческий фактор и аспекты человеческой природы, проявляющиеся у хакеров и различных злоумышленников.

Необходимо четко уяснить два момента. Во-первых, безопасность состоит из двух составляющих – технологии и политики. Политика заключается в методологии применения технологии. Комбинация этих двух компонент, в конечном счете, определяет надежность защиты. Во-вторых, безопасность не является такой проблемой, которую можно решить раз и навсегда. Для достижения достаточно высокого уровня безопасности необходимо постоянно комбинировать современные технологии и организационные меры.

Контрольные вопросы к главе 11

1. Что такое корпоративная сеть? Опишите структуру и основные компоненты корпоративной сети.
2. Каковы основные принципы проектирования информационных систем корпоративных сетей?
3. Основные этапы проектирования информационных систем.
4. Для чего необходима система защиты информации в информационных системах и сетях?
5. Дайте определения основных понятий информационной безопасности информационных сетей и систем.
6. Каковы основные виды атак в IP-сетях?
7. В чем заключаются основные причины уязвимости IP-сетей?
8. Каковы основные цели защиты в области информационных процессов?
9. В чем заключаются особенности информационных систем распределенного типа с точки зрения защиты информации?
10. Опишите структурную схему модели информационной безопасности.
11. Каковы основные уровни уязвимости информационных систем распределенного типа?
12. Дайте характеристику основных способов и средств защиты информации в сетях.
13. Дайте классификацию компьютерных вирусов.
14. Опишите стандартные методы защиты информации в сетях.
15. Что такое межсетевой экран?
16. Что такое виртуальная частная сеть?
17. В чем заключается особенность защиты информации в беспроводных сетях?
18. Какими стандартами определяются требования к системе обеспечения безопасности сетей? Каковы основные функциональные требования к системе защиты?
19. Основные принципы построения системы безопасности сети?
20. Этапы построения системы информационной безопасности.
21. Назовите основные законы информационной безопасности.

Литература

1. Ботт Э., Зихерт К. Эффективная работа: Безопасность Windows. СПб.: Питер, 2003. – 682 с.

2. Бройдо В.Л. Вычислительные системы, сети и телекоммуникации. СПб.: Питер, 2002. – 688 с.

3. Волокитин А.В., Панкратов А.И., Солдатенков А.В., Рейман Л.Д. Интернет-технологии в Федеральной целевой программе «Электронная Россия (2002–2010 годы)»: Справочное пособие. – М., 2003. – 272 с.

4. Воройский Ф.С. Основы проектирования автоматизированных библиотечно-информационных систем. М.: ФИЗМАТЛИТ, 2002. – 384 с.

5. Галицкий А.В., Рябко С.Д., Шаньгин В.Ф. Защита информации в сети – анализ технологий и синтез решений. М.: ДМК Пресс, 2004. – 616 с.

6. Галкин В.А. Телекоммуникации и сети. М.: МГТУ им. Н.Э. Баумана, 2003. – 608 с.

7. Гук М. Аппаратные средства локальных сетей. СПб.: Питер, 2000. – 576 с.

8. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.

9. ГОСТ Р 50922-96 Защита информации. Основные термины и определения.

10. ГОСТ Р 51275-99 Защита информации. Объект информации. Факторы, воздействующие на информацию. Общие положения.

11. ГОСТ Р 51583-2000 Защита информации. Порядок создания систем в защищенном исполнении.

12. ГОСТ Р ИСО/МЭК 15408-х-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий»

13. ГОСТ 34.601-90 «Автоматизированные системы. Стадии создания»

14. ГОСТ 34.602-89 «Техническое задание на создание автоматизированной системы»

15. ГОСТ 34.603-92 «Виды испытаний АС»

16. ГОСТ 34.601-90 «Автоматизированные системы. Стадии создания»

17. ГОСТ 34.602-89 «Техническое задание на создание автоматизированной системы»

18. ГОСТ 34.603-92 «Виды испытаний АС»

19. Камышников В.В. Основы сетевой архитектуры Internet. Самара: Издательство «Самарский университет», 2001. – 107 с.

20. Корниенко А.А., Яковлев В.В. Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта. М.: УМК МПС России, 2002. – 328 с.

21. Коннов В.В., Клековкин Г.А., Коннова Л.П. Геометрическая теория графов. М.: Народное образование, 1999. – 240 с.

22. Кулыгин М. Технологии корпоративных сетей: Энциклопедия. – СПб.: Питер, 2000. – 704 с.

23. Курило А.П. и др. Обеспечение информационной безопасности бизнеса. – М.: ВДС-пресс, 2005. – 512с.

24. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. 2-е изд., СПб.: Питер, 2004. – 864 с.

25. Пятибратов А.П., Гудыно Л.П., Кириченко А.А. Вычислительные системы, сети и телекоммуникации/ Под ред. Пятибратова А.П. М.: Финансы и статистика, 2001. – 512 с.

26. Роб П., Коронел К. Системы баз данных: проектирование, реализация и управление. 5-е изд. Перераб. И доп.: Пер с англ. – СПб.: БХВ-Петербург, 2004. – 1040 с.

27. Родичев Ю.А., Чарковский К.В. Принципы проектирования корпоративных информационных сетей образовательных учреждений. Вестник СамГТУ. Серия: Физико-математические науки. 2003, выпуск 19 с. 150-155

28. Родичев А.Ю., Родичев Ю.А. Системная модель защиты информации информационных систем распределенного типа. Вестник Самарского гос. ун-та. 2003., № 2, с.15-20

29. Родичев Ю.А. Элементы теории корпоративных информационных систем сферы подготовки и развития интеллекта. Вестник Самарского гос. ун-та. 2004., № 2, с. 176-187

30. Семенов А.Б., Стрижаков С.К., Сунчелей И.Р. Структурированные кабельные системы. 3-е изд. – М.: Лайт Лтд, 2001, – 608 с.

31. Соколов А.В., Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах. – М.: ДМК Пресс, 2002. – 656 с.

32. Танненбаум Э. Компьютерные сети. 4-е изд., МПб.: Питер, 2003. – 992 с.

33. Титоренко Г.А. Методы и средства построения систем информационной безопасности. Их структура. 2-е издание, дополненное. – М., 2003. – 205 с.

34. Титоренко Г.А. Информационные технологии управления. Уч. пособие для вузов. 2- изд., доп. – М.: ЮНИТИ-ДАНА, 2003. – 439 с.

35. Уткин В.Б. Информационные системы и технологии в экономике. М.: ЮНИТИ-ДАНА, 2003. – 335 с.

36. Шамраев А.В. Правовое регулирование информационных технологий (анализ проблем и основные документы). Версия 1.0. М.: «Статут», «Интертех», «БЦД-пресс», 2003. – 1013 с.

37. Шикин Е.В., Чхартишвили А.Г. Математические методы и модели в управлении: Учебное пособие для студентов управленческих специальностей вузов/ – М.: Дело, 2002. – 440 с.

38. Яковлев В.В., Корниенко А.А. Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта. М.: УМК МПС России, 2002. – 328 с.

39. Information Security. Информационная безопасность. № 1, 2005.

Интернет-ресурсы

1. http://www. educom. ru/ru/projects/programs/development/
2. http://www. citforum. ru/
3. http://www. citforum. ru/internet/infsecure/
4. http://www. osp/ru
5. http://www. kaspersky. ru
6. http://www. uni. ru
7. http://www. infosec. ru/
8. http://www. ibm. com/ru
9. http://www. nic. ru/
10. http://internet. ru/
11. http://www. doctorweb. com/

12. http://www. ieee802. org/11
13. http://www. wi-fi. org/
14. http://microsoft. com/rus/security/
15. http://www. hp. ru
16. http://www. intel. com/ru
17. http://www/infotecs/ru/
18. http://www. itsec. ru/

Юрий Андреевич Родичев

КОМПЬЮТЕРНЫЕ СЕТИ: АРХИТЕКТУРА, ТЕХНОЛОГИИ, ЗАЩИТА

Учебное пособие для вузов.

Корректор: Н.В. Голубева
Компьютерная верстка, макет А.Ю. Гречищев

Подписано в печать 27.12.05
Гарнитура Times New Roman. Формат 60x84/16. Бумага офсетная. Печать оперативная.
Усл.-печ. л. 29,25. Уч.-изд. л. 20,5. Тираж 300 экз. Заказ № 381
Издательство «Универс-групп», 443011, Самара, ул. Академика Павлова, 1
Отпечатано ООО «Универс-групп»