Учреждение образования
«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

П. П. Урбанович,
Д. М. Романенко, Е. В. Кабак

КОМПЬЮТЕРНЫЕ СЕТИ

Допущено
Министерством образования Республики Беларусь
в качестве учебного пособия для студентов высших
учебных заведений по техническим специальностям

Минск 2011

УДК 004.056(075.8)
БКК 32.97я7
У 69

Р е ц е н з е н т ы :
доктор технических наук, профессор,
проректор по научной работе УО «Гомельский
государственный университет им. Ф. Скорины» *О. М. Демиденко*;
кандидат технических наук, доцент кафедры ЭВМ
УО «Белорусский государственный университет информатики
и радиоэлектроники» *А. В. Отвагин*

Урбанович, П. П.

У 69 Компьютерные сети : учеб. пособие для студентов высших учебных заведений по техническим специальностям / П. П. Урбанович, Д. М. Романенко, Е. В. Кабак. – Минск : БГТУ, 2011. – 400 с.

ISBN 978-985-530-044-2.

В учебном пособии в простой и доступной форме даны общие понятия компьютерных сетей, их структуры, сетевых компонентов, а также перспективы развития. Приведены виды топологий для соединения компьютеров в сети, методы доступа к каналу связи, физические среды передачи данных. Описаны правила и процедуры передачи данных между информационными системами, типы сетевого оборудования, их назначение и принципы работы. Представлены наиболее популярные сетевые операционные системы, их достоинства и недостатки. Рассмотрены принципы межсетевого взаимодействия, основные понятия из области сетевой безопасности.

Предназначено для студентов технических специальностей, также может быть полезно аспирантам, изучающим избранные аспекты по вышеуказанным вопросам.

УДК 004.056(075.8)
ББК 32.97я7

ISBN 978-985-530-044-2

ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ

Дисциплина «Компьютерные сети» представляет собой введение в сетевую тематику и дает базовые знания по организации и функционированию сетей.

Из опыта преподавания данной и других смежных дисциплин известно, что структура одно- или двухсеместрового курса сильно отличается от структуры краткого курса по тому же предмету. В данной книге основные понятия, общие подходы в проектировании компьютерных сетей, особенности различных видов и топологий сетей, их программного и аппаратного обеспечения и практического использования авторы пытались изложить в контексте унифицированной структуры. При этом предполагалось, что читатель знаком с основами информационных технологий.

Основная задача пособия – дать студентам общие систематизированные сведения об организации и структуре важной отрасли, которая затрагивает профессиональные, бытовые, познавательно-развлекательные сферы жизнедеятельности человека, которая интенсивно меняется, развивается. В целом, в учебном пособии в простой и доступной форме даны общие понятия компьютерных сетей, их структуры, сетевых компонентов, а также перспективы развития. Приведены виды топологий, используемые для физического соединения компьютеров в сети, методы доступа к каналу связи, физические среды передачи данных. Передача данных в сети рассматривается на базе эталонной базовой модели, разработанной Международной организацией по стандартам взаимодействия открытых сетей. Также в издании приводятся правила и процедуры передачи данных между информационными системами, типы сетевого оборудования, их назначение и принципы работы. Описывается сетевое программное обеспечение, используемое для организации сетей. Изучаются наиболее популярные сетевые операционные системы, их достоинства и недостатки. Рассматриваются принципы межсетевого взаимодействия. Приводятся основные принципы безопасности в сетях передачи данных, касающиеся главным образом симметричного шифрования и шифрования с открытыми ключами, цифровых подписей, помехоустойчивых кодов, методов и средств защиты от удаленных атак.

При создании и использовании любой сети всегда возникает множество больших и маленьких проблем. Описание способов решения некоторых из них также рассмотрено в данном пособии. При этом основное внимание уделяется решению технических вопросов, которые возникают при ежедневном обслуживании компьютерной сети, в частности диагностика функционирования протокола TCP/IP.

Теоретический материал учебного пособия дополнен иллюстрациями, которые в наглядной форме поясняют теоретические основы сетевых технологий, а также представляют их практическую реализацию.

В конце издания приведены русско- и англоязычные термины и понятия, англоязычные сокращения и предметный указатель, которые упрощают процесс пользования книгой и работы с материалом.

Пособие предназначено для студентов технических специальностей высших учебных заведений, получающих образование в области информационных технологий. Однако может быть полезна и студентам других специальностей, а также студентам средних специальных учебных заведений, для которых авторы рекомендуют ограничиться материалами 1–3, 5, 6, 8, 10 разделов.

1. ПРЕДПОСЫЛКИ И ЭТАПЫ РАЗВИТИЯ СЕТЕЙ. ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ И ТЕРМИНЫ

1.1. История развития компьютерных и вычислительных сетей

Концепция вычислительных сетей является логическим результатом эволюции компьютерной технологии. Первые компьютеры 50-х годов были большими, громоздкими и дорогими. Такие компьютеры не были предназначены для интерактивной работы, а использовались в режиме пакетной обработки.

Системы пакетной обработки, как правило, строились на базе *мэйнфрейма* – мощного и надежного компьютера универсального назначения. Подготавливались перфокарты, содержащие данные и команды программ, и передавались 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, *интерактивный режим* работы, при котором можно с терминала оперативно руководить процессом обработки своих данных, был бы гораздо удобней. Но интересами программистов и 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 задач, чем любые другие режимы. Наибольшее значение предавалось эффективности работы самого дорогого устройства вычислительной машины – процессора, в ущерб эффективности работы использующих его специалистов.

1.1.1. Многотерминальные системы – прообраз сети

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 (*рис. 1.1*).

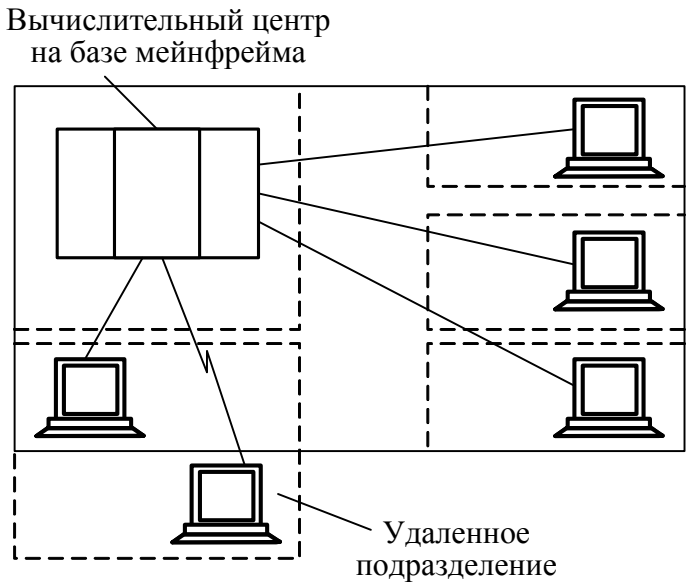


Рис. 1.1. Многотерминальная система – прообраз вычислительной сети

В таких системах компьютер использовали сразу несколько программистов-пользователей. Причем время реакции вычислительной системы было настолько малым, что пользователь не замечал параллельной работы с компьютером других программистов-пользователей.

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*. Такие многотерминальные централизованные системы внешне уже были очень похожи на локальные вычислительные сети. Действительно, рядовой программист-пользователь работу за терминалом мэйнфрейма воспринимал примерно так же, как сейчас он воспринимает работу за подключенным к сети персональным компьютером.

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 централизованный характер 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 – их суммарная мощность оказывалась намного ниже мощности дорогой машины.

1.1.2. Появление глобальных сетей

Тем не менее, потребность в соединении компьютеров, находящихся на большом расстоянии друг от друга, к этому времени вполне назрела.

В 1962 году Американское агентство исследовательских проектов Министерства обороны США (Advanced Research Projects Agency of the U.S. Department of Defense, ARPA) начало реализацию проекта, который позднее получил название ARPANET и из которого позднее вырос современный Интернет (Internet).

В 1962 году важные исследования были начаты в ряде учебных заведений США и прежде всего в Массачусетском технологическом институте (MIT). Именно в 1962 году молодой американский ученый из MIT Дж. С. Ликлидер написал работу, где высказал идею *глобальной сети*, которая обеспечивала бы каждому жителю земли доступ к данным и программам из любой точки земного шара. В это же время другой ученый Л. Клейнрок закончил работу над своей докторской диссертацией в области теории коммуникационных сетей.

В 1963 году происходит важное событие: появляется первый универсальный **стандарт ASCII** – схема кодирования, назначающая численные значения-коды буквам, цифрам, знакам пунктуации и некоторым другим символам, в результате чего возникает возможность обмена информацией между компьютерами от различных изготовителей.

В 1964 году практически одновременно в MIT, RAND Corporation и Great Britain National Physical Laboratory (GBNPL) были развернуты работы по надежной передаче информации. Появилась идея *коммутации пакетов*, суть которой сводилась к тому, что любая информация, передаваемая по сети, разбивается на несколько частей (пакетов), которые затем независимо друг от друга перемещаются различными путями (маршрутами), пока не достигнут адресата. П. Бэран, Д. Дэвис, Л. Клейнрок параллельно вели исследования в этой области. П. Бэран был одним из первых, кто опубликовал свои исследования в статье «Передача данных в сетях».

В 1967 году произошло событие, которое сыграло важную роль в развитии сетевых технологий: модем, изобретенный в начале шестидесятых, был существенно усовершенствован Дж. Ван Гином из Станфордского научно-исследовательского института (Stanford Research Institute, SRI). Ученый предложил приемник, который мог надежно распознавать биты информации на фоне шумовых помех, создаваемых междугородними телефонными линиями. В 1967 году Л. Робертс организовал научную конференцию в Анн-Арбор в штате Мичиган, на которую он пригласил основных разработчиков сетевого проекта. Конференция имела огромное значение – параллельно проводимые работы начали объединяться. Термин «ARPANET» впервые упоминался в ходе выступления Л. Робертса именно на этой конференции. На этой же конференции другой выдающийся ученый У. Кларк впервые высказал идею и предложил термин «IMP» – Interface Message Processors, обозначающий *устройства для управления трафиком в сети*, которые впоследствии эволюционировали в современные маршрутизаторы.

В 1968 году началась работа по созданию IMP и уже через один год, в 1969 году, заработала сеть **ARPANET**, охватившая все Западное побережье США.

В 1970 году наблюдался рост сети – каждый месяц добавляется новый узел. В этом же году произошло еще два важных события. Во-первых, Д. Ритчи и К. Томпсон из BelLabs закончили работу над созданием операционной системы UNIX. Во-вторых, в этом же году рабочая группа NWG (Network Working Group) под руководством С. Крокера завершила работу над протоколом NCP (Network Control Protocol), а еще годом позже закончила работу над *протоколом эмуляции терминала* (*Telnet*) и существенно

продвинулась в работе над *протоколом передачи файлов* (*FTP*). В 1971 году BBN разработала новую платформу – так называемые TIP-устройства (Terminal IMP, Terminal Interface Processor), что обеспечило возможность входить на удаленные хосты, сделав, таким образом, ARPANET доступной большему числу пользователей.

В 1972 году сеть ARPANET была публично продемонстрирована. Однако в этом же году произошло еще, по крайней мере, два события, которые оказали огромное влияние на развитие компьютерных технологий: Р. Томильсон написал программу, позволяющую отправлять *электронную почту* по ARPANET, ввел обозначение «*user@host*» и использовал символ *@*, который позднее (с 1980 года) был закреплен в международном стандарте адресов электронной почты. Постепенно сеть ARPANET расширялась, и среди клиентов появились такие частные организации, как BBN, Xerox PARC и MITRE Corporation, а также государственные – NASA's Ames Research Laboratories, National Bureau of Standards и Air Force Research Facilities.

В 1973 году фирма ARPA переименовывается в DARPA, где буква «D» указывает на Defense (защита, оборона). DARPA (Defense Advanced Research Projects Agency) – агенство перспективного планирования оборонных научно-исследовательских работ, центральная научно-исследовательская организация министерства обороны, основной целью которой является выдача рекомендаций по внедрению принципиально новых технологий для военной промышленности. Под руководством Б. Кана начинается весьма сложная работа по объединению сетей, имеющих разные интерфейсы, скорости передачи данных и размеры пакетов. По сути дела, это была работа по созданию *межсетевого протокола*. В сентябре 1973 году появилась первая публикация по новому протоколу *TCP* (Transmition Control Protocol). TCP/IP со временем стал одним из наиболее популярных протоколов сетевого взаимодействия и стандартом для реализации глобальных сетевых соединений в силу открытости, масштабируемости и за счет предоставления одинаковых возможностей глобальным и локальным сетям.

В 1977 году был анонсирован компьютер Apple II, и появление настольных компьютеров с потенциальной возможностью коммуникаций при помощи модемного подключения дало новый толчок развитию *сетевых технологий* и *модемной* индустрии. К началу 1978 года эксперимент ARPANET был практически

закончен. Годом позже появилась служба USENET4, которая стала одним из первых примеров клиент-серверной организации.

К концу семидесятых годов архитектура и протоколы TCP/IP приобрели современный вид. К этому времени агентство DARPA стало признанным лидером в разработке сетей с коммутацией пакетов. Дальнейшее развитие сетевых технологий, в том числе беспроводных радиосетей и спутниковых каналов связи, стимулировало активность DARPA в исследовании проблем межсетевого взаимодействия и реализации принципов Интернета в ARPANET. DARPA не делало тайны из своей деятельности в области развития технологий Интернета, поэтому различные научные группы проявляли интерес к разработкам технологии глобальной сети.

Свое начало Интернет берет от сети ARPANET, но чаще Интернет называют наследницей NSFNET – американской сети, объединившей ученых NSF (National Science Foundation), которая сотрудничала, объединялась с ARPANET, а затем поглотила ее.

Многие эксперты называют временем зарождения Интернета начало 80-х годов. В это время DARPA инициировало перевод машин, подсоединенных к его исследовательским сетям, на использование стека TCP/IP. В 1981 году IWG (Internet Working Group) в DARPA публикует документ, в котором говорится о полном переходе с протокола NCP (Network Control Protocol) на протокол TCP/IP. С этих пор ARPANET становится магистральной сетью Интернет и активно используется для многочисленных экспериментов с TCP/IP. Окончательный переход к технологии Интернет произошел в январе 1983 года: в этом году протокол TCP/IP был принят Министерством обороны США, а сеть ARPANET была разбита на две независимые части. Одна из них, предназначенная для научных целей, сохранила название ARPANET, а вторая, большая по масштабу сеть MILNET, отошла к военному ведомству.

Для того чтобы стимулировать использование новых протоколов в учебных заведениях, DARPA сделало реализацию TCP/IP широко доступной для университетских кругов. В это время многие исследователи использовали версию ОС Unix университета Беркли (штат Калифорния), называемую BSD Unix (от Berkeley Software Distribution). Благодаря тому, что DARPA в свое время субсидировала компанию BBN и университет в Беркли с целью реализации протоколов TCP/IP для использования вместе с популярной ОС Unix, более 90% компьютерных факультетов университетов

адаптировали новую сетевую технологию, и версия BSD стала фактическим стандартом для реализаций стека протоколов TCP/IP. Было выпущено несколько версий BSD, каждая из которых добавляла в TCP/IP новые возможности, в том числе 4.2BSD (1983 год), 4.3BSD (1986 год), 4.3BSD Tahoe (1988 год), 4.3BSD Reno (1990 год), 4.4BSD (1993 год).

С 1985 года NSF реализовала программу создания сетей вокруг своих суперкомпьютерных центров. И в 1986 году создание опорной сети (56 Кбит/с) между суперкомпьютерными центрами NSF привело к появлению целого ряда региональных сетей, таких как JVNCNET, NYSERNET, SURANET, SDSCNET, BARRNET и других. Так появилась магистральная сеть NSFNET, которая в конце концов объединила все эти научные центры и связала их с ARPANET. Таким образом, NSFNET связала пять суперкомпьютерных центров и открыла доступ к мощным вычислительным ресурсам для широкого круга исследователей. Для уменьшения платы за использование междугородних линий связи решено было развивать систему *региональных сетей*, которая объединяет компьютеры внутри какого-то региона и имеет выходы на подобные сети поблизости. При такой конфигурации все компьютеры являются равноправными и имеют связь «по цепочке» через соседние компьютеры как друг с другом, так и с суперкомпьютерами NSF. Таким образом, начиная с 1986 года можно говорить о становлении глобальной компьютерной сети Интернет.

В 1988 году Интернет становится международной сетью – к нему присоединяются Канада, Дания, Финляндия, Франция, Норвегия и Швеция. Годом позже сеть уже насчитывала 80 000 узлов; в ноябре к Интернету присоединились Австрия, Германия, Израиль, Италия, Япония, Мексика, Нидерланды, Новая Зеландия и Великобритания – и вскоре количество узлов в сети выросло до 160 000. В том же году появилась технология FDDI (Fiber Distributed Data Interface) – распределенный *интерфейс передачи данных по волоконно-оптическим каналам*.

Если Интернет – изобретение коллективное, то идею гипертекста и WWW связывают с именем конкретного человека. В 1989 году Т. Бернерс-Ли высказал идею гипертекста, которая и послужила толчком к созданию *World Wide Web*. Т. Бернерс-Ли написал программу *Eniquire*, которая стала прообразом будущей WWW. В том же 1989 году Т. Бернерс-Ли начал работу над глобальным проектом

Всемирной паутины, и всего два года спустя (в 1991 году) первые WWW-объекты были помещены в Интернет.

1.1.3. Первые локальные сети

В начале 70-х годов произошел технологический прорыв в области производства компьютерных компонентов – появились большие интегральные схемы. Их сравнительно невысокая стоимость и высокие функциональные возможности привели к созданию мини-компьютеров, которые стали реальными конкурентами мэйнфреймов. Закон Гроша перестал соответствовать действительности, так как десяток мини-компьютеров выполнял некоторые задачи (как правило, хорошо распараллеливаемые) быстрее одного мэйнфрейма, а стоимость такой *мини-компьютерной* системы была меньше.

Даже небольшие подразделения предприятий получили возможность покупать для себя компьютеры. Мини-компьютеры выполняли задачи управления технологическим оборудованием, складом и другие задачи уровня подразделения предприятия. Таким образом, появилась концепция распределения компьютерных ресурсов по всему предприятию. Однако при этом все компьютеры одной организации по-прежнему продолжали работать автономно (*рис. 1.2*).

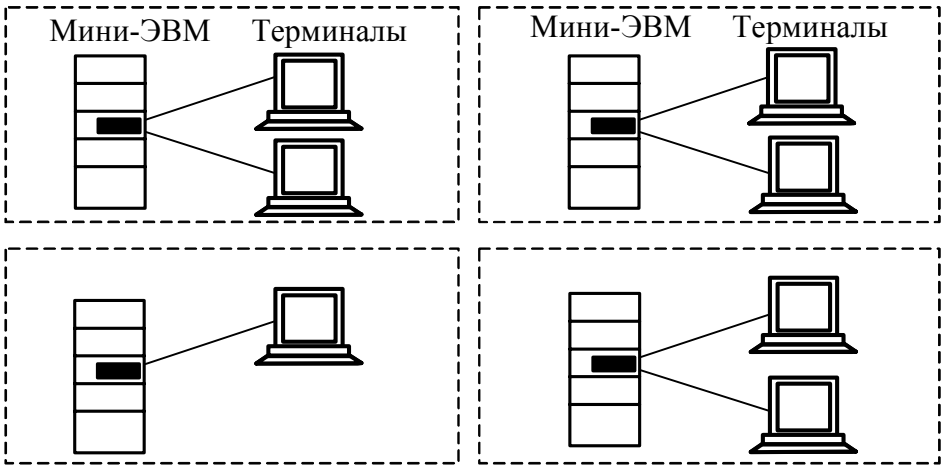


Рис. 1.2. Автономное использование нескольких мини-компьютеров на одном предприятии

Позднее предприятия и организации стали соединять свои мини-компьютеры вместе и разрабатывать программное обеспечение,

необходимое для их взаимодействия. В результате появились первые *локальные вычислительные сети* (*рис. 1.3*). Они еще во многом отличались от современных локальных сетей, в первую очередь, своими устройствами сопряжения.

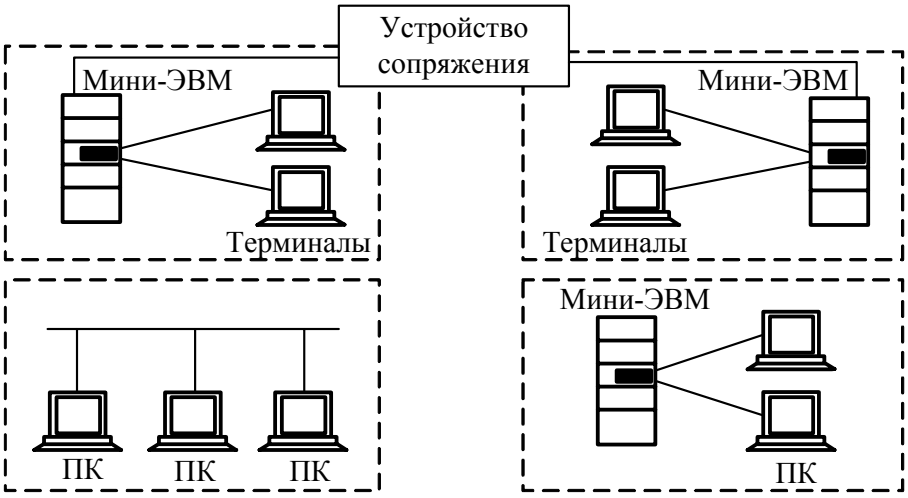


Рис. 1.3. Различные типы связей
в первых локальных сетях

На первых порах для соединения компьютеров друг с другом использовались самые разнообразные нестандартные устройства со своим способом представления данных на линиях связи, своими типами кабелей и т. п.

1.1.4. Создание стандартных технологий локальных сетей

В середине 80-х годов положение дел в локальных сетях стало кардинально меняться. Утвердились стандартные технологии объединения компьютеров в сеть – Ethernet, Arcnet, Token Ring. Мощным стимулом для их развития послужили персональные компьютеры, которые 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.

Стандартные сетевые технологии превратили процесс построения локальной сети из искусства в рутинную работу. 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, NetWare.

Локальные сети в сравнении с глобальными внесли много нового в способы организации работы пользователей. Доступ к разделяемым ресурсам стал гораздо удобнее – пользователь мог просто просматривать списки имеющихся ресурсов, а не запоминать их идентификаторы или имена. После соединения с удаленным ресурсом можно было работать с ним с помощью уже знакомых пользователю по работе с локальными ресурсами команд. Возможность реализовать все нововведения разботчики локальных сетей получили в результате появления качественных кабельных линий связи, на которых даже сетевые адаптеры первого поколения обеспечивали скорость передачи данных до 10 Мбит/с.

Наибольшее распространение на тот момент получили телефонные каналы связи, но они были плохо приспособлены для высокоскоростной передачи *дискретных* данных – скорость в 1200 бит/с была для них хорошим достижением. Поэтому экономное расходование *пропускной способности* каналов связи часто являлось основным критерием эффективности методов передачи данных в глобальных сетях.

1.1.5. Современные тенденции развития компьютерных вычислительных сетей

Сегодня компьютерные сети продолжают развиваться, причем достаточно быстро. Разрыв между локальными и глобальными сетями постоянно сокращается во многом из-за появления высокоскоростных территориальных каналов связи, не уступающих по качеству кабельным системам локальных сетей.

Изменяются и локальные сети. Вместо соединяющего компьютеры пассивного кабеля в них в большом количестве появилось разнообразное *коммуникационное оборудование* – коммутаторы, маршрутизаторы, шлюзы. Благодаря такому оборудованию появилась возможность построения больших корпоративных сетей, насчитывающих тысячи компьютеров и имеющих сложную структуру. Возродился интерес к крупным компьютерам, в основном из-за того, что после спада эйфории по поводу легкости работы с персональными компьютерами выяснилось, что системы, состоящие из сотен серверов, обслуживать слож-

нее, чем несколько больших компьютеров. Поэтому на новом витке эволюционной спирали мэйнфреймы стали возвращаться в *корпоративные вычислительные системы*, но уже как полноправные сетевые узлы, поддерживающие Ethernet или Token Ring, а также стек протоколов TCP/IP, ставший благодаря Internet сетевым стандартом де-факто.

Проявилась еще одна очень важная тенденция, затрагивающая в равной степени как локальные, так и глобальные сети. В них стала обрабатываться несвойственная ранее вычислительным сетям информация – голос, видеоизображения, рисунки. Это потребовало внесения изменений в работу протоколов, сетевых операционных систем и коммуникационного оборудования. Сложность передачи такой мультимедийной информации по сети связана с ее чувствительностью к задержкам при передаче пакетов данных, задержки обычно приводят к искажению такой информации в конечных узлах сети. Так как традиционные службы вычислительных сетей, такие как передача файлов или электронная почта, создают малочувствительный к задержкам трафик и все элементы сетей разрабатывались в расчете на него, то появление трафика реального времени привело к большим проблемам.

Сегодня эти проблемы решаются различными способами, в том числе и с помощью специально рассчитанной на передачу различных типов трафика технологии ATM. Однако, несмотря на значительные усилия, предпринимаемые в этом направлении, до приемлемого решения проблемы пока далеко. И в этой области предстоит еще много сделать, чтобы достичь заветной цели – слияния технологий не только локальных и глобальных сетей, но и технологий любых информационных сетей – вычислительных, телефонных, телевизионных и т. п. Хотя эта идея многим кажется утопией, серьезные специалисты считают, что предпосылки для такого синтеза уже существуют, и их мнения расходятся только в оценке примерных сроков такого объединения – называются сроки от 10 до 25 лет. Причем считается, что основой для объединения послужит технология коммутации пакетов, применяемая сегодня в вычислительных сетях, а не технология коммутации каналов, используемая в телефонии, что, наверно, должно повысить интерес к сетям этого типа.

1.2. Основные понятия и определения

Сеть – это совокупность объектов, образуемых устройствами передачи и обработки данных. Международная организация по стандартизации определила компьютерную сеть *как последовательную бит-ориентированную передачу информации между связанными друг с другом независимыми устройствами*.

В общем случае различают два понятия сети: коммуникационная сеть и информационная сеть (*рис. 1.4*).

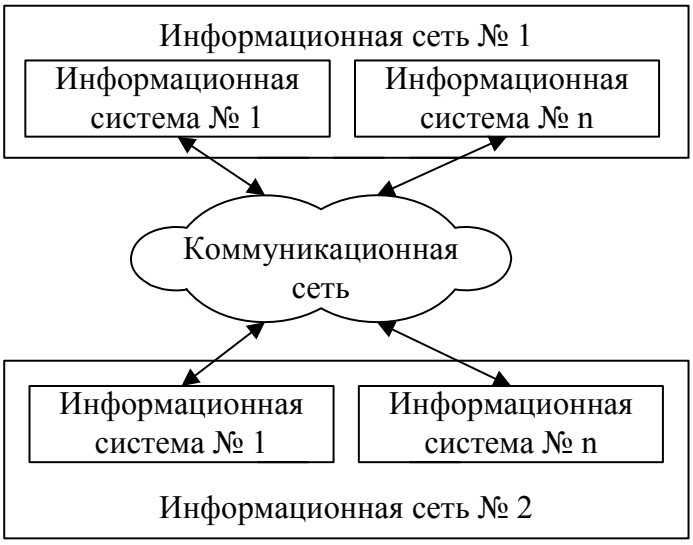


Рис. 1.4. Информационные и коммуникационные сети

Коммуникационная сеть предназначена для передачи данных, также она выполняет задачи, связанные с преобразованием данных. Коммуникационные сети различаются по типу используемых физических средств соединения.

Информационная сеть предназначена для хранения информации и состоит из *информационных систем*. На базе коммуникационной сети может быть построена группа информационных сетей.

Под **информационной системой** следует понимать систему, которая является поставщиком или потребителем информации.

Вычислительная сеть – это одна из разновидностей распределенных систем, предназначенная для распараллеливания вычислений, за счет чего может быть достигнуто повышение производительности и отказоустойчивости системы.

В общем, компьютерная сеть состоит из информационных систем и каналов связи.

Под **информационной системой** в данном случае следует понимать объект, способный осуществлять хранение, обработку или передачу информации. В состав информационной системы входят: компьютеры, программы, пользователи и другие составляющие, предназначенные для процесса обработки и передачи данных. В дальнейшем информационная система, предназначенная для решения задач пользователя, будет называться **рабочей станцией** (**client**). Рабочая станция в сети отличается от обычного персонального компьютера (ПК) наличием **сетевой карты** (**сетевого адаптера**), канала для передачи данных и сетевого программного обеспечения.

Под **каналом связи** следует понимать путь или средство, по которому передаются сигналы. Средство передачи сигналов называют ***физическим каналом***. **Абонентский канал** – это физический канал, соединяющий коммуникационную сеть с абонентской системой. Параметры и характеристики абонентского канала в точке подключения системы определяются абонентским интерфейсом.

Каналы связи создаются по **линиям связи** при помощи сетевого оборудования и физических средств связи. Физические средства связи построены на основе витых пар, коаксиальных кабелей, оптических каналов или эфира. Между взаимодействующими информационными системами через физические каналы коммуникационной сети и узлы коммутации устанавливаются *логические каналы*.

Логический канал – это путь для передачи данных от одной системы к другой. Логический канал прокладывается по маршруту в одном или нескольких физических каналах. Логический канал можно охарактеризовать как маршрут, проложенный через физические каналы и узлы коммутации.

Информация в сети передается **блоками данных** по процедурам обмена между объектами. Эти процедуры называют **протоколами передачи данных**.

Протокол – это совокупность правил, устанавливающих формат и процедуры обмена информацией между двумя или несколькими устройствами.

Интерфейс – совокупность средств и методов взаимодействия между элементами или устройствами системы. Интерфейсы являются основой взаимодействия всех современных информационных

систем. Если интерфейс какого-либо объекта (рабочей станции, сетевой карты, программы и т. д.) не изменяется (стандартизирован), это дает возможность модифицировать сам объект, не перестраивая принципы его взаимодействия с другими объектами.

Загрузка сети характеризуется параметром, называемым трафиком.

Трафик – это поток сообщений в сети передачи данных. Под ним понимают количественное измерение в выбранных точках сети числа проходящих блоков данных и их длины, выраженное в битах в секунду.

Существенное влияние на характеристику сети оказывает метод доступа.

Метод доступа – это способ определения того, как сеть управляет доступом к каналу связи (кабелю), что существенно влияет на ее характеристики. В сети все рабочие станции физически соединены между собою каналами связи по определенной структуре, называемой топологией.

Топология – это описание физических соединений в сети, указывающее какие рабочие станции могут связываться между собой. Тип топологии определяет производительность, работоспособность и надежность эксплуатации рабочих станций, а также время обращения к файловому серверу. В зависимости от топологии сети используется тот или иной метод доступа.

Состав основных элементов в сети зависит от ее архитектуры.

Архитектура – это концепция, определяющая взаимосвязь, структуру и функции взаимодействия рабочих станций в сети. Она предусматривает логическую, функциональную и физическую организацию технических и программных средств сети. Архитектура определяет принципы построения и функционирования аппаратного и программного обеспечения элементов сети.

1.3. Классификации компьютерных сетей

Чаще всего термин «*локальные сети*» или «**локальные вычислительные сети**» (LAN, Local Area Network) понимают буквально, то есть это такие сети, которые имеют небольшие, локальные размеры, соединяют близкорасположенные компьютеры. Однако некоторые локальные сети легко обеспечивают связь на

расстоянии нескольких десятков километров. Это уже размеры не комнаты, не здания, не близкорасположенных зданий, а может быть, даже целого города. С другой стороны, по глобальной сети (WAN, Wide Area Network или GAN, Global Area Network) вполне могут связываться компьютеры, находящиеся на соседних столах в одной комнате.

Как правило, локальная сеть связывает от двух до нескольких десятков компьютеров. Но предельные возможности современных локальных сетей гораздо выше: максимальное число абонентов может достигать тысячи. Называть такую сеть малой неправильно.

В пределах одной сети могут использоваться как электрические кабели различных типов (витая пара, коаксиальный кабель), так и оптоволоконные кабели.

По сути, компьютеры, связанные локальной сетью, объединяются в один виртуальный компьютер, ресурсы которого могут быть доступны всем пользователям, причем этот доступ не менее удобен, чем к ресурсам, входящим непосредственно в каждый отдельный компьютер. Под удобством в данном случае понимается высокая реальная скорость доступа, скорость обмена информацией между приложениями, практически незаметная для пользователя.

Скорость передачи по локальной сети обязательно должна расти по мере роста быстродействия наиболее распространенных компьютеров.

Таким образом, главное отличие локальной сети от любой другой – высокая скорость передачи информации по сети. Но это еще не все, не менее важны и другие факторы. В частности, принципиально необходим низкий уровень *ошибок* передачи, вызванных как внутренними, так и внешними факторами. Ведь даже очень быстро переданная информация, которая искажена ошибками, просто не имеет смысла, ее придется передавать еще раз. Поэтому локальные сети обязательно используют специально прокладываемые высококачественные и хорошо защищенные от помех линии связи.

Особое значение имеет и такая характеристика сети, как возможность работы с большими нагрузками, то есть с высокой интенсивностью обмена (или, как еще говорят, с большим *трафиком*). Ведь если механизм управления обменом, используемый в сети, не слишком эффективен, то компьютеры могут подолгу ждать своей очереди на передачу.

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

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

– *высокая скорость передачи* информации, большая пропускная способность сети; приемлемая скорость сейчас – не менее 10 Мбит/с;

– *низкий уровень ошибок передачи* (или, что то же самое, высококачественные каналы связи); допустимая вероятность ошибок передачи данных не должна превышать порядок 10^{-8}–10^{-12};

– эффективный, быстродействующий механизм управления обменом по сети;

– заранее четко ограниченное количество компьютеров, подключаемых к сети.

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

Нередко выделяют еще один класс компьютерных сетей – **городские**, **региональные** сети (MAN, Metropolitan Area Network), которые обычно по своим характеристикам ближе к глобальным сетям, хотя иногда все-таки имеют некоторые черты локальных сетей, например, высококачественные каналы связи и сравнительно высокие скорости передачи. В принципе городская сеть может быть локальной со всеми ее преимуществами.

Сейчас нельзя провести четкую границу между локальными и глобальными сетями. Большинство локальных сетей имеет выход в глобальную. Но характер передаваемой информации, принципы

организации обмена, режимы доступа к ресурсам внутри локальной сети, как правило, сильно отличаются от тех, что приняты в глобальной сети.

По локальной сети может передаваться самая разная цифровая информация: данные, изображения, телефонные разговоры, электронные письма и т. д. Кстати, именно задача передачи изображений, особенно полноцветных динамических, предъявляет самые высокие требования к быстродействию сети. Чаще всего локальные сети используются для разделения (совместного использования) таких ресурсов, как дисковое пространство, принтеры и выход в глобальную сеть, но это всего лишь незначительная часть тех возможностей, которые предоставляют средства локальных сетей.

1.4. Вычислительные сети – частный случай распределенных систем

Компьютерные сети относятся к **распределенным** (или децентрализованным) **вычислительным системам**. Поскольку основным признаком распределенной вычислительной системы является наличие нескольких центров обработки данных, то наряду с компьютерными сетями к распределенным системам относят также *мультипроцессорные* компьютеры.

В **мультипроцессорных компьютерах** имеется несколько процессоров, 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.

Сам по себе процессорный блок не является законченным компьютером и поэтому не может выполнять программы без остальных блоков мультипроцессорного компьютера – памяти и периферийных устройств. Все периферийные устройства являются для всех процессоров мультипроцессорной системы общими. *Территориальную распределенность* мультипроцессор не поддерживает – все его блоки располагаются в одном или нескольких близкорасположенных конструктивах, как и у обычного компьютера.

Основное достоинство мультипроцессора – его высокая производительность, которая достигается за счет параллельной работы нескольких процессоров.

Еще одним важным свойством мультипроцессорных систем является **отказоустойчивость**, то есть способность к продолжению работы при отказах некоторых элементов, например, процессоров или блоков памяти.

Многомашинная система – это вычислительный комплекс, включающий в себя несколько 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.

Работа любой многомашинной системы определяется двумя главными компонентами: высокоскоростным механизмом связи процессоров и системным программным обеспечением, которое предоставляет пользователям и приложениям прозрачный доступ к ресурсам всех компьютеров, входящих в комплекс. В состав средств связи входят программные модули, которые занимаются распределением *вычислительной нагрузки*, *синхронизацией вычислений* и *реконфигурацией системы*. Если происходит отказ одного из компьютеров комплекса, его задачи могут быть автоматически переназначены и выполнены на другом компьютере. Если в состав многомашинной системы входят несколько контроллеров внешних устройств, то в случае отказа одного из них, другие контроллеры автоматически подхватывают его работу. Таким образом, достигается высокая отказоустойчивость комплекса в целом.

Многомашинные системы позволяют достичь высокой производительности за счет организации *параллельных* вычислений. По сравнению с мультипроцессорными системами возможности параллельной обработки в многомашинных системах ограничены: эффективность распараллеливания резко снижается, если параллельно выполняемые задачи тесно связаны между собой по данным.

В вычислительных сетях программные и аппаратные связи являются более слабыми, а автономность обрабатывающих блоков проявляется в наибольшей степени – основными элементами сети являются стандартные компьютеры, не имеющие ни общих блоков

памяти, ни общих периферийных устройств. Связь между компьютерами осуществляется с помощью специальных периферийных устройств – *сетевых адаптеров*, соединенных относительно протяженными каналами связи. Каждый компьютер работает под управлением собственной операционной системы, а какая-либо «общая» операционная система, распределяющая работу между компьютерами сети, отсутствует. Взаимодействие между компьютерами сети происходит за счет передачи сообщений через сетевые адаптеры и каналы связи. С помощью этих сообщений один компьютер обычно запрашивает доступ к локальным ресурсам другого компьютера. Такими ресурсами могут быть как данные, хранящиеся на диске, так и разнообразные периферийные устройства – принтеры, модемы, факс-аппараты и т. д. Разделение локальных ресурсов каждого компьютера между всеми пользователями сети – основная цель создания вычислительной сети.

На тех компьютерах, ресурсы которых должны быть доступны всем пользователям сети, необходимо добавить модули (приложения), которые постоянно будут находиться в режиме ожидания *запросов*, поступающих по сети от других компьютеров. Обычно такие модули называются *серверными приложениями* или **программными серверами (server)**, так как их главная задача – обслуживать запросы на доступ к ресурсам своего компьютера. На компьютерах, пользователи которых хотят получать доступ к ресурсам других компьютеров, также нужно добавить к операционной системе некоторые специальные программные модули, которые должны вырабатывать запросы на доступ к удаленным ресурсам и передавать их по сети на нужный компьютер. Такие модули обычно называют *клиентскими приложениями* или **программными клиентами (client)**. Сетевые адаптеры и каналы связи решают в сети достаточно простую задачу – они передают сообщения с запросами и ответами от одного компьютера к другому, а основную работу по организации совместного использования ресурсов выполняют клиентские и серверные части операционных систем.

Пара модулей «*клиент – сервер*» обеспечивает совместный доступ пользователей к определенному типу ресурсов, например, к файлам. В этом случае говорят, что пользователь имеет дело с файловой службой (service). Обычно сетевая операционная система поддерживает несколько видов сетевых служб для своих

пользователей – файловую службу, службу печати, службу электронной почты, службу удаленного доступа и т. п.

Термины «клиент» и «сервер» используются не только для обозначения 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 (более подробно это описано в пункте 2.1.3). Иногда (в распределенных системах) один и тот же компьютер может одновременно играть роль и сервера, и клиента.

Сетевые службы всегда представляют собой распределенные программы.

Распределенная программа – это программа, которая состоит из нескольких взаимодействующих частей, причем каждая часть, как правило, выполняется на отдельном компьютере сети.

В сети могут выполняться и распределенные пользовательские программы – *приложения*. Распределенное приложение также состоит из нескольких частей, каждая и которых выполняет какую-то определенную законченную работу по решению прикладной задачи. Например, одна часть приложения, выполняющаяся на компьютере пользователя, может поддерживать специализированный графический интерфейс, вторая – работать на мощном выделенном компьютере и заниматься статистической обработкой введенных пользователем данных, а третья – заносить полученные результаты в базу данных на компьютере с установленной стандартной **СУБД** (системой управления базами данных).

Распределенные приложения в полной мере используют потенциальные возможности распределенной обработки, предоставляемые вычислительной сетью, и поэтому часто называются сетевыми приложениями.

1.5. Основные программные и аппаратные компоненты сети

Вычислительная сеть – это сложный комплекс взаимосвязанных и согласованно функционирующих программных и аппаратных компонентов. Изучение сети в целом предполагает знание принципов работы ее отдельных элементов:

- компьютеров;
- коммуникационного оборудования;
- операционных систем;
- сетевых приложений.

Весь комплекс программно-аппаратных средств сети может быть описан *многослойной моделью*. В основе любой сети лежит аппаратный слой стандартизованных компьютерных платформ.

В настоящее время в сетях широко и успешно применяются компьютеры различных классов – от персональных до мэйнфреймов и суперЭВМ. Набор компьютеров в сети должен соответствовать набору разнообразных задач, решаемых сетью.

Второй слой – это коммуникационное оборудование. Хотя компьютеры и являются центральными элементами обработки данных в сетях, в последнее время не менее важную роль стали играть коммуникационные устройства. Кабельные системы, повторители, мосты, коммутаторы, маршрутизаторы и модульные концентраторы из вспомогательных компонентов сети превратились в основные наряду с компьютерами и системным программным обеспечением как по влиянию на характеристики сети, так и по стоимости. Сегодня коммуникационное устройство может представлять собой сложный специализированный мультипроцессор, который нужно конфигурировать, оптимизировать и администрировать. Изучение принципов работы коммуникационного оборудования требует знакомства с большим количеством протоколов, используемых как в локальных, так и глобальных сетях.

Третьим слоем, образующим программную платформу сети, являются операционные системы (ОС). От того, какие концепции управления локальными и распределенными ресурсами положены в основу сетевой ОС, зависит эффективность работы всей сети. При проектировании сети важно учитывать, насколько просто данная операционная система может взаимодействовать с другими ОС сети, насколько она обеспечивает безопасность и защищенность данных, до какой степени она позволяет наращивать число пользователей, можно ли перенести ее на компьютер другого типа и многие другие соображения.

Самым верхним слоем сетевых средств являются различные сетевые приложения, такие как сетевые базы данных, почтовые системы, средства архивирования данных, системы автоматизации

коллективной работы и др. Очень важно представлять диапазон возможностей приложений для различных областей применения, а также знать, насколько они совместимы с другими сетевыми приложениями и операционными системами.

1.6. Преимущества и недостатки использования сетей

Основные преимущества сетей вытекают из их принадлежности к распределенным системам.

Концептуальным преимуществом распределенных систем (а значит, и сетей) перед централизованными системами является их способность выполнять параллельные вычисления. За счет этого в системе с несколькими обрабатывающими узлами в принципе может быть достигнута производительность, превышающая максимально возможную на данный момент производительность любого отдельного, сколь угодно мощного процессора. Распределенные системы потенциально имеют лучшее соотношение производительность – стоимость, чем централизованные системы.

Еще одно очевидное и важное достоинство распределенных систем – это их принципиально более высокая отказоустойчивость. Основой повышенной отказоустойчивости распределенных систем является **избыточность**. Избыточность обрабатывающих узлов (процессоров в многопроцессорных системах или компьютеров в сетях) позволяет при отказе одного узла переназначать приписанные ему задачи на другие узлы. С этой целью в распределенной системе могут быть предусмотрены процедуры динамической или статической реконфигурации. В вычислительных сетях некоторые наборы данных могут дублироваться на внешних запоминающих устройствах нескольких компьютеров сети, так что при отказе одного их них данные остаются доступными.

Для пользователя, кроме вышеназванных, распределенные системы дают еще и такие преимущества, как возможность совместного использования данных и устройств, а также возможность гибкого распределения работ по всей системе. Такое разделение дорогостоящих периферийных устройств, таких как дисковые

массивы большой емкости, цветные принтеры, графопостроители, модемы, оптические диски, во многих случаях является основной причиной развертывания сети на предприятии.

В последнее время стал преобладать другой побудительный мотив развертывания сетей, гораздо более важный в современных условиях, чем экономия средств за счет разделения между сотрудниками корпорации дорогой аппаратуры или программ. Этим мотивом стало стремление обеспечить сотрудникам оперативный доступ к обширной корпоративной информации. В условиях жесткой конкурентной борьбы в любом секторе рынка выигрывает, в конечном счете, та фирма, сотрудники которой могут быстро и правильно ответить на любой вопрос клиента: о возможностях их продукции, об условиях ее применения, о решении любых возможных проблем и т. п. В большой корпорации вряд ли даже хороший менеджер может знать все тонкости каждого из выпускаемых фирмой продуктов, тем более что их номенклатура обновляется сейчас каждый квартал, если не месяц. Поэтому очень важно, чтобы менеджер имел возможность со своего компьютера, подключенного к корпоративной сети, скажем, в Минске, передать вопрос клиента на сервер, расположенный в центральном отделении предприятия в Жодино, и оперативно получить качественный ответ, удовлетворяющий клиента. В этом случае клиент не обратится к другой фирме, а будет пользоваться услугами данного менеджера и впредь.

Этот аспект сетевой работы всегда был «узким местом» в организации доставки информации сотрудникам – даже при существовании мощных СУБД информация в них попадала не самая «свежая» и не в том объеме, который был нужен. В последнее время в этой области наметился некоторый прогресс, связанный с использованием гипертекстовой информационной службы WWW – так называемой технологии **Intranet**. Эта технология поддерживает достаточно простой способ представления текстовой и графической информации в виде гипертекстовых страниц, что позволяет быстро поместить самую свежую информацию на WWW-серверы корпорации. Кроме того, она унифицирует просмотр информации с помощью стандартных программ – Web-*браузеров*, работа с которыми несложна даже для неспециалиста.

Корпоративная сеть – сеть, которая интегрирует данные и мультимедийную информацию, может использоваться для организации аудио- и видеоконференций. Кроме того, на ее основе может быть создана собственная внутренняя телефонная сеть.

Конечно, вычислительные сети имеют и свои проблемы. Эти проблемы в основном связаны с организацией эффективного взаимодействия отдельных частей распределенной системы.

Во-первых, это сложности, связанные с программным обеспечением – операционными системами и приложениями. Программирование для распределенных систем принципиально отличается от программирования для централизованных систем. Так, сетевая операционная система, выполняя в общем случае все функции по управлению локальными ресурсами компьютера, сверх того решает многочисленные задачи по предоставлению сетевых служб. Разработка сетевых приложений осложняется из-за необходимости организовать совместную работу их частей, выполняющихся на разных машинах.

Во-вторых, много проблем связано с транспортировкой сообщений по каналам связи между компьютерами. Основные задачи здесь – обеспечение *надежности* (чтобы передаваемые данные не терялись и не искажались) и производительности (чтобы обмен данными происходил с приемлемыми задержками). В структуре общих затрат на вычислительную сеть расходы на решение транспортных вопросов составляют существенную часть, в то время как в централизованных системах эти проблемы полностью отсутствуют.

В-третьих, это вопросы, связанные с обеспечением безопасности, которые гораздо сложнее решаются в вычислительной сети, чем в централизованной системе. В некоторых случаях, когда безопасность особенно важна, от использования сети лучше вообще отказаться.

ВЫВОДЫ

1. Компьютерная сеть – это совокупность компьютеров, соединенных линиями связи. Линии связи образованы кабелями (или построены на основе беспроводных технологий), сетевыми адаптерами и другими коммуникационными устройствами. Все

сетевое оборудование работает под управлением системного и прикладного программного обеспечения.

2. Основная задача сети – обеспечить пользователям потенциальную возможность совместного использования ресурсов всех компьютеров.

3. Вычислительная сеть – это одна из разновидностей распределенных систем, достоинством которых является возможность распараллеливания вычислений, за счет чего может быть достигнуто повышение производительности и отказоустойчивости системы.

4. Важнейшим этапом в развитии сетей явилось появление стандартных сетевых технологий типа Ethernet, позволяющих быстро и эффективно объединять компьютеры различных типов.

5. Использование сетей предоставляет следующие возможности:
- разделение дорогостоящих ресурсов;
- совершенствование коммуникаций;
- улучшение доступа к информации;
- быстрое и качественное принятие решений;
- свобода в территориальном размещении компьютеров.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Дайте определение сети.

2. Чем отличается коммуникационная сеть от информационной сети?

3. Как разделяются сети по территориальному признаку?

4. Что такое информационная система?

5. Что такое каналы связи?

6. Дайте определение физического канала связи.

7. Дайте определение логического канала связи.

8. Как называется совокупность правил обмена информацией между двумя или несколькими устройствами?

9. Что такое метод доступа?

10. Привести основные методы доступа, используемые в компьютерных сетях.

11. Что такое совокупность правил, устанавливающих процедуры и формат обмена информацией?

12. Чем отличается рабочая станция в сети от обычного персонального компьютера?

13. Как называется описание физических соединений в сети?

14. Что такое архитектура сети?

15. Как называется способ определения рабочей станции, которая будет следующей использовать канал связи?

16. Перечислите преимущества использования сетей.

17. Назначения компьютерных сетей с архитектурой терминал – главный компьютер.

18. Чем отличается одноранговая архитектура от клиент-серверной архитектуры?

19. Каковы преимущества крупномасштабной сети с выделенным сервером?

20. Какие сервисы предоставляет клиент-серверная архитектура?

21. Как называются рабочие станции, которые используют ресурсы сервера?

22. Что такое сервер?

2. ОБЩИЕ ПРИНЦИПЫ ПОСТРОЕНИЯ СЕТЕЙ

2.1. Архитектура сетей

Архитектура сети определяет основные элементы сети, характеризует ее общую логическую организацию, техническое обеспечение, программное обеспечение, описывает методы кодирования. Архитектура также определяет принципы функционирования и интерфейс пользователя.

В данном пособии будут рассмотрены три вида архитектур:

- архитектура *терминал – главный компьютер*;
- *одноранговая* архитектура;
- архитектура *клиент – сервер*.

2.1.1. Архитектура терминал – главный компьютер

Архитектура терминал – главный компьютер (terminal – host computer architecture) – это концепция информационной сети, в которой вся обработка данных осуществляется одним или группой главных компьютеров (*рис. 2.1*).

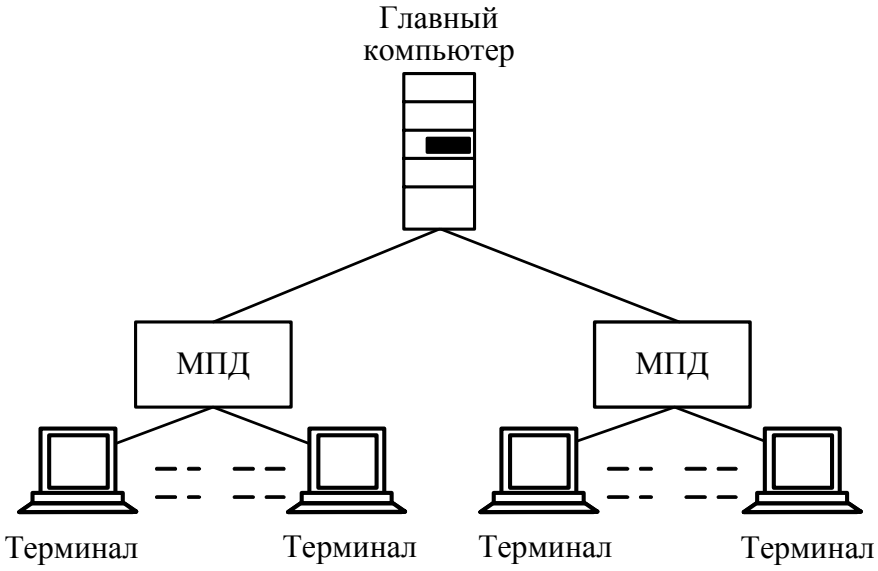


Рис. 2.1. Архитектура терминал – главный компьютер

Рассматриваемая архитектура предполагает два типа оборудования:

– главный компьютер, на котором осуществляется управление сетью, хранение и обработка данных;

– терминалы, предназначенные для передачи главному компьютеру команд на организацию сеансов и выполнение заданий, для ввода данных и получения результатов.

Главный компьютер через *мультиплексоры* передачи данных (МПД) взаимодействует с терминалами, как представлено на *рис. 2.1*. Классический пример архитектуры сети с главными компьютерами – системная сетевая архитектура (System Network Architecture, SNA).

2.1.2. Одноранговая архитектура

Одноранговая архитектура (peer-to-peer architecture) – это концепция информационной сети, в которой ее ресурсы рассредоточены по всем взаимодействующим между собой системам (*рис. 2.2*). Данная архитектура характеризуется тем, что в ней все системы равноправны.

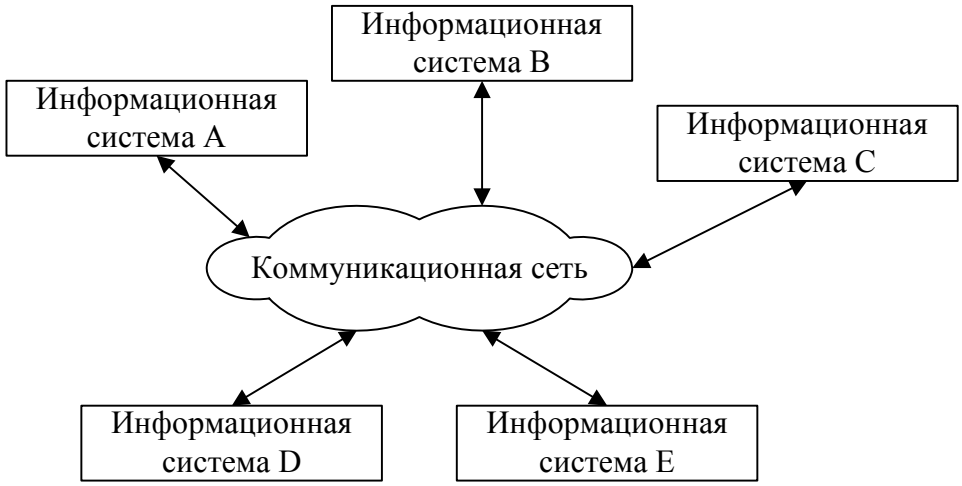


Рис. 2.2. Одноранговая архитектура

К одноранговым сетям относятся малые сети, где любая рабочая станция может выполнять одновременно функции файлового сервера и рабочей станции. В одноранговых ЛВС дисковое пространство и файлы на любом компьютере могут быть общими. Чтобы ресурс стал общим, его необходимо отдать в общее пользование, используя службы удаленного доступа сетевых одноранго-

вых операционных систем. В зависимости от того, как будет установлена защита данных, другие пользователи смогут пользоваться файлами сразу же после их создания. Одноранговые ЛВС достаточно хороши только для небольших рабочих групп.

Одноранговые ЛВС являются наиболее легким и дешевым типом сетей для установки. Они требуют на компьютере, кроме сетевой карты и сетевого носителя, наличие пользовательской операционной системы. При соединении компьютеров, пользователи могут предоставлять ресурсы и информацию в совместное пользование.

Одноранговые сети имеют следующие преимущества:

– легки в установке и настройке;
– отдельные ПК не зависят от выделенного сервера;
– пользователи в состоянии контролировать свои ресурсы;
– малая стоимость и легкая эксплуатация;
– минимум оборудования и программного обеспечения;
– нет необходимости в администраторе;
– хорошо подходят для сетей с количеством пользователей, не превышающим десяти.

Проблемой одноранговой архитектуры является ситуация, когда компьютеры отключаются от сети. В этих случаях из сети исчезают виды сервиса, которые они предоставляли. Сетевую безопасность одновременно можно применить только к одному ресурсу, и пользователь должен помнить столько паролей, сколько сетевых ресурсов. При получении доступа к разделяемому ресурсу ощущается падение производительности компьютера. Существенным недостатком одноранговых сетей является отсутствие централизованного администрирования.

Использование одноранговой архитектуры не исключает применения в той же сети также архитектуры терминал – главный компьютер или архитектуры клиент – сервер.

2.1.3. Архитектура клиент – сервер

Архитектура клиент – сервер (client – server architecture) – это концепция информационной сети, в которой основная часть ее ресурсов сосредоточена в серверах, обслуживающих своих клиентов (*рис. 2.3*). Рассматриваемая архитектура определяет два типа компонентов: серверы и клиенты.

Сервер – это объект, предоставляющий сервис другим объектам сети по их запросам. **Сервис** – это процесс обслуживания клиентов.

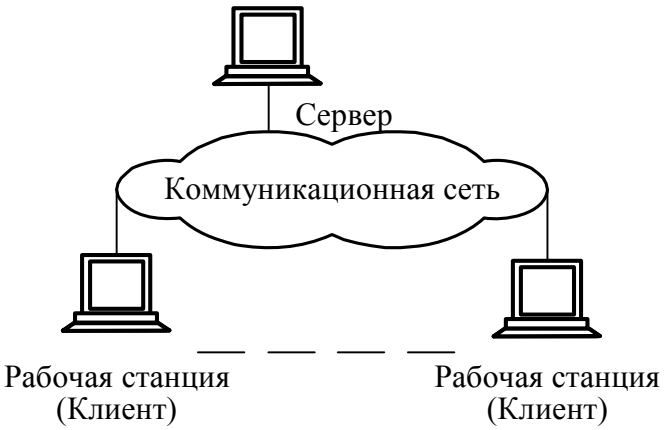


Рис. 2.3. Архитектура клиент – сервер

Сервер работает по заданиям клиентов и управляет выполнением их заданий. После выполнения каждого задания сервер посылает полученные результаты клиенту, пославшему это задание.

Сервисная функция в архитектуре клиент – сервер описывается комплексом прикладных программ, в соответствии с которым выполняются разнообразные прикладные процессы.

Процесс, который вызывает сервисную функцию с помощью определенных операций, называется клиентом. Им может быть программа или пользователь. На *рис. 2.4* приведен перечень сервисов в архитектуре клиент – сервер.

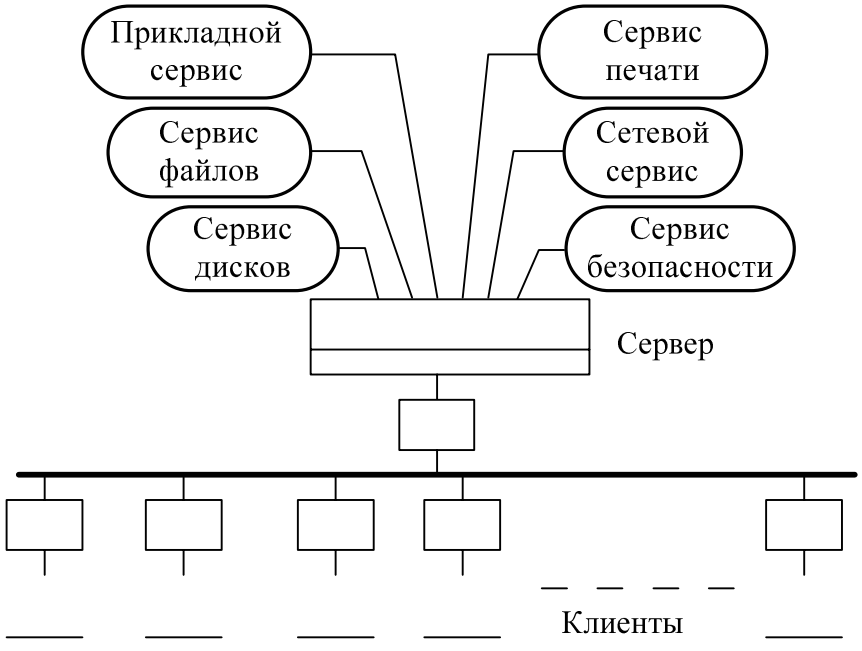


Рис. 2.4. Модель клиент – сервер

Клиенты – это рабочие станции, которые используют ресурсы сервера и предоставляют удобные интерфейсы пользователя. **Интерфейсы пользователя** – это процедуры взаимодействия пользователя с системой или сетью.

Клиент является инициатором и использует электронную почту или другие сервисы сервера. В этом процессе клиент запрашивает вид обслуживания, устанавливает сеанс, получает нужные ему результаты и сообщает об окончании работы.

В **сетях с выделенным файловым сервером** на выделенном автономном ПК (персональном компьютере) устанавливается серверная сетевая операционная система. Этот ПК становится сервером. Программное обеспечение (ПО), установленное на рабочей станции, позволяет ей обмениваться данными с сервером. Наиболее распространенные сетевые операционная системы:

- NetWare фирмы Novel;
- Windows фирмы Microsoft;
- UNIX фирмы AT&T;
- Linux.

Помимо сетевой операционной системы, необходимы сетевые прикладные программы, реализующие преимущества, предоставляемые сетью.

Сети на базе серверов имеют лучшие характеристики и повышенную надежность. Сервер владеет главными ресурсами сети, к которым обращаются остальные рабочие станции.

В современной клиент-серверной архитектуре выделяется четыре группы объектов: клиенты, серверы, данные и сетевые службы. Клиенты располагаются в системах на рабочих местах пользователей. Данные в основном хранятся на серверах. Сетевые службы являются совместно используемыми серверами и данными. Кроме того, службы управляют процедурами обработки данных.

Сети клиент-серверной архитектуры имеют следующие преимущества:

– позволяют организовывать сети с большим количеством рабочих станций;

– обеспечивают централизованное управление учетными записями пользователей, безопасностью и доступом, что упрощает сетевое администрирование;

– эффективный доступ к сетевым ресурсам;

– пользователю нужен один пароль для входа в сеть и для получения доступа ко всем ресурсам, на которые распространяются права пользователя.

Наряду с преимуществами сети клиент-серверной архитектуры имеют и ряд недостатков:

– неисправность сервера может сделать сеть неработоспособной либо, как минимум, привести к потере сетевых ресурсов;

– требуют квалифицированного персонала для администрирования;

– имеют более высокую стоимость сетей и сетевого оборудования.

2.1.4. Выбор архитектуры сети

Выбор архитектуры сети зависит от назначения сети, количества рабочих станций и от выполняемых на ней действий.

Следует выбирать одноранговую сеть, если:

– количество пользователей не превышает десяти;

– все машины находятся близко друг от друга;

– имеют место небольшие финансовые возможности;

– нет необходимости в специализированном сервере, таком как сервер БД, факс-сервер или какой-либо другой;

– нет возможности или необходимости в централизованном администрировании.

Следует выбирать клиент-серверную сеть, если:

– количество пользователей превышает десять;

– требуется централизованное управление, безопасность, управление ресурсами или резервное копирование;

– необходим специализированный сервер;

– нужен доступ к глобальной сети;

– требуется разделять ресурсы на уровне пользователей.

Выводы

1. Существуют три основные архитектуры сети: терминал – главный компьютер, одноранговая и клиент-серверная. В настоящее время наибольшее распространение получили одноранговая и клиент-серверная архитектуры.

2. Ключевой особенностью одноранговой архитектуры является рассредоточенность ресурсов по всем взаимодействующим между собой системам. Данная архитектура характеризуется тем, что в ней все системы равноправны.

3. Важнейшим моментом клиент-серверной архитектуры сети является то, что основная часть ее ресурсов сосредоточена в серверах, обслуживающих своих клиентов. В клиент-серверной архитектуре выделяется четыре группы объектов: клиенты, серверы, данные и сетевые службы. Клиенты располагаются в системах на рабочих местах пользователей. Данные в основном хранятся в серверах. Сетевые службы являются совместно используемыми серверами и данными, кроме того службы обычно управляют процедурами обработки данных.

4. Выбор архитектуры сети осуществляется в зависимости от назначения сети, количества узлов и от выполняемых в ней действий.

2.2. Топология компьютерной сети

2.2.1. Понятие и виды топологии

Понятие **топологии** широко используется при создании сетей. Одним из подходов к классификации топологий ЛВС является выделение двух основных классов топологий: широковещательные и последовательные.

В **широковещательных топологиях** ПК передает сигналы, которые могут быть восприняты остальными ПК. К таким топологиям относятся топологии: общая шина, дерево, звезда.

В **последовательных топологиях** информация передается только одному ПК. Примерами таких топологий являются: произвольная (произвольное соединение ПК), кольцо, цепочка.

При выборе оптимальной топологии преследуются три основные цели:

– обеспечение *альтернативной маршрутизации* и максимальной надежности передачи данных;

– выбор *оптимального маршрута* передачи блоков данных;

– предоставление приемлемого *времени ответа* и нужной *пропускной способности*.

При выборе конкретного типа сети важно учитывать ее топологию. Основными сетевыми топологиями являются: шинная (линейная) топология, звездообразная, кольцевая и древовидная.

Например, в конфигурации сети ArcNet используется одновременно и линейная, и звездообразная топология. Сети Token Ring физически выглядят как звезда, но логически их пакеты передаются по кольцу. Передача данных в сети Ethernet происходит по линейной шине, так что все станции видят сигнал одновременно.

Существуют пять основных топологий:

- *общая шина* (Bus);
- *кольцо* (Ring);
- звезда (Star);
- *древовидная* (Tree);
- *сеточная*, *ячеистая* (Mesh).

Также возможны комбинации нескольких различных топологий.

2.2.2. Топология общая шина

Общая шина – это тип сетевой топологии, в которой рабочие станции расположены вдоль одного участка кабеля, называемого *сегментом* (*рис. 2.5*).

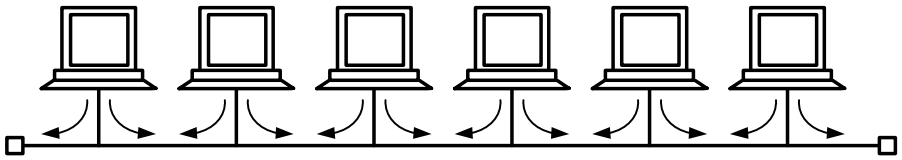


Рис. 2.5. Топология **общая шина**

Топология *общая шина* предполагает использование одного кабеля, к которому подключаются все компьютеры сети. В случае топологии общая шина кабель используется всеми станциями по очереди. Для уменьшения зашумленности среды отраженными сигналами, мешающими передаче данных, используют так называемые **терминаторы** – специальные резистры на концах кабеля, предотвращающие появление «отраженной волны».

Все сообщения, посылаемые отдельными компьютерами, принимаются и прослушиваются всеми остальными компьютерами, подключенными к сети. Рабочая станция отбирает адресованные ей сообщения, пользуясь **адресной информацией**. Надежность здесь выше, так как выход из строя отдельных компьютеров не

нарушит работоспособность сети в целом. Поиск неисправности в сети затруднен. Кроме того, так как используется только один кабель, в случае обрыва нарушается работа всей сети. Шинная топология – это наиболее простая и наиболее распространенная топология сети.

Примерами использования топологии общая шина является сеть 10Base-5 (соединение ПК толстым коаксиальным кабелем) и 10Base-2 (соединение ПК тонким коаксиальным кабелем).

2.2.3. Кольцевая топология

Кольцо – это топология ЛВС, в которой каждая рабочая станция соединена с двумя другими рабочими станциями, образуя кольцо (*рис. 2.6*). Данные передаются от одной рабочей станции к другой в одном направлении (по кольцу).

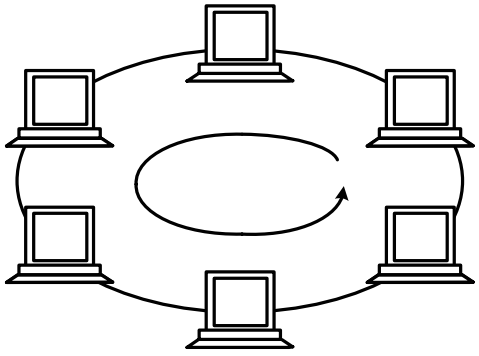


Рис. 2.6. Топология **кольцо**

Каждая рабочая станция выполняет роль **повторителя**, ретранслируя сообщения к следующей рабочей станции, т. е. данные передаются от одного компьютера к другому как по эстафете. Если компьютер получает данные, предназначенные для другого компьютера, он передает их дальше по кольцу, в ином случае они дальше не передаются.

Основная проблема при кольцевой топологии заключается в том, что каждая рабочая станция должна активно участвовать в пересылке информации, и в случае выхода из строя хотя бы одной из них, вся сеть парализуется. Подключение новой рабочей станции требует краткосрочного выключения сети, так как во время установки кольцо должно быть разомкнуто. Топология кольцо имеет хорошо предсказуемое время отклика, определяемое числом рабочих станций.

Чистая кольцевая топология используется редко. Вместо этого кольцевая топология играет транспортную роль в схеме метода доступа. Кольцо описывает логический маршрут, а пакет передается от одной станции к другой, совершая в итоге полный круг.

В сетях ***Token Ring*** кабельная ветвь из центрального концентратора называется MAU (Multiple Access Unit). MAU имеет внутреннее кольцо, соединяющее все подключенные к нему станции, и используется как альтернативный путь, когда оборван или отсоединен кабель одной рабочей станции. Когда кабель рабочей станции подсоединен к MAU, он просто образует расширение кольца: сигналы поступают к рабочей станции, а затем возвращаются обратно во внутреннее кольцо.

2.2.4. Топология звезда

Звезда – это топология ЛВС (*рис. 2.7*), в которой все рабочие станции присоединены к центральному узлу (например, к концентратору), который устанавливает, поддерживает и разрывает связи между рабочими станциями.

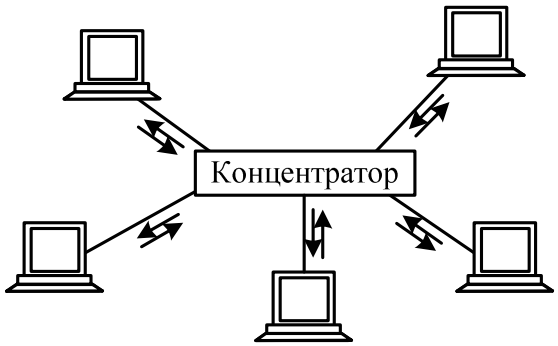


Рис. 2.7. Топология **звезда**

Преимуществом такой топологии является возможность простого исключения неисправного узла. Однако, если неисправен центральный узел, вся сеть выходит из строя. В этом случае каждый компьютер через специальный сетевой адаптер подключается отдельным кабелем к объединяющему устройству.

При необходимости можно объединять вместе несколько сетей с топологией звезда, при этом получаются разветвленные конфигурации сети. В каждой точке ветвления необходимо использовать специальные соединители (распределители, повторители или устройства доступа).

Примером звездообразной топологии является топология **Ethernet** с кабелем типа **витая пара** 10BASE-T, 100BASE-T и т. д. *Центром* звезды обычно является **hub** (**хаб**, **концентратор**).

Звездообразная топология обеспечивает защиту от разрыва кабеля. Если кабель рабочей станции будет поврежден, это не приведет к выходу из строя всего сегмента сети. Она позволяет также легко диагностировать проблемы подключения, так как каждая рабочая станция имеет свой собственный кабельный сегмент, подключенный к концентратору. Для диагностики достаточно найти разрыв кабеля, который ведет к неработающей станции. Остальная часть сети продолжает нормально работать.

Однако звездообразная топология имеет и недостатки. Во-первых, она требует для организации сети большое количество кабеля. Во-вторых, концентраторы довольно дороги. В-третьих, кабельные концентраторы при большом количестве кабеля трудно обслуживать. Однако в большинстве случаев в такой топологии используется недорогой кабель типа витая пара. В некоторых случаях можно даже использовать существующие телефонные кабели. Кроме того, для диагностики и тестирования выгодно собирать все кабельные концы в одном месте. По сравнению с концентраторами **ArcNet** концентраторы Ethernet и MAU Token Ring достаточно дороги. Новые подобные концентраторы включают в себя средства тестирования и диагностики, что делает их еще более дорогими.

2.2.5. Другие типы топологии

Кроме трех рассмотренных базовых топологий нередко применяется также сетевая топология **дерево** (**tree**), которую можно рассматривать как комбинацию нескольких звезд. Причем, как и в случае звезды, дерево может быть активным или истинным (*рис. 2.8*).

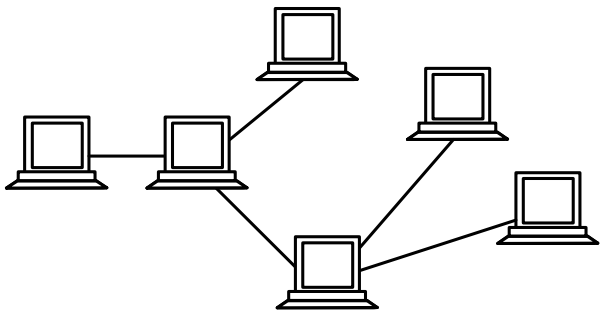


Рис. 2.8. Топология **активное дерево**

Также дерево может быть пассивным (*рис. 2.9*). При **активном дереве** в центрах объединения нескольких линий связи находятся центральные компьютеры, а при **пассивном** – концентраторы (хабы).

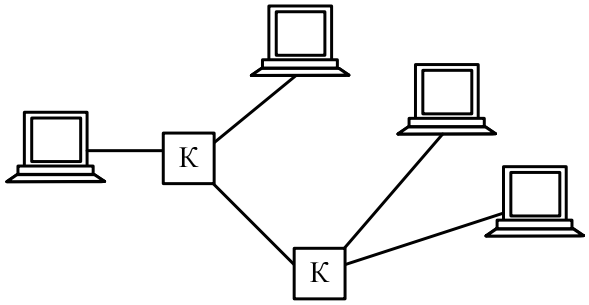


Рис. 2.9. Топология **пассивное дерево**
(К – концентраторы)

Сетевая топология **fat tree (утолщенное дерево)**, изобретенная Чарльзом Лейзерсоном, является дешевой и эффективной для суперкомпьютеров (*рис. 2.10*).

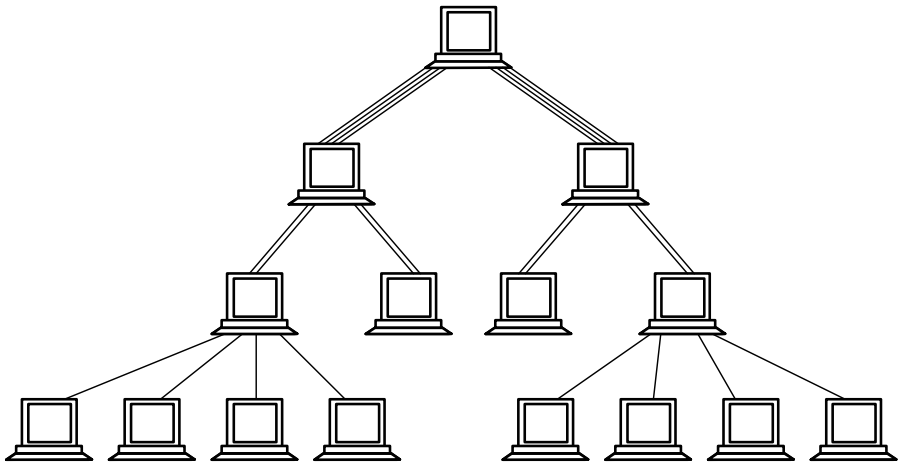


Рис. 2.10. Топология **fat tree**

В отличие от классической топологии дерево, в которой все связи между узлами одинаковы, связи в утолщенном дереве становятся более широкими (производительными по пропускной способности) с каждым уровнем по мере приближения к корню дерева. Часто используют удвоение пропускной способности на каждом уровне. Сети с топологией fat tree являются предпочтительными для построения кластерных межсоединений.

Довольно часто применяются комбинированные топологии, среди которых наиболее распространены **звездно-шинная** (star-bus) (*рис. 2.11*) и **звездно-кольцевая** (star-ring) (*рис. 2.12*).

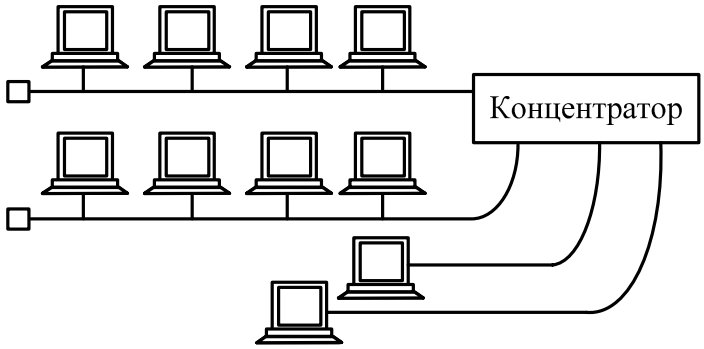


Рис. 2.11. Пример **звездно-шинной** топологии

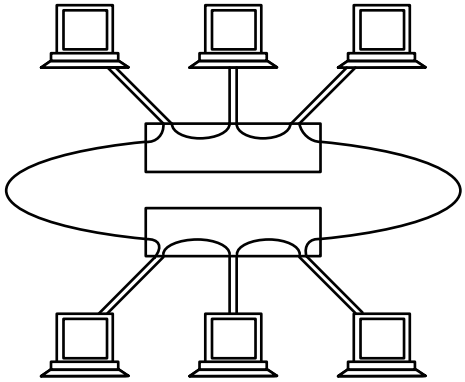
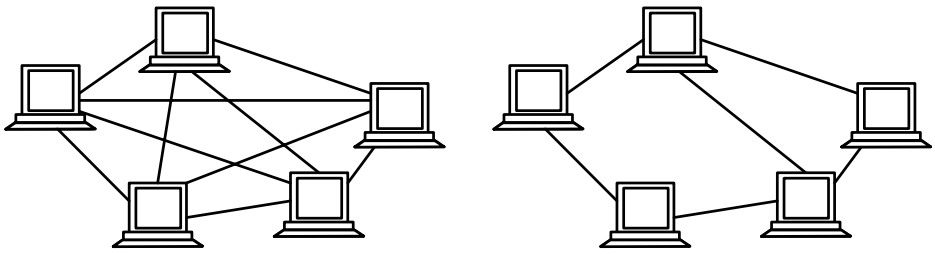


Рис. 2.12. Пример **звездно-кольцевой** топологии

В звездно-шинной топологии используется комбинация шины и пассивной звезды. К концентратору подключаются как отдельные компьютеры, так и целые шинные сегменты. На самом деле реализуется физическая топология шина, включающая все компьютеры сети. В данной топологии может использоваться и несколько концентраторов, соединенных между собой и образующих так называемую магистральную, опорную шину. К каждому из концентраторов при этом подключаются отдельные компьютеры или шинные сегменты. В результате получается звездно-шинное дерево. Таким образом, пользователь может гибко комбинировать преимущества шинной и звездной топологий, а также легко изменять количество компьютеров, подключенных к сети. С точки зрения распространения информации данная топология равноценна классической шине.

В случае звездно-кольцевой топологии в кольцо объединяются не сами компьютеры, а специальные концентраторы (*рис. 2.11*), к которым в свою очередь подключаются компьютеры с помощью звездообразных двойных линий связи. В действительности все компьютеры сети включаются в замкнутое кольцо, так как внутри концентраторов линии связи образуют замкнутый контур. Данная топология дает возможность комбинировать преимущества звездной и кольцевой топологий. Например, концентраторы позволяют собрать в одно место все точки подключения кабелей сети. Если говорить о распространении информации, данная топология равноценна классическому кольцу.

В **сеточной (ячеистой) (mesh) топологии** компьютеры связываются между собой не одной, а многими линиями связи, образующими сетку (*рис. 2.13*).



а *б*

Рис. 2.13. **Сеточная** топология:
полная (*а*) и частичная (*б*)

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

Частичная сеточная топология предполагает прямые связи только для самых активных компьютеров, передающих максимальные объемы информации. Остальные компьютеры соединяются через промежуточные узлы. Сеточная топология позволяет выбирать маршрут для доставки информации от абонента к абоненту, обходя неисправные участки. С одной стороны, это увеличивает надежность сети, с другой же – требует существенного усложнения сетевой аппаратуры, которая должна выбирать маршрут.

В заключение несколько слов о **решетчатой топологии**, в которой узлы образуют регулярную многомерную решетку. При этом каждое ребро решетки параллельно ее оси и соединяет два смежных узла вдоль этой оси.

Одномерная решетка – это цепь, соединяющая два внешних узла (имеющих лишь одного соседа) через некоторое количество внутренних (у которых по два соседа – слева и справа). При соединении обоих внешних узлов получается топология кольцо. Двух- и трехмерные решетки используются в архитектуре суперкомпьютеров. Многомерная решетка, соединенная циклически в более чем одном измерении, называется тор.

Основным достоинством топологии решетка является высокая надежность, а недостатком – сложность реализации.

2.2.6. Многозначность понятия топологии

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

Более того, физическое расположение компьютеров, соединяемых сетью, почти не влияет на выбор топологии. Как бы ни были расположены компьютеры, их можно соединить с помощью любой заранее выбранной топологии (*рис. 2.14*).

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

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

Строго говоря, при упоминании о топологии сети, могут подразумеваться четыре совершенно разных понятия, относящихся к различным уровням сетевой архитектуры.

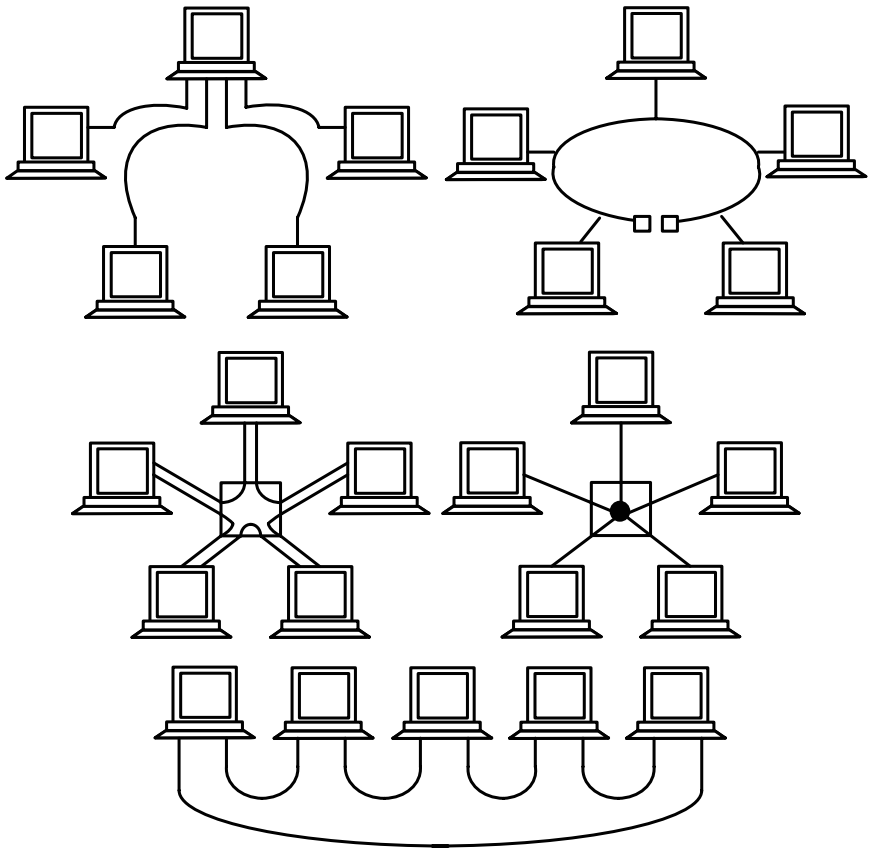


Рис. 2.14. Примеры использования разных топологий для соединения компьютеров

Физическая топология – географическая схема расположения компьютеров и прокладки кабелей. В этом смысле, например, пассивная звезда ничем не отличается от активной, поэтому ее нередко называют просто звездой.

Логическая топология – структура связей, характер распространения сигналов по сети. Это наиболее правильное определение топологии.

Топология управления обменом – принцип и последовательность передачи права на захват сети между отдельными компьютерами.

Информационная топология – направление потоков информации, передаваемой по сети.

Например, сеть с физической и логической топологией шина может в качестве метода управления использовать эстафетную передачу права захвата сети (быть в этом смысле кольцом) и одновременно передавать всю информацию через выделенный компьютер (быть в этом смысле звездой). Или сеть с логической топологией

шина может иметь физическую топологию звезда (пассивная) или дерево (пассивное).

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

Выводы

1. Топология сети определяет как физическое расположение компьютеров, так и характер связей между ними, особенности распространения информации, сигналов по сети. Все это определяет степень отказоустойчивости сети, задает требуемую сложность сетевой аппаратуры, наиболее подходящий метод управления обменом, возможные типы сред передачи (каналов связи), допустимый размер сети (длина линий связи и количество абонентов), необходимость электрического согласования и многое другое.

2. Выделяют два основных класса топологий: широковещательные и последовательные. В широковещательных топологиях передаемые сигналы могут быть восприняты всеми узлами сети. В последовательных топологиях информация передается только одному сетевому узлу.

3. Выделяют 5 базовых топологий: общая шина, дерево, звезда, ячеистая, кольцо, однако часто на практике применяются комбинированные топологии, среди которых наибольшее распространение получили звездно-шинная и звездно-кольцевая.

2.3. Требования, предъявляемые к сетям

При организации и эксплуатации сети важными требованиями, предъявляемыми к их работе, являются следующие:

- *производительность*;
- *надежность* и *безопасность*;
- *расширяемость* и *масштабируемость*;
- *прозрачность*;
- *поддержка разных видов трафика*;
- *управляемость*;
- *совместимость*.

2.3.1. Производительность

Производительность – это характеристика сети, позволяющая оценить, насколько быстро информация передающей рабочей станции достигнет до приемной рабочей станции.

На производительность сети влияют следующие характеристики сети:

- конфигурация;
- скорость передачи данных;
- метод доступа к каналу;
- топология сети;
- технология.

Если производительность сети перестает отвечать предъявляемым к ней требованиям, то администратор сети может прибегнуть к различным приемам:

– изменить конфигурацию сети таким образом, чтобы структура сети более соответствовала структуре информационных потоков;

– перейти к другой модели построения распределенных приложений, которая позволила бы уменьшить сетевой трафик;

– заменить мосты более скоростными коммутаторами.

Но самым радикальным решением в такой ситуации является переход на более скоростную технологию. Если в сети используются традиционные технологии Ethernet или Token Ring, то переход на Fast Ethernet, FDDI или 100VG-AnyLAN позволит сразу в 10 раз увеличить пропускную способность каналов.

С ростом масштаба сетей возникла необходимость в повышении их производительности. Одним из способов достижения этого стала их ***микросегментация***. Она позволяет уменьшить число пользователей на один сегмент и снизить объем широковещательного трафика, а значит, повысить производительность сети.

Первоначально для микросегментации использовались маршрутизаторы, которые в целом не очень приспособлены для этой цели. Решения на их основе были достаточно дорогостоящими и отличались большой временной задержкой и невысокой пропускной способностью. Более подходящими устройствами для микросегментации сетей стали коммутаторы. Благодаря относительно низкой стоимости, высокой производительности и простоте в использовании, они быстро завоевали популярность.

Таким образом, сети стали строить на базе коммутаторов и маршрутизаторов. Первые обеспечивали высокоскоростную пересылку трафика между сегментами, входящими в одну подсеть, а вторые передавали данные между подсетями, ограничивали распространение широковещательного трафика, решали задачи безопасности и т. д.

2.3.2. Прозрачность

Прозрачность – это такое состояние сети, при котором пользователь воспринимает сеть как отдельный (персональный) компьютер.

Коммуникационная сеть является прозрачной относительно проходящей сквозь нее информации, если выходной поток битов в точности повторяет входной поток. Но сеть может быть непрозрачной во времени, если из-за меняющихся размеров очередей блоков данных изменяется и время прохождения различных блоков через узлы коммутации. Прозрачность сети по скорости передачи данных указывает, что данные можно передавать с любой нужной скоростью.

Если в сети по одним и тем же маршрутам передаются информационные и управляющие (синхронизирующие) сигналы, то говорят, что сеть прозрачна по отношению к типам сигналов.

Если передаваемая информация может кодироваться любым способом, то это означает, что сеть прозрачна для любых методов кодировок.

Прозрачная сеть является простым решением, в котором для взаимодействия локальных сетей, расположенных на значительном расстоянии друг от друга, используется принцип ***Plug-and-play*** (подключись и работай).

Прозрачное соединение. Служба прозрачных локальных сетей обеспечивает сквозное (end-to-end) соединение, связывающее

между собой удаленные локальные сети. Привлекательность данного решения состоит в том, что эта служба объединяет удаленные друг от друга на значительное расстояние узлы как части локальной сети. Поэтому не нужно вкладывать средства в изучение новых технологий и создание территориально распределенных сетей (Wide Area Network, WAN). Пользователям требуется только поддерживать локальное соединение, а провайдер службы прозрачных сетей обеспечит беспрепятственное взаимодействие узлов через сеть масштаба города (Metropolitan Area Network, MAN) или сеть WAN.

Службы Прозрачной локальной сети имеют много преимуществ. Например, пользователь может быстро и безопасно передавать большие объемы данных на значительные расстояния, не обременяя себя сложностями, связанными с работой в сетях WAN.

2.3.3. Поддержка разных видов трафика

Трафик в сети складывается случайным образом, однако, в нем отражены и некоторые закономерности. Как правило, некоторые пользователи, работающие над общей задачей (например, сотрудники одного отдела), чаще всего обращаются с запросами либо друг к другу, либо к общему серверу, и только иногда они испытывают необходимость доступа к ресурсам компьютеров другого отдела. Желательно, чтобы структура сети соответствовала структуре информационных потоков. В зависимости от сетевого трафика компьютеры в сети могут быть разделены на группы – **сегменты сети**. Компьютеры объединяются в группу, если большая часть порождаемых ими сообщений адресована компьютерам этой же группы.

Для разделения сети на сегменты используются **мосты** и **коммутаторы**. Они экранируют локальный трафик внутри сегмента, не передавая за его пределы никаких кадров, кроме тех, которые адресованы компьютерам, находящимся в других сегментах. Таким образом, сеть распадается на отдельные подсети. Это позволяет более рационально выбирать пропускную способность имеющихся линий связи, учитывая интенсивность трафика внутри каждой группы, а также активность обмена данными между группами.

Однако локализация трафика средствами мостов и коммутаторов имеет существенные ограничения. С другой стороны, использование механизма виртуальных сегментов, реализованного в коммутаторах локальных сетей, приводит к полной локализации трафика; такие сегменты полностью изолированы друг от друга,

даже в отношении широковещательных кадров. Поэтому в сетях, построенных только на мостах и коммутаторах, компьютеры, принадлежащие разным виртуальным сегментам, не образуют единой сети.

Для того чтобы эффективно консолидировать различные виды трафика в сети ATM, требуется специальная предварительная подготовка (адаптация) данных, имеющих различный характер: кадры – для цифровых данных, сигналы импульсно-кодовой модуляции – для голоса, потоки битов – для видео. Эффективная консолидация трафика требует также учета и использования статистических вариаций интенсивности различных типов трафика.

2.3.4. Управляемость

Международная организация по стандартам (ISO) внесла большой вклад в стандартизацию сетей. Модель управления сетью является основным средством для понимания главных функций систем управления. Эта модель состоит из 5 концептуальных областей:

- управление эффективностью;
- управление конфигурацией;
- управление учетом использования ресурсов;
- управление неисправностями;
- управление защитой данных.

Цель **управления эффективностью** – измерение, обеспечение и поддержание различных аспектов эффективности сети на приемлемом уровне.

Примерами переменных эффективности являются *пропускная способность* сети, *время реакции* пользователей и *коэффициент использования линии*.

Управление эффективностью включает несколько этапов:

– сбор информации об эффективности по тем переменным, которые представляют интерес для *администраторов сети*;

– анализ информации для определения нормальных (базовая строка) уровней;

– определение соответствующих порогов эффективности для каждой важной переменной таким образом, чтобы превышение этих порогов указывало на наличие проблемы в сети, достойной внимания.

Цель **управления конфигурацией** – контролирование информации о сетевой и системной конфигурации для того, чтобы можно было отслеживать происходящее и управлять воздействием на

работу различных аппаратных и программных элементов. Так как все аппаратные и программные элементы имеют эксплуатационные отклонения, погрешности (или то и другое вместе), которые могут влиять на работу сети, такая информация важна для поддержания гладкой работы сети.

Каждое устройство сети располагает разнообразной информацией о версиях, ассоциируемых с ним. Чтобы обеспечить легкий доступ, подсистемы управления конфигурацией хранят эту информацию в базе данных. Когда возникает какая-нибудь проблема, в этой базе данных может быть проведен поиск ключей, которые могли бы помочь решить эту проблему.

Цель **управления учетом использования ресурсов** – измерение параметров использования сети, чтобы можно было соответствующим образом регулировать ее использование индивидуальными или групповыми пользователями. Такое регулирование минимизирует число проблем в сети (т. к. ресурсы сети могут быть поделены исходя из возможностей источника) и максимизирует равнодоступность к сети для всех пользователей.

Цель **управления неисправностями** – выявить, зафиксировать, уведомить пользователей и (в пределах возможного) автоматически устранить проблемы в сети для того, чтобы эффективно поддерживать работу сети. Так как неисправности могут привести к простоям или недопустимой деградации сети, управление неисправностями, по всей вероятности, является наиболее широко используемым элементом модели управления сети ISO.

Управление неисправностями включает в себя несколько шагов:

- определение симптомов проблемы;
- изолирование проблемы;
- устранение проблемы;
- проверка устранения неисправности на всех важных подсистемах;
- регистрация обнаружения проблемы и ее решения.

Цель **управления защитой данных** – контроль доступа к сетевым ресурсам в соответствии с местными руководящими принципами, чтобы сделать невозможными *саботаж сети* и доступ к *конфиденциальной* информации лицам, не имеющим соответствующего разрешения.

Например, одна из подсистем управления защитой данных может контролировать регистрацию пользователей ресурса сети,

отказывая в доступе тем, кто вводит коды доступа, не соответствующие установленным.

Подсистемы управления защитой данных работают путем разделения источников на *санкционированные* и *несанкционированные* области. Для некоторых пользователей доступ к любому источнику сети является несоответствующим.

Подсистемы управления защитой данных выполняют следующие функции:

– идентифицируют конфиденциальные ресурсы сети (включая системы, файлы и другие объекты);

– определяют отображения в виде карт между конфиденциальными источниками сети и набором пользователей;

– контролируют точки доступа к конфиденциальным ресурсам сети;

– регистрируют несанкционированный доступ к конфиденциальным ресурсам сети.

2.3.5. Совместимость

Концепция **программной совместимости** впервые в широких масштабах была применена разработчиками системы IBM/360. Основная задача при проектировании всего ряда моделей этой системы заключалась в создании такой архитектуры, которая была бы одинаковой с точки зрения пользователя для всех моделей системы независимо от цены и производительности каждой из них.

Огромные преимущества такого подхода, позволяющего сохранять существующий задел программного обеспечения при переходе на новые (как правило, более производительные) модели, были быстро оценены как производителями компьютеров, так и пользователями. Начиная с этого времени, практически все фирмы-поставщики компьютерного оборудования взяли на вооружение эти принципы, поставляя серии совместимых компьютеров. Следует заметить, однако, что со временем даже самая передовая архитектура неизбежно устаревает и возникает потребность внесения радикальных изменений в архитектуру и способы организации вычислительных систем.

В настоящее время одним из наиболее важных факторов, определяющих тенденции в развитии информационных технологий, является ориентация компаний-поставщиков компьютерного оборудования на рынок прикладных программных средств.

Вычислительная среда должна, во-первых, позволять гибко менять количество и состав аппаратных средств и программного обеспечения в соответствии с меняющимися требованиями решаемых задач. Во-вторых, она должна обеспечивать возможность запуска одних и тех же программных систем на различных аппаратных платформах, т. е. обеспечивать мобильность программного обеспечения. В-третьих, эта среда должна гарантировать возможность применения одних и тех же человеко-машинных интерфейсов на всех компьютерах, входящих в неоднородную сеть.

В условиях жесткой конкуренции производителей аппаратных платформ и программного обеспечения сформировалась **концепция открытых систем**, представляющая собой совокупность стандартов на различные компоненты вычислительной среды, предназначенных для обеспечения мобильности программных средств в рамках неоднородной *распределенной вычислительной системы*.

2.3.6. Надежность и безопасность

Быстрое развитие компьютерных информационных технологий и их все возрастающая роль в жизни современного общества приводит к тому, что информация становится одним из самых дорогих продуктов в сфере межличностных отношений. При этом стоимость информации часто превосходит в сотни и тысячи раз стоимость компьютерной системы, в которой она обрабатывается. Это обстоятельство приводит к тому, что именно информация и информационные системы (в том числе компьютерные сети) все чаще становятся объектами ***атак*** (несанкционированного доступа). Поэтому вполне естественно возникает необходимость в защите информации. Однако по сравнению с другими информационно-вычислительными системами проблема защиты информации в компьютерных сетях значительно усложняется и происходит это по ряду следующих причин:

– наличие большого числа пользователей в компьютерной сети и их переменный состав; защита на уровне имени и пароля пользователя недостаточна для предотвращения входа в сеть посторонних лиц;

– значительная протяженность сети и наличие многих потенциальных каналов проникновения в сеть;

– уже отмеченные недостатки в аппаратном и программном обеспечении, которые зачастую обнаруживаются не на

предпродажном этапе, называемом бета-тестированием, а в процессе эксплуатации.

Кроме того, любые дополнительные соединения сегментов компьютерной сети с другими сегментами или подключение к сети Интернет порождают новые проблемы в компьютерной сети.

Более подробно вопросы безопасности и надежности сетей будут рассмотрены в разделе 11.

Выводы

1. На практике качество работы сети, как правило, определяется следующими свойствами: производительность, надежность, совместимость, управляемость, защищенность, расширяемость и масштабируемость.

2. Существуют два основных подхода к обеспечению качества работы сети. Первый состоит в том, что сеть гарантирует пользователю соблюдение некоторой числовой величины показателя качества обслуживания, например, заданный уровень пропускной способности. При втором подходе сеть «старается» по возможности более качественно обслужить пользователя, но ничего при этом не гарантирует.

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

4. Для оценки надежности сетей используются различные характеристики, в том числе: коэффициент готовности, безопасность, отказоустойчивость.

5. Предполагается, что любая локальная сеть должна легко расширяться, это в свою очередь предоставляет возможность сравнительно легкого добавления отдельных элементов сети (пользователей, компьютеров, приложений, сервисов), наращивания длины сегментов сети и замены существующей аппаратуры более мощной. Немаловажным является и масштабируемость сети, при этом сеть позволяет наращивать количество узлов

и протяженность связей в очень широких пределах, при этом производительность сети не ухудшается.

7. На практике очень важным бывает скрытие от пользователя деталей внутреннего устройства сети, что упрощает тем самым его работу в сети (прозрачность), дает возможность централизованного управления и обеспечивает совместимость с разнообразным программным и аппаратным обеспечением.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Поясните понятие архитектуры сети.
2. В каком случае используется одноранговая архитектура?
3. Что характерно для сетей с выделенным сервером?
4. Что такое топология?
5. Основные достоинства и недостатки топологии общая шина.
6. Основные достоинства и недостатки топологии кольцо.
7. Основные достоинства и недостатки топологии звезда.
8. Основные достоинства и недостатки ячеистой топологии.
9. В чем заключаются основные различия между активным и пассивным деревом?
10. Приведите основные различия между полной и частичной ячеистыми топологиями.
11. Поясните понятия «надежности» и «безопасности» компьютерных сетей.
12. Назовите основные технические и эксплуатационные свойства сетей.

3. ОСНОВЫ ПЕРЕДАЧИ ДАННЫХ ПО СЕТИ

3.1. Пакеты и их структура

3.1.1. Назначение пакетов

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

Локальная сеть, как уже отмечалось, должна обеспечивать качественную, прозрачную связь всем абонентам (компьютерам) сети.

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

Ожидание начала передачи связано с тем, что в сети не может происходить несколько передач одновременно (во всяком случае, при топологиях шина и кольцо). Всегда есть только один передатчик и один приемник (реже – несколько приемников). В противном случае информация от разных передатчиков смешивается и искажается. В связи с этим абоненты передают свою информацию по очереди. И каждому абоненту, прежде чем начать передачу, надо дождаться своей очереди. Вот это время ожидания своей очереди и есть *время доступа*.

Если бы вся требуемая информация передавалась каким-то абонентом сразу, непрерывно, без разделения на пакеты, то это привело бы к монопольному захвату сети этим абонентом на довольно продолжительное время. Все остальные абоненты вынуждены были бы ждать окончания передачи всей информации, что в ряде случаев могло бы потребовать десятков секунд и даже минут

(например, при копировании содержимого целого жесткого диска). С тем, чтобы уравнять в правах всех абонентов, а также сделать примерно одинаковой величину времени доступа к сети и интегральную скорость передачи информации, как раз и применяются пакеты (кадры) ограниченной длины.

Важно также и то, что при передаче больших массивов информации *вероятность ошибки* (передана «1» – принимается «0», или наоборот) из-за помех и сбоев довольно высока. Например, при характерной для локальных сетей величине вероятности одиночной ошибки в 10^{-8} (в среднем одна ошибка приходится на 100 Мбайт переданных двоичных символов) пакет длиной 10 Кбит будет искажен с вероятностью 10^{-4}, а массив длиной 10 Мбит – уже с вероятностью 10^{-1}. К тому же выявить ошибку в массиве из нескольких мегабайт намного сложнее, чем в пакете из нескольких килобайт, а при обнаружении ошибки придется повторить передачу всего большого массива. Но и при повторной передаче большого массива снова высока вероятность ошибки, и процесс этот при слишком большом массиве может повторяться до бесконечности.

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

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

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

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

В частном случае (*рис. 3.1*) все эти пакеты могут передаваться одним абонентом (когда другие абоненты «не хотят» передавать). Но обычно в сети чередуются пакеты, посланные разными абонентами (*рис. 3.2*).

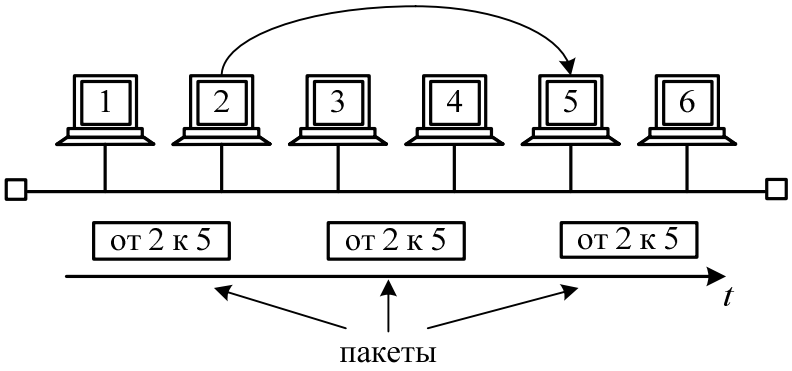


Рис. 3.1. Передача пакетов в сети между двумя абонентами

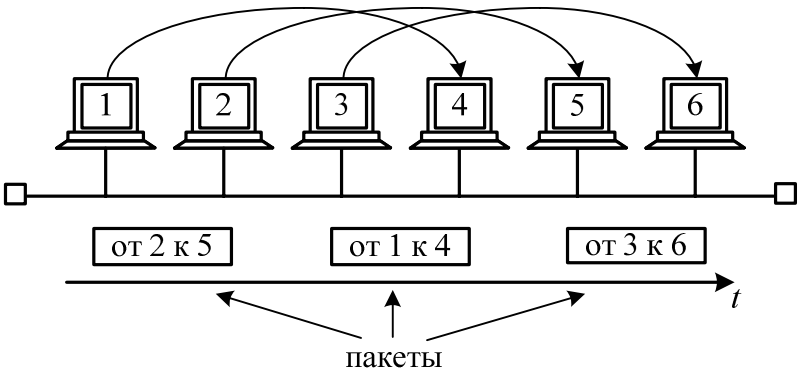


Рис. 3.2. Передача пакетов в сети между несколькими абонентами

3.1.2. Структура пакетов

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

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

Чаще всего пакет содержит в себе следующие основные *поля*, или части, представленные на *рис. 3.3*.

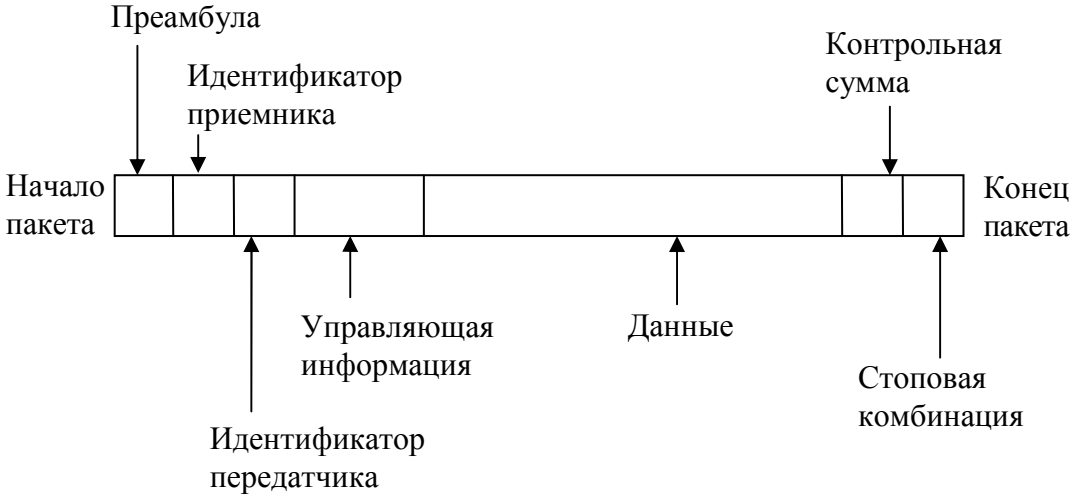


Рис. 3.3. Типичная структура пакета

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

Сетевой адрес (*идентификатор*) принимающего абонента – индивидуальный или групповой номер, присвоенный каждому принимающему абоненту (компьютеру) в сети. Этот адрес (или *IP-адрес*) позволяет приемнику распознать пакет, адресованный ему лично, группе, в которую он входит, или всем абонентам сети одновременно (при широком вещании).

Сетевой адрес (*идентификатор*) передающего абонента – индивидуальный номер, присвоенный каждому передающему абоненту. Этот адрес информирует принимающего абонента, откуда пришел данный пакет. Включение в пакет адреса передатчика необходимо в том случае, когда одному приемнику могут попеременно приходить пакеты от разных передатчиков.

Служебная информация может указывать на тип пакета, его номер, размер, формат, маршрут его доставки, на то, что с ним надо делать приемнику и т. д.

Данные (поле данных) – это та информация, ради передачи которой используется пакет. В отличие от всех остальных полей пакета поле данных имеет переменную длину, которая, собственно, и определяет полную длину пакета. Существуют специальные управляющие пакеты, которые не имеют поля данных. Их можно рассматривать как сетевые команды. Пакеты, включающие поле данных, называются информационными пакетами. Управляющие пакеты могут выполнять функцию начала и конца сеанса связи, подтверждения приема информационного пакета, запроса информационного пакета и т. д.

Контрольная сумма пакета – это числовой код, формируемый передатчиком по определенным правилам и содержащий в свернутом виде информацию обо всем пакете. Приемник, повторяя вычисления, сделанные передатчиком с принятым пакетом, сравнивает их результат с контрольной суммой и делает вывод о правильности или ошибочности передачи пакета. Если пакет ошибочен, то приемник запрашивает его повторную передачу. Обычно используется циклическая контрольная сумма (CRC).

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

Нередко в структуре пакета выделяют всего три поля:

– начальное управляющее поле пакета (или заголовок пакета), то есть поле, включающее в себя стартовую комбинацию, сетевые адреса приемника и передатчика, а также служебную информацию;

– поле данных пакета;

– конечное управляющее поле пакета (заключение, трейлер), куда входят контрольная сумма и стоповая комбинация, а также, возможно, служебная информация.

Структура и вид отдельных полей зависят от применяемой технологии (Ethernet, Token Ring, Arcnet, FDDI и т. д.) и будут рассмотрены в разделе 9.

Как уже упоминалось, помимо термина «*пакет*» (packet) в литературе также нередко встречается термин «*кадр*» (frame). Иногда под этими терминами имеется в виду одно и то же. Но иногда подразумевается, что кадр вложен в пакет. В этом случае все

перечисленные поля пакета, кроме преамбулы и стоповой комбинации, относятся к кадру (*рис. 3.4*).

Например, в описаниях сети Ethernet говорится, что в конце преамбулы передается признак начала кадра.

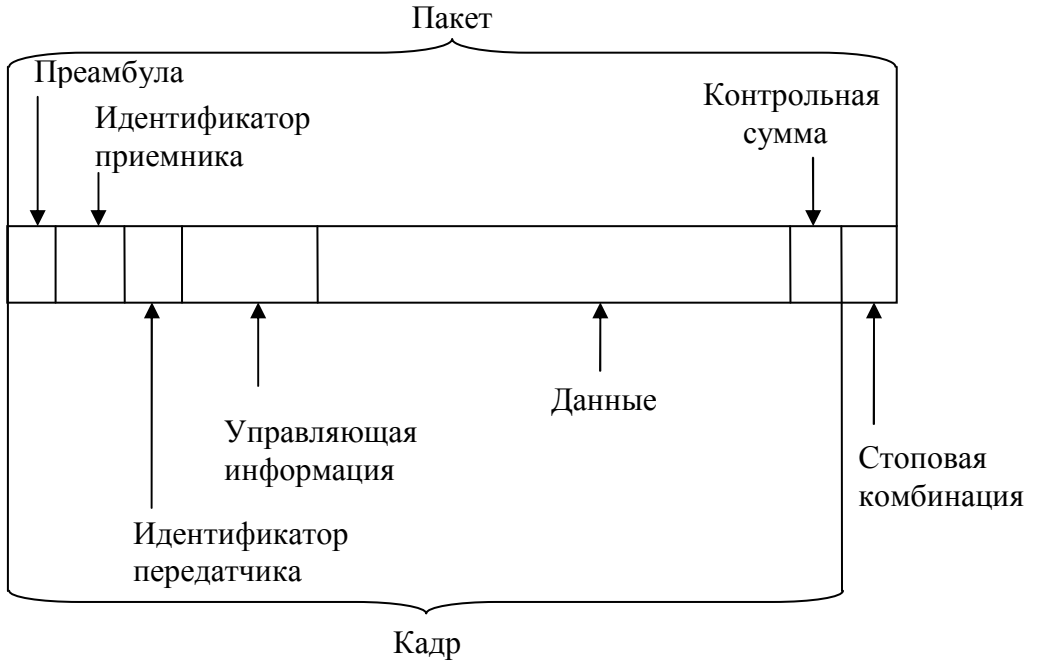


Рис. 3.4. Вложение кадра в пакет

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

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

3.1.3. Правила обмена и управления пакетами

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

Пример простейшего протокола показан на *рис. 3.5*.

Сеанс обмена начинается с запроса передатчиком готовности приемника принять данные. Для этого используется управляющий

пакет «*Запрос*». Если приемник не готов, он отказывается от сеанса специальным управляющим пакетом. В случае, когда приемник готов, он посылает в ответ управляющий пакет «*Готовность*». Затем начинается собственно передача данных. При этом на каждый полученный информационный пакет приемник отвечает управляющим пакетом «*Подтверждение*».

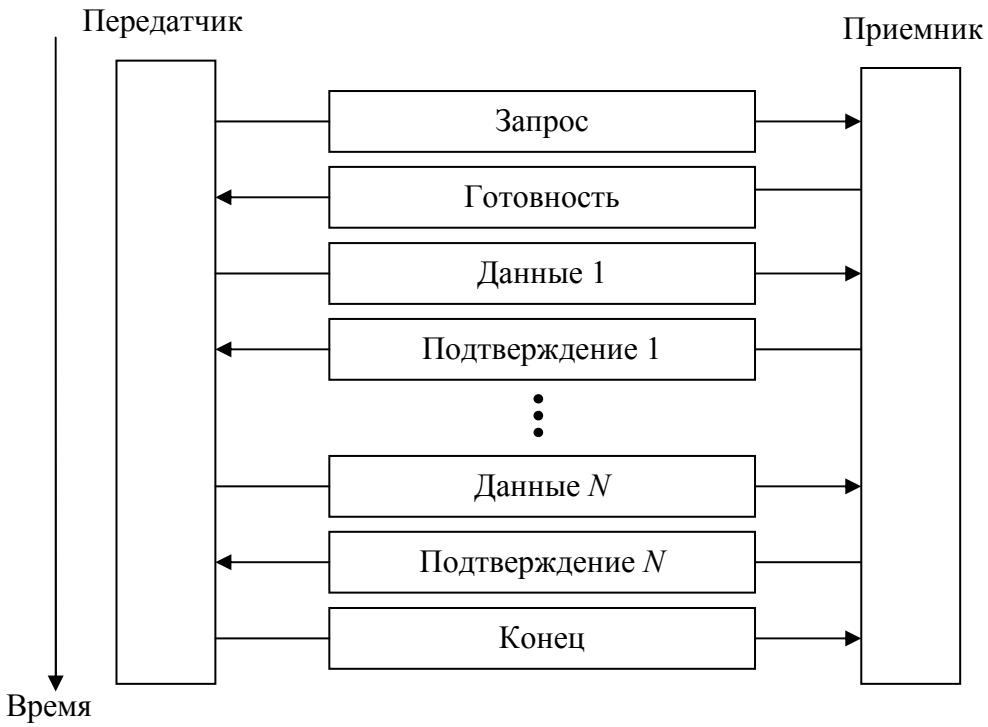


Рис. 3.5. Пример обмена пакетами при сеансе связи

В случае, когда пакет данных передан с ошибками, в ответ на него приемник запрашивает повторную передачу. Заканчивается сеанс управляющим пакетом «*Конец*», которым передатчик сообщает о разрыве связи.

Существует множество стандартных протоколов, которые используют как передачу с подтверждением (с гарантированной доставкой пакета), так и передачу без подтверждения (без гарантии доставки пакета). Подробнее о протоколах обмена будет рассказано в следующем разделе.

При реальном обмене по сети применяются *многоуровневые протоколы*, каждый из уровней которых предполагает свою структуру пакета (адресацию, управляющую информацию, формат данных и т. д.). Ведь протоколы высоких уровней имеют дело с такими

понятиями, как *файл-сервер* или приложение, запрашивающее данные у другого приложения, и вполне могут не иметь представления ни о типе аппаратуры сети, ни о методе управления обменом. Все пакеты более высоких уровней последовательно вкладываются в передаваемый пакет, точнее, в поле данных передаваемого пакета (*рис. 3.6*). Этот процесс последовательной упаковки данных для передачи называется также **инкапсуляцией пакетов**.

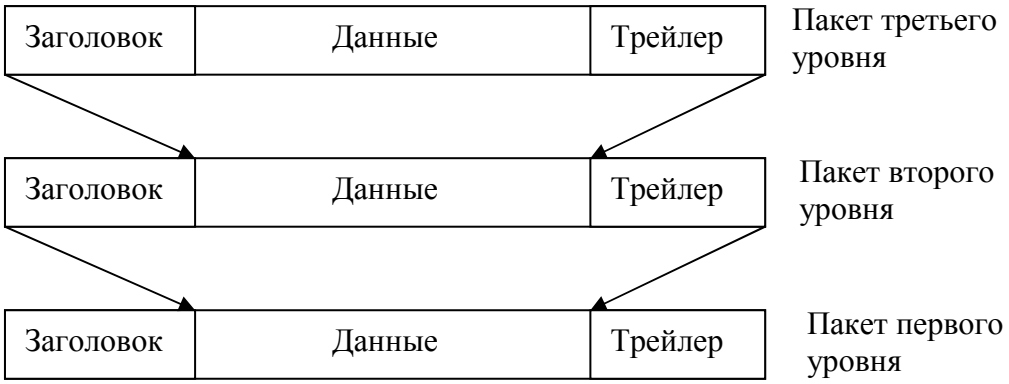


Рис. 3.6. Многоуровневая система вложения пакетов

Каждый следующий вкладываемый пакет может содержать собственную служебную информацию, располагающуюся как до данных (заголовок), так и после них (трейлер), причем ее назначение может быть различным.

Безусловно, доля вспомогательной информации в пакетах при этом возрастает с каждым следующим уровнем, что снижает эффективную скорость передачи данных. Для увеличения этой скорости предпочтительнее, чтобы протоколы обмена были проще и уровней этих протоколов было меньше. Иначе никакая скорость передачи битов не поможет, и быстрая сеть может передавать файл дольше, чем медленная сеть, которая пользуется более простым протоколом.

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

Выводы

1. Информация в локальных сетях передается отдельными порциями, называемыми пакетами. Причем предельная длина

этих пакетов, как минимальная, так и максимальная, ограничена и в основном зависит от сетевой технологии (Ethernet, Token Ring, FDDI и т. д.).

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

3. Локальная сеть характеризуется таким важнейшим параметром, как время доступа, которое определяется как временной интервал между моментом готовности абонента к передаче (когда ему есть, что передавать) и моментом начала этой передачи.

4. В общем случае, пакет содержит в себе следующие основные поля: перамбула, идентификатор передатчика, идентификатор приемника, служебная информация, данные, контрольная сумма, стоповая комбинация.

3.2. Методы доступа в сетях

В современных сетях, в основном, используются следующие методы доступа:

– *множественный доступ с прослушиванием несущей и разрешением коллизий* (Carrier Sense Multiple Access with Collision Detection, CSMA/CD);

– *множественный доступ с передачей полномочия* (Token Passing Multiple Access, TPMA), или метод с передачей *маркера*;

– *множественный доступ с разделением во времени* (Time Division Multiple Access, TDMA);

– *множественный доступ с разделением частоты* (Frequency Division Multiple Access, FDMA), или *множественный доступ с разделением длины волны* (Wavelength Division Multiple Access, WDMA).

3.2.1. Множественный доступ с прослушиванием несущей и разрешением коллизий

Алгоритм множественного доступа с прослушиванием несущей и разрешением коллизий приведен на *рис. 3.7*.

Метод множественного доступа с прослушиванием несущей и разрешением коллизий (**CSMA/CD**) устанавливает следующий порядок: если рабочая станция «хочет» воспользоваться

сетью для передачи данных, она сначала должна проверить состояние канала, начинать передачу рабочая станция может, если канал свободен.

Рис. 3.7. Алгоритм CSMA/CD

В процессе передачи рабочая станция продолжает прослушивание сети для обнаружения возможных конфликтов (коллизий). Если возникает конфликт из-за того, что два узла попытаются занять канал, то обнаружившая конфликт интерфейсная плата соответствующего компьютера выдает в сеть специальный сигнал, и обе станции одновременно прекращают передачу. Принимающая рабочая станция отбрасывает частично принятое сообщение, а все рабочие станции, желающие передать сообщение,

в течение некоторого, случайно выбранного промежутка времени выжидают, прежде чем начать сообщение.

Все сетевые интерфейсные платы запрограммированы на разные псевдослучайные промежутки времени ожидания. Если конфликт возникнет во время повторной передачи сообщения, этот промежуток времени будет увеличен.

Стандарт типа ***Ethernet*** определяет сеть с конкуренцией, в которой несколько рабочих станций должны конкурировать друг с другом за право доступа к сети.

В некоторых сетях применяется метод доступа **Demand Priority**, который является развитием метода доступа CSMA/CD и обеспечивает более справедливое распределение пропускной способности сети. Этот метод доступа поддерживает приорететный доступ для синхронных приложений.

Метод доступа Demand Priority основан на передаче концентратору функций арбитра, решающего проблему доступа к разделяемой среде. Концентратор циклически выполняет опрос портов.

Рабочая станция, желающая передать пакет, посылает специальный низкочастотный сигнал концентратору, запрашивая передачу кадра и указывая его приоретет (низкий, высокий). Низкий уровень приоритета соответствует обычным данным (файловая служба, служба печати и т. п.), а высокий приоритет соответствует данным, чувствительным к временным задержкам (например, мультимедиа).

3.2.2. Множественный доступ с передачей полномочия (маркера)

Алгоритм множественного доступа с передачей полномочия, или маркера, приведен на *рис. 3.8*.

Метод с передачей маркера (TPMA) – это метод доступа к среде, при котором от рабочей станции к рабочей станции передается маркер, дающий разрешение на передачу сообщения.

При получении маркера рабочая станция может передавать сообщение, присоединяя его к маркеру, который переносит это сообщение по сети. Каждая рабочая станция между передающей станцией и принимающей видит это сообщение, но только станция-адресат принимает его. При этом она создает новый маркер.

Маркер (token), или **полномочие** – уникальная комбинация битов, позволяющая начать передачу данных.

Рис. 3.8. Алгоритм TPMA

Каждый узел принимает пакет от предыдущего, восстанавливает уровни сигналов до номинального (требуемого) уровня и передает дальше. Передаваемый пакет может содержать данные или являться

маркером. Когда рабочей станции необходимо передать пакет, ее адаптер дожидается поступления маркера, а затем преобразует его в пакет, содержащий данные, отформатированные по протоколу соответствующего уровня, и передает результат далее по ЛВС. Пакет распространяется по ЛВС от адаптера к адаптеру, пока не найдет своего адресата, который установит в нем определенные биты для подтверждения того, что данные достигли адресата, и ретранслирует его вновь в ЛВС. После чего пакет возвращается в узел, из которого был отправлен. Здесь после проверки безошибочной передачи пакета узел освобождает ЛВС, генерируя новый маркер. Таким образом, в ЛВС с передачей маркера невозможны **коллизии** (конфликты).

Метод с передачей маркера в основном используется в кольцевой топологии.

Данный метод характеризуется следующими достоинствами:

– гарантирует время доставки блоков данных в сети;

– дает возможность предоставления различных *приоритетов передачи данных*.

Вместе с тем он имеет существенные недостатки:

– в сети возможны потеря маркера, а также появление нескольких маркеров, при этом сеть прекращает работу;

– включение новой рабочей станции и отключение связаны с изменением адресов всей системы.

3.2.3. Множественный доступ с разделением во времени

Множественный доступ с разделением во времени (TDMA) основан на распределении времени работы канала между системами (*рис. 3.9*).

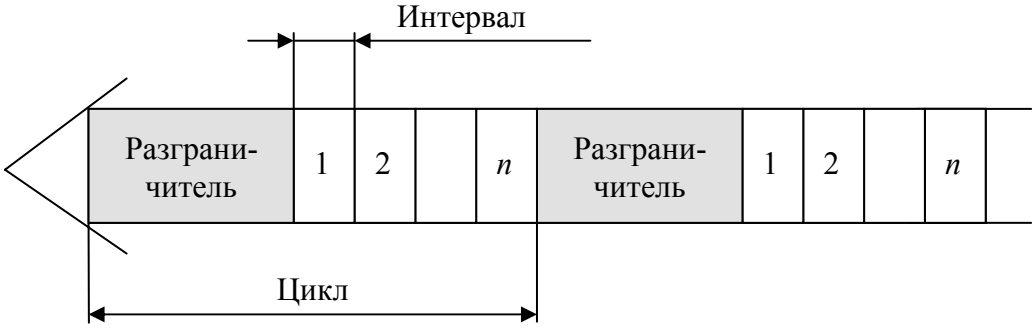


Рис. 3.9. Структура множественного доступа с разделением во времени

Доступ TDMA основан на использовании специального устройства, называемого тактовым генератором. Этот генератор делит время канала на повторяющиеся циклы. Каждый из циклов начинается *сигналом-разграничителем*. Цикл включает *n* пронумерованных временных интервалов, называемых *ячейками*. Интервалы предоставляются для загрузки в них блоков данных.

Данный способ позволяет организовать передачу данных с *коммутацией пакетов* и с *коммутацией каналов*.

Первый (простейший) вариант использования интервалов заключается в том, что их число (*n*) делается равным количеству абонентских систем, подключенных к рассматриваемому каналу. Тогда во время цикла каждой системе предоставляется один интервал, в течение которого она может передавать данные. При использовании рассмотренного метода доступа часто оказывается, что в одном и том же цикле одним системам нечего передавать, а другим не хватает выделенного времени. В результате – неэффективное использование пропускной способности канала.

Второй более сложный, но высокоэкономичный вариант заключается в том, что система получает интервал только тогда, когда у нее возникает необходимость в передаче данных, например, при асинхронном способе передачи. Для передачи данных система может в каждом цикле получать интервал с одним и тем же номером. В этом случае передаваемые системой блоки данных появляются через одинаковые промежутки времени и приходят с одним и тем же временем запаздывания. Это режим передачи данных с имитацией коммутации каналов. Способ особенно удобен при передаче речи.

3.2.4. Множественный доступ с разделением частоты

Множественный доступ с разделением частоты (FDMA) основан на разделении *полосы пропускания* канала на группу полос частот (*рис. 3.10*), образующих *логические каналы*.

Широкая полоса пропускания канала делится на ряд узких полос, разделенных защитными полосами. Размеры узких полос могут быть различными.

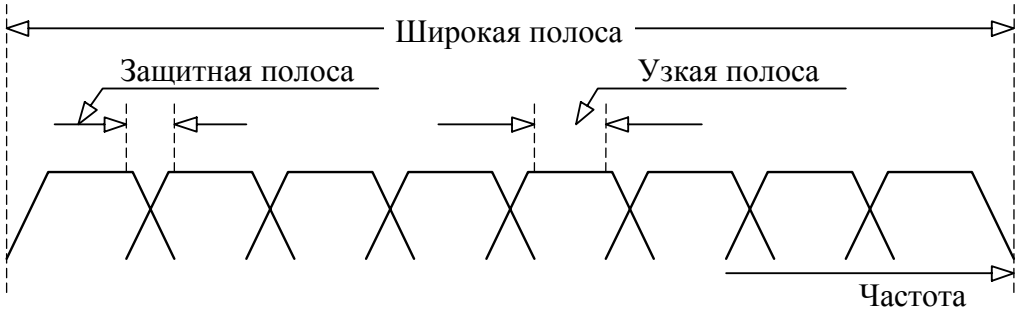


Рис. 3.10. Схема выделения логических каналов

При использовании FDMA, именуемого также **множественным доступом с разделением волны (WDMA)**, широкая полоса пропускания канала делится на ряд узких полос, разделенных защитными полосами. В каждой узкой полосе создается логический канал. Размеры узких полос могут быть различными. Передаваемые по логическим каналам сигналы накладываются на разные несущие и поэтому в частотной области не должны пересекаться. Вместе с этим, иногда, несмотря на наличие защитных полос, спектральные составляющие сигнала могут выходить за границы логического канала и вызывать *шум* в соседнем логическом канале.

В *оптических* каналах разделение частоты осуществляется направлением в каждый из них лучей света с различными частотами. Благодаря этому пропускная способность физического канала увеличивается в несколько раз. При осуществлении этого мультиплексирования в один световод большое число лазеров излучает свет (на различных частотах). Через световод излучение каждого из них проходит независимо от другого. На приемном конце разделение частот сигналов, прошедших физический канал, осуществляется путем фильтрации выходных сигналов.

Метод доступа FDMA относительно прост, но для его реализации необходимы передатчики и приемники, работающие на различных частотах.

Выводы

1. В современных сетях, в основном, используются следующие методы доступа: множественный доступ с прослушиванием несущей и разрешением коллизий; множественный доступ с передачей

полномочия, или метод с передачей маркера; множественный доступ с разделением во времени; множественный доступ с разделением частоты, или множественный доступ с разделением длины волны.

2. Множественный доступ с прослушиванием несущей является самым простым с точки зрения реализации и применяется в технологии Ethernet в качестве базового.

3. Множественный доступ с передачей полномочия, применяемый в сетевых технологиях типа Token Ring или Token Bus гарантирует определенное время доставки блоков данных в сети, а также дает возможность предоставления различных приоритетов передачи данных, но включение новой рабочей станции и/или ее отключение приводит к изменениям адресов всей системы.

4. Множественный доступ с разделением во времени, используемый при передаче речи или мультимедийной информации, позволяет организовать передачу данных с коммутацией пакетов и с коммутацией каналов.

5. Множественный доступ с разделением частоты нашел применение в беспроводных системах связи, в то же время множественный доступ с разделением длины волны активно применяется в оптоволоконных системах.

3.3. Семиуровневая модель OSI

Для единого представления данных в сетях с неоднородными устройствами и программным обеспечением международная организация по стандартам ISO (International Standartization Organization) разработала базовую **модель связи открытых систем OSI** (Open System Interconnection). Эта модель описывает правила и процедуры передачи данных в различных сетевых средах при организации сеанса связи. Основными элементами модели являются уровни, прикладные процессы и физические средства соединения. На *рис. 3.11* представлена структура базовой модели.

Каждый уровень модели OSI выполняет определенную задачу в процессе передачи данных по сети. Базовая модель является основой для разработки сетевых протоколов. OSI разделяет коммуникационные функции в сети на семь уровней, каждый из которых обслуживает различные части процесса взаимодействия открытых систем.

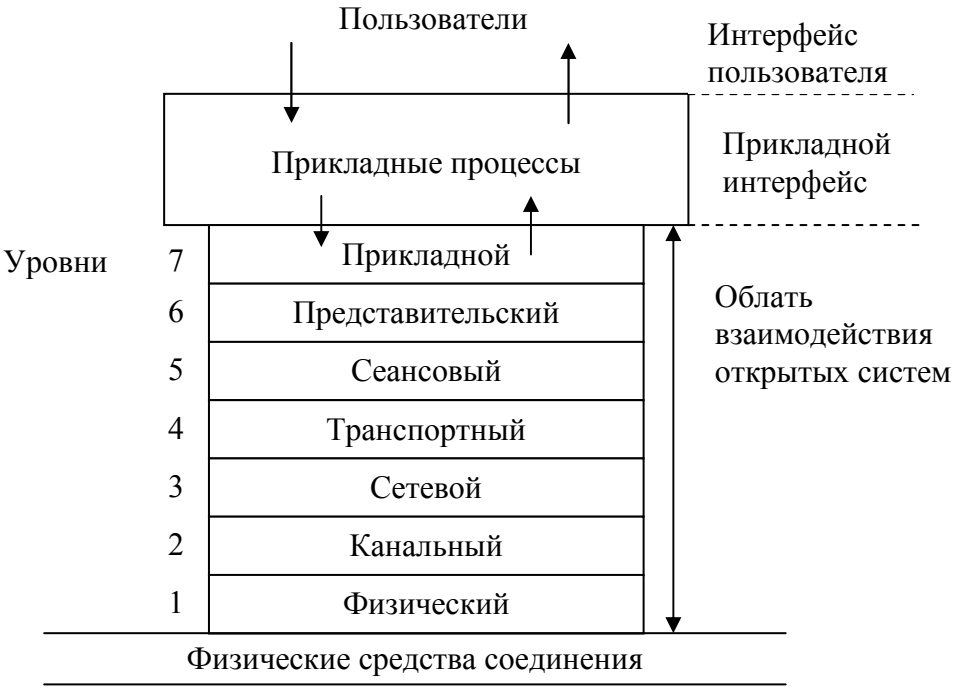


Рис. 3.11. Модель OSI

Модель OSI описывает только системные средства взаимодействия, при этом не затрагивает приложений конечных пользователей. Приложения реализуют свои собственные протоколы взаимодействия, обращаясь к системным средствам. Если приложение может взять на себя функции некоторых верхних уровней модели OSI, то для обмена данными оно обращается напрямую к системным средствам, выполняющим функции оставшихся нижних уровней модели OSI.

3.3.1. Взаимодействие уровней модели OSI

Модель OSI можно разделить на 2 различные модели (*рис. 3.12*):

– **горизонтальную модель** на базе протоколов, обеспечивающую механизм взаимодействия программ и процессов на различных машинах;

– **вертикальную модель** на основе услуг, обеспечиваемых соседними уровнями друг другу на одной машине.

Каждый уровень компьютера-отправителя взаимодействует с таким же уровнем компьютера-получателя, как будто он связан напрямую. Такая связь называется **логической** или ***виртуальной связью***. В действительности взаимодействие осуществляется между смежными уровнями одного компьютера.

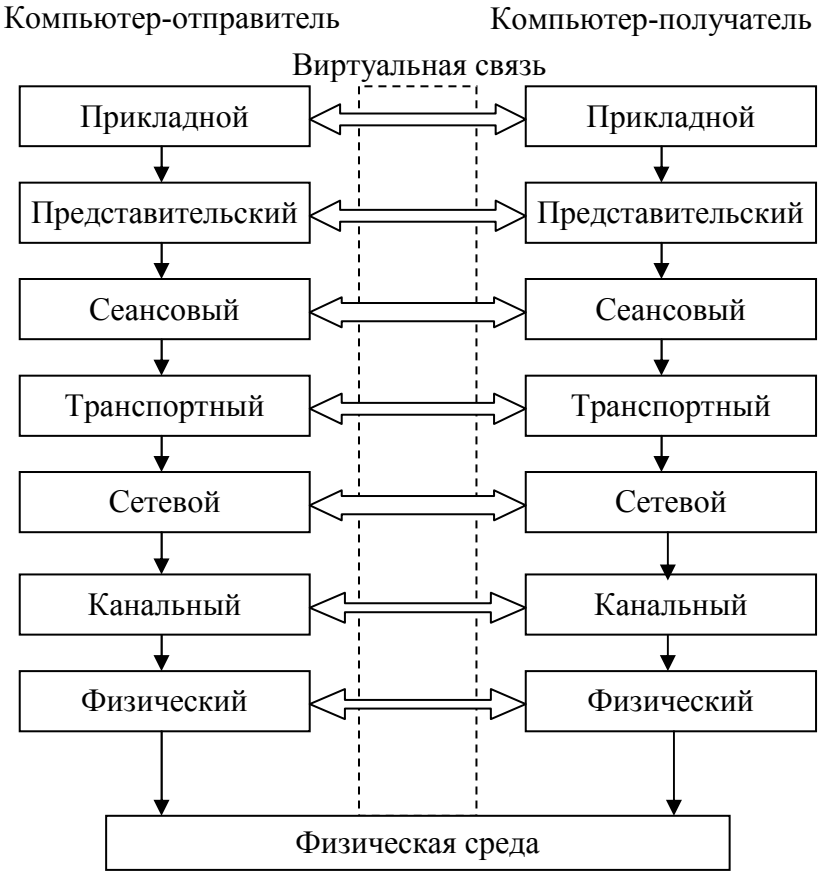


Рис. 3.12. Схема взаимодействия компьютеров в базовой эталонной модели OSI

Итак, информация на компьютере-отправителе должна пройти через все уровни. Затем она передается по физической среде до компьютера-получателя и опять проходит сквозь все слои, пока не доходит до того же уровня, с которого она была послана на компьютере-отправителе.

В горизонтальной модели двум программам требуется общий протокол для обмена данными. В вертикальной модели соседние уровни обмениваются данными с использованием интерфейсов прикладных программ *API* (Application Programming Interface).

Перед подачей в сеть данные разбиваются на *пакеты*. При отправке данных пакет проходит последовательно через все уровни программного обеспечения. На каждом уровне к пакету добавляется управляющая информация данного уровня (заголовок), которая необходима для успешной передачи данных по сети, как это показано на *рис. 3.13*, где *Заг* – заголовок пакета, *Кон* – конец пакета.

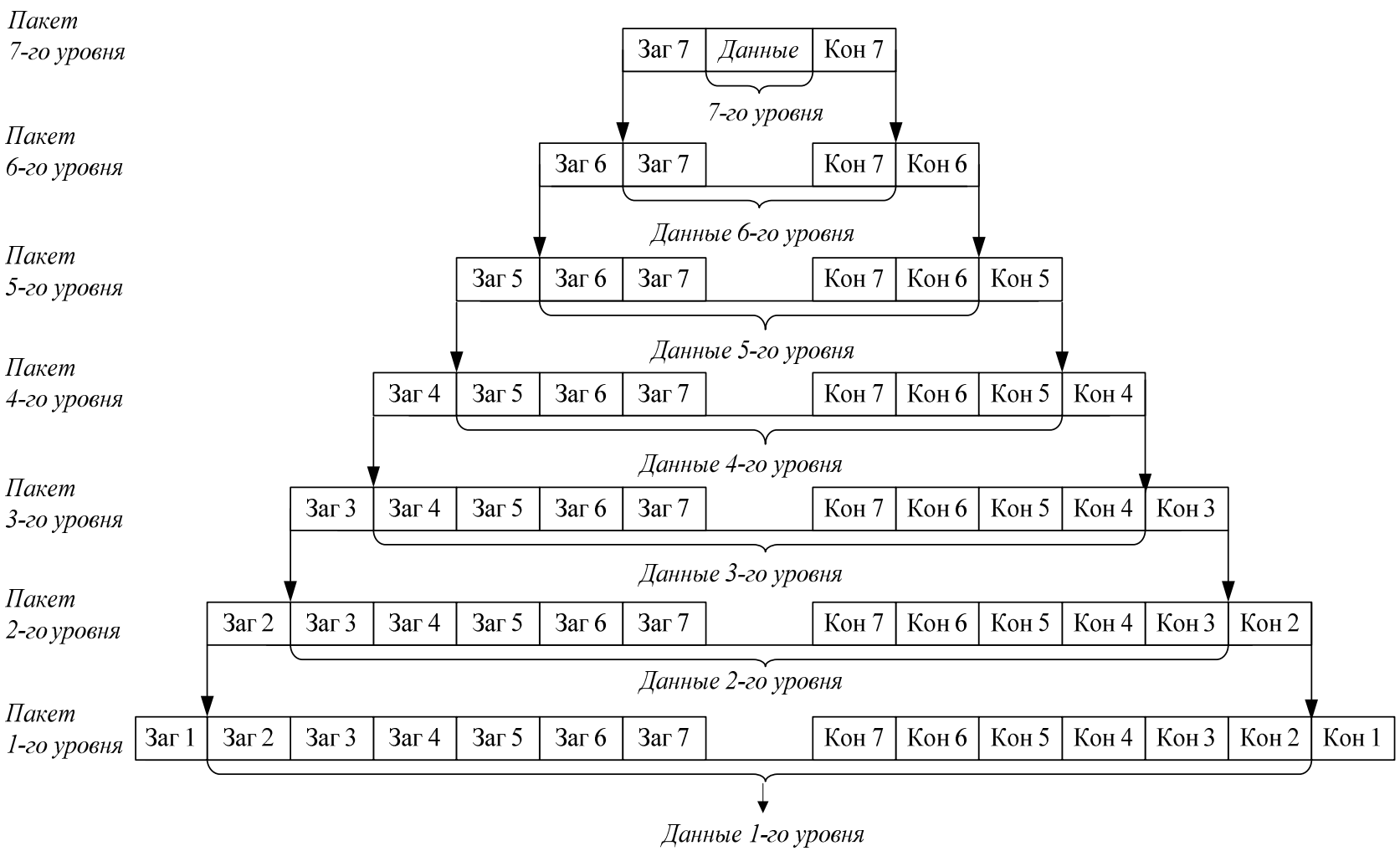


Рис. 3.13. Формирование пакета каждого уровня семиуровневой модели

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

Каждый уровень модели выполняет свою функцию. Чем выше уровень, тем более сложную задачу он решает. Отдельные уровни модели OSI удобно рассматривать как группы программ, предназначенных для выполнения конкретных функций. Один уровень, к примеру, отвечает за обеспечение преобразования данных из ASCII в EBCDIC и содержит программы, необходимые для выполнения этой задачи.

Каждый уровень обеспечивает сервис для вышестоящего уровня, запрашивая в свою очередь, сервис у нижестоящего уровня. Верхние уровни запрашивают сервис почти одинаково: как правило, это требование маршрутизации каких-то данных из одной сети в другую. Практическая реализация принципов адресации данных возложена на нижние уровни.

Рассматриваемая модель определяет *взаимодействие открытых систем* разных производителей в одной сети. Поэтому она выполняет для них координирующие действия по следующим аспектам:

- взаимодействие прикладных процессов;
- формы представления данных;
- единообразное хранение данных;
- управление сетевыми ресурсами;
- безопасность данных и защита информации;
- диагностика программ и технических средств.

В *таблице* представлено краткое описание функций всех уровней модели OSI.

Краткое описание функций уровней модели OSI

Наименование уровня	Функция
Прикладной	Представляет набор интерфейсов, позволяющий получить доступ к сетевым службам
Представления	Преобразует данные в общий формат

Окончание таблицы

Наименование уровня	Функция
Сеансовый	Поддержка взаимодействия (сеанса) между удаленными процессами
Транспортный	Управляет передачей данных по сети, обеспечивает подтверждение передачи
Сетевой	Маршрутизация, управление потоками данных, адресацией сообщений для доставки, преобразование логических сетевых адресов и имен в соответствующие им физические
Канальный	Управляет формированием кадров (LLC) и доступом к среде (MAC)
Физический	Битовые протоколы передачи данных

3.3.2. Физический уровень

Физический уровень (Physical Layer) предназначен для сопряжения с физическими средствами соединения.

Физические средства соединения – это совокупность физической среды, аппаратных и программных средств, обеспечивающая передачу сигналов между системами.

Физическая среда – это материальная субстанция, через которую осуществляется передача сигналов. Физическая среда является основой, на которой строятся физические средства соединения. В качестве физической среды широко используются эфир, металлы, оптическое стекло и кварц.

Физический уровень состоит из *подуровня стыковки* со средой и *подуровня преобразования передачи*. Первый из них обеспечивает сопряжение потока данных с используемым физическим каналом связи. Второй осуществляет преобразования, связанные с применяемыми протоколами.

Физический уровень обеспечивает физический интерфейс с каналом передачи данных, а также описывает процедуры передачи сигналов в канал и получения их из канала. На этом уровне определяются электрические, механические, функциональные и процедурные параметры для физической связи в системах. Физический уровень получает пакеты данных от вышележащего канального уровня и преобразует их в оптические или электрические сигналы, соответствующие 0 и 1 бинарного потока. Эти сигналы

посылаются через среду передачи на приемный узел. Механические и электрические/оптические свойства среды передачи определяются на физическом уровне и включают:

- тип кабелей и разъемов;
- разводку контактов в разъемах;
- схему кодирования сигналов для значений 0 и 1.

Физический уровень выполняет следующие функции:

- установление и разъединение физических соединений;
- передача сигналов в последовательном коде и прием;
- прослушивание, в нужных случаях, каналов;
- идентификация каналов;
- оповещение о появлении неисправностей и отказов.

Оповещение о появлении неисправностей и отказов связано с тем, что на физическом уровне происходит обнаружение определенного класса событий, мешающих нормальной работе сети (столкновение кадров, посланных сразу несколькими системами, обрыв канала, отключение питания, потеря механического контакта и т. д.). Виды сервиса, предоставляемого канальному уровню, определяются протоколами физического уровня. Прослушивание канала необходимо в тех случаях, когда к одному каналу подключается группа систем, но одновременно передавать сигналы разрешается только одной из них. Поэтому прослушивание канала позволяет определить, свободен ли он для передачи. В ряде случаев для более четкого определения структуры физический уровень разбивается на несколько подуровней. Например, физический уровень беспроводной сети делится на три подуровня (*рис. 3.14*).

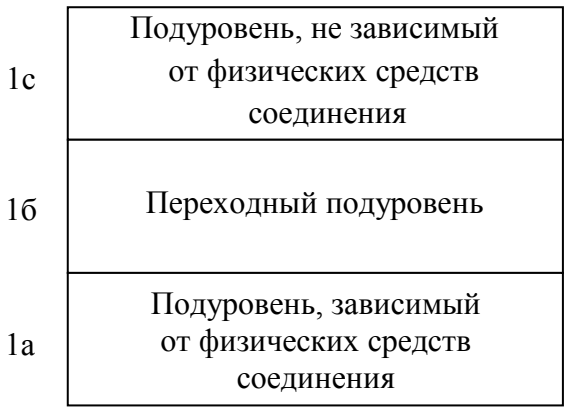


Рис. 3.14. Физический уровень беспроводной локальной сети

Функции физического уровня реализуются во всех устройствах, подключенных к сети. Со стороны компьютера функции физического уровня выполняются сетевым адаптером. Повторители являются единственным типом оборудования, которое работает только на физическом уровне.

На данном уровне выполняется преобразование данных, поступающих от более высокого уровня, в сигналы, передаваемые по кабелю. В глобальных сетях на этом уровне могут использоваться модемы и интерфейс ***RS-232C***. В локальных сетях для преобразования данных применяют сетевые адаптеры, обеспечивающие скоростную передачу данных в цифровой форме. Пример протокола физического уровня – это широко известный интерфейс ***RS-232C/CCITT V.2***, который является наиболее широко распространенной стандартной последовательной связью между компьютерами и периферийными устройствами.

Можно считать этот уровень отвечающим за аппаратное обеспечение. Физический уровень может обеспечивать как *асинхронную* (последовательную), так и *синхронную* (параллельную) передачу, которая применяется для некоторых мэйнфреймов и миникомпьютеров. На физическом уровне должна быть определена схема кодирования для представления двоичных значений с целью их передачи по каналу связи. Во многих локальных сетях используется манчестерское кодирование.

Примером протокола физического уровня может служить спецификация 100Base-T технологии Ethernet, которая определяет в качестве используемого кабеля *неэкранированную витую пару* категории 5 с волновым сопротивлением 100 Ом, разъем RJ-45, максимальную длину физического сегмента 100 метров, манчестерский код для представления данных на кабеле и другие характеристики среды и электрических сигналов.

К числу наиболее распространенных спецификаций физического уровня относятся:

– EIA-RS-232-C, CCITT V.24/V.28 – механические/электрические характеристики несбалансированного последовательного интерфейса;

– EIA-RS-422/449, CCITT V.10 – механические, электрические и оптические характеристики сбалансированного последовательного интерфейса;

– Ethernet – сетевая технология по стандарту IEEE 802.3 для сетей, использующая шинную топологию и коллективный доступ с прослушиванием несущей и обнаружением конфликтов;

– Token Ring – сетевая технология по стандарту IEEE 802.5, использующая кольцевую топологию и метод доступа к кольцу с передачей маркера.

Модель OSI представляет собой 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, сервисами, предоставляемыми на верхних уровнях, и прочими параметрами.

Иерархически организованная совокупность протоколов, решающих задачу взаимодействия узлов сети, называется **стеком коммуникационных протоколов**. Протоколы соседних уровней, находящихся в одном узле, взаимодействуют друг с другом также в соответствии с четко определенными правилами и с помощью стандартизованных форматов сообщений. Эти правила принято называть **интерфейсом**. Интерфейс определяет набор услуг, которые нижележащий уровень предоставляет вышележащему уровню.

3.3.3. Канальный уровень

Единицей информации **канального уровня (Data Link)** является *кадр* (*frame*).

Кадр – это логически организованная структура, в которую можно помещать данные (взаимосвязь *кадра* и *пакета* представлена в подразделе 3.1). Задача канального уровня – передавать кадры от сетевого уровня к физическому уровню.

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.

Канальный уровень обеспечивает корректность передачи каждого кадра, помещая специальную последовательность бит

в начало и конец каждого кадра, чтобы отметить его, а также вычисляет *контрольную сумму*, суммируя все байты кадра определенным способом и добавляя контрольную сумму к кадру. Когда кадр приходит, 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*.

Задача канального уровня – брать пакеты, поступающие с сетевого уровня, и готовить их к передаче, укладывая в кадр соответствующего размера. Этот уровень обязан определить, где начинается и где заканчивается блок, а также обнаруживать ошибки передачи.

На этом же уровне определяются правила использования физического уровня узлами сети. Электрическое представление данных в ЛВС (биты данных, методы кодирования данных и маркеры) распознается на этом и только на этом уровне. Здесь обнаруживаются и исправляются (путем требований повторной передачи данных) ошибки.

Канальный уровень обеспечивает создание, передачу и прием кадров данных. Этот уровень обслуживает запросы сетевого уровня и использует сервис физического уровня для приема и передачи пакетов.

Спецификации IEEE 802.X делят канальный уровень на два подуровня:

– LLC-подуровень (Logical Link Control) – управление логическим каналом осуществляет логический контроль связи. Подуровень LLC обеспечивает обслуживание сетевого уровня и связан с передачей и приемом пользовательских сообщений;

– MAC-подуровень (Media Access Control) – контроль доступа к среде. Подуровень MAC регулирует доступ к разделяемой физической среде (передача маркера или обнаружение коллизий или столкновений) и управляет доступом к каналу связи. Подуровень LLC находится выше подуровня MAC.

Канальный уровень определяет доступ к среде и управление передачей посредством процедуры передачи данных по каналу. При больших размерах передаваемых блоков данных канальный уровень делит их на кадры и передает кадры в виде последовательностей. При получении кадров уровень формирует

из них переданные блоки данных. Размер блока данных зависит от способа передачи, качества канала, по которому он передается.

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.

Канальный уровень может выполнять следующие виды функций:

– организация (установление, управление, расторжение) канальных соединений и идентификация их портов;
– организация и передача кадров;
– обнаружение и исправление ошибок;
– управление потоками данных;
– обеспечение прозрачности логических каналов (передачи по ним данных, закодированных любым способом).

Наиболее часто используемые протоколы на канальном уровне включают:

– HDLC (High Level Data Link Control) – протокол управления каналом передачи данных высокого уровня, для последовательных соединений;
– IEEE 802.2 LLC (тип I и тип II) обеспечивают MAC для сред 802.x;
– Ethernet – сетевая технология по стандарту IEEE 802.3 для сетей, использующая шинную топологию и коллективный доступ с прослушиванием несущей и обнаружением конфликтов;
– Token Ring – сетевая технология по стандарту IEEE 802.5, использующая кольцевую топологию и метод доступа к кольцу с передачей маркера;
– FDDI (Fiber Distributed Date Interface Station) – сетевая технология по стандарту IEEE 802.6, использующая оптоволоконный носитель;
– X.25 – международный стандарт для глобальных коммуникаций с коммутацией пакетов;
– Frame relay – сеть, организованная из технологий X25 и ISDN.

3.3.4. Сетевой уровень

Сетевой уровень (Network layer) служит для образования единой транспортной системы, объединяющей несколько сетей, причем эти сети могут использовать совершенно различные

принципы передачи сообщений между конечными узлами и обладать произвольной структурой связей. Сетевой уровень обеспечивает прокладку каналов, соединяющих абонентские и административные системы через коммуникационную сеть, и выбор наиболее быстрого и надежного пути.

Сетевой уровень устанавливает связь в вычислительной сети между двумя системами и обеспечивает прокладку *виртуальных каналов* между ними.

Виртуальный, или **логический, канал** – это такое функционирование компонентов сети, при котором между взаимодействующими компонентами создается иллюзия прокладки нужного канала. Кроме этого, сетевой уровень сообщает транспортному уровню о появляющихся ошибках.

Протокол канального уровня обеспечивает доставку данных любым узлам только в сети с соответствующей *типовой топологией*. Это очень жесткое ограничение, которое не позволяет строить сети с развитой структурой, например, сети, объединяющие несколько сетей предприятия в единую сеть, или высоконадежные сети, в которых существуют избыточные связи между узлами.

Таким образом, внутри сети доставка данных регулируется канальным уровнем, а вот доставкой данных между сетями занимается сетевой уровень. При организации доставки пакетов на сетевом уровне используется понятие номер сети. В этом случае **адрес получателя** состоит из **номера сети** и **номера компьютера** в этой сети.

Сети соединяются между собой специальными устройствами, называемыми маршрутизаторами.

Маршрутизатор – это устройство, которое собирает информацию о топологии межсетевых соединений и на ее основании пересылает пакеты сетевого уровня в сеть назначения. Для того чтобы передать сообщение от отправителя, находящегося в одной сети, получателю, находящемуся в другой сети, нужно совершить некоторое количество транзитных передач (hops) между сетями, каждый раз выбирая подходящий маршрут. Таким образом, маршрут представляет собой последовательность маршрутизаторов, по которым проходит пакет.

На *рис. 3.15* показаны четыре сети, связанные маршрутизаторами. Между узлами *A* и *B* данной сети пролегают два маршрута:

первый – через маршрутизаторы 1 и 3, а второй – через маршрутизаторы 1, 2 и 3.

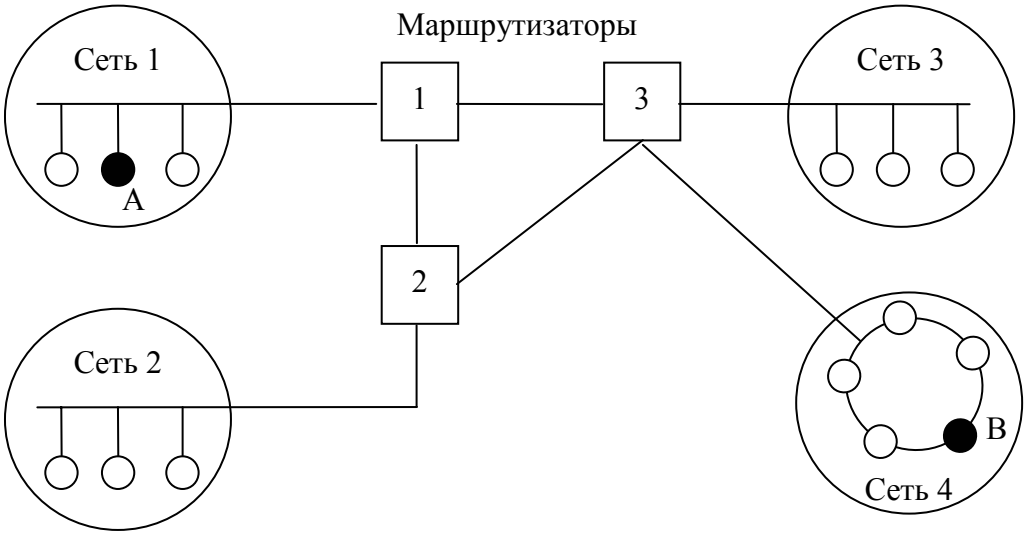


Рис. 3.15. Пример составной сети

Прокладка наилучшего пути для передачи данных называется **маршрутизацией**, и ее решение является главной задачей 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 модели OSI отвечает за деление пользователей на группы и маршрутизацию пакетов на основе преобразования MAC-адресов в *сетевые адреса*. Сетевой уровень обеспечивает также прозрачную передачу пакетов на транспортный уровень.

В целом, сетевой уровень выполняет функции:

- создание сетевых соединений и идентификация их портов;
- управление потоками пакетов;

– организация (упорядочение) последовательностей пакетов;
– маршрутизация и коммутация;
– сегментирование и объединение пакетов.

На сетевом уровне определяется два вида протоколов. Первый вид относится к определению правил передачи пакетов с данными конечных узлов от узла к маршрутизатору и между маршрутизаторами. 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. 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.

Наиболее часто на сетевом уровне используются протоколы:

– IP (Internet Protocol) – протокол Internet, сетевой протокол стека TCP/IP, который предоставляет адресную и маршрутную информацию;
– IPX (Internetwork Packet Exchange) – протокол межсетевого обмена пакетами, предназначенный для адресации и маршрутизации пакетов в сетях Novell;
– X.25 – международный стандарт для глобальных коммуникаций с коммутацией пакетов (частично этот протокол реализован на уровне 2);
– CLNP (Connection Less Network Protocol) – сетевой протокол без организации соединений.

3.3.5. Транспортный уровень

Транспортный уровень (Transport Layer) предназначен для передачи пакетов через коммуникационную сеть.

На пути от отправителя к получателю пакеты могут быть *искажены* (появятся *ошибки*) или утеряны. Хотя некоторые приложения имеют собственные средства обработки (обнаружения и/или исправления) ошибок, существуют и такие, которые изначально предполагают реализацию надежного соединения.

Работа транспортного уровня заключается в том, чтобы обеспечить приложениям или верхним уровням модели (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 качеством 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.

Транспортный уровень определяет логическую адресацию физических устройств (систем, их частей) в сети. Этот уровень гарантирует доставку информации адресатам и управляет этой доставкой. Его главной задачей является обеспечение эффективных, удобных и надежных форм передачи информации между системами. Когда в процессе обработки находится более одного пакета, транспортный уровень контролирует очередность прохождения пакетов. Если проходит дубликат принятого ранее пакета, то данный уровень опознает это и игнорирует пакет.

В функции транспортного уровня входят:

– управление передачей по сети и обеспечение целостности пакетов данных;

– обнаружение ошибок, частичная их ликвидация и сообщение о неисправленных ошибках;

– восстановление передачи после отказов и неисправностей;

– укрупнение или разделение пакетов данных;

– предоставление приоритетов при передаче пакетов (нормальная или срочная);

– подтверждение передачи;

– ликвидация пакетов при тупиковых ситуациях в сети.

Начиная с транспортного уровня, все вышележащие протоколы реализуются программными средствами, обычно включаемыми в состав сетевой операционной системы.

Наиболее распространенные протоколы транспортного уровня включают в себя:

– TCP (Transmission Control Protocol) – протокол управления передачей стека TCP/IP;

– UDP (User Datagram Protocol) – пользовательский протокол дейтаграмм стека TCP/IP;

– NCP (NetWare Core Protocol) – базовый протокол сетей NetWare;

– SPX (Sequenced Packet eXchange) – упорядоченный обмен пакетами стека Novell;

– TP4 (Transmission Protocol) – протокол передачи класса 4.

3.3.6. Сеансовый уровень

Сеансовый уровень (Session layer) – это уровень, определяющий процедуру проведения сеансов между пользователями или прикладными процессами.

Сеансовый уровень обеспечивает управление диалогом для того, чтобы фиксировать, какая из сторон является активной в настоящий момент, а также предоставляет средства синхронизации. Последние позволяют вставлять контрольные точки в длинные передачи, чтобы в случае отказа можно было вернуться назад к последней контрольной точке вместо того, чтобы начинать все сначала. На практике немногие приложения используют сеансовый уровень, и он редко реализуется.

Сеансовый уровень управляет передачей информации между прикладными процессами, координирует прием, передачу и выдачу одного сеанса связи. Кроме того, сеансовый уровень содержит дополнительно функции управления паролями, управления диалогом, синхронизации и отмены связи в сеансе передачи после сбоя вследствие ошибок в нижерасположенных уровнях.

Функции этого уровня состоят в координации связи между двумя прикладными программами, работающими на разных рабочих станциях. Это происходит в виде хорошо структурированного диалога. В число этих функций входит создание сеанса, управление передачей и приемом пакетов сообщений во время сеанса и завершение сеанса.

На сеансовом уровне определяется, какой будет передача между двумя прикладными процессами:

– ***полудуплексной*** (half duplex; процессы или средства будут передавать и принимать данные по очереди);

– ***дуплексной*** (duplex или full duplex; процессы или средства будут передавать и принимать данные одновременно).

В полудуплексном режиме сеансовый уровень выдает маркер данных тому процессу, который начинает передачу. Когда второму процессу приходит время отвечать, маркер данных передается ему. Сеансовый уровень разрешает передачу только той стороне, которая обладает маркером данных.

Сеансовый уровень обеспечивает выполнение следующих функций:

– установление и завершение на сеансовом уровне соединения между взаимодействующими системами;

– выполнение нормального и срочного обмена данными между прикладными процессами;

– управление взаимодействием прикладных процессов;

– синхронизация сеансовых соединений;

– извещение прикладных процессов об исключительных ситуациях;

– установление в прикладном процессе меток, позволяющих после отказа либо ошибки восстановить его выполнение от ближайшей метки;

– прерывание в нужных случаях прикладного процесса и его корректное возобновление;

– прекращение сеанса без потери данных;

– передача особых сообщений о ходе проведения сеанса.

Сеансовый уровень отвечает за организацию сеансов обмена данными между оконечными машинами. Протоколы сеансового уровня обычно являются составной частью протоколов трех верхних уровней модели.

3.3.7. Уровень представления данных

Уровень представления данных (представительский уровень) (Presentation layer) представляет данные, передаваемые между прикладными процессами, в нужной форме.

Этот уровень обеспечивает то, что информация, передаваемая прикладным уровнем, будет «понятна» прикладному уровню в другой системе или транспортному уровню той же системы. В случаях необходимости уровень представления в момент передачи информации выполняет преобразование форматов данных в некоторый общий формат представления, а в момент приема, соответственно, выполняет обратное преобразование.

Таким образом, прикладные уровни могут преодолеть, например, синтаксические различия в представлении данных. Такая ситуация может возникнуть в ЛВС с неоднотипными компьютерами (IBM PC и Macintosh), которым необходимо обмениваться данными. Так, в полях баз данных информация должна быть представлена в виде букв и цифр, а зачастую и в виде графического изображения. Обрабатывать же эти данные нужно, например, как числа с плавающей запятой.

В основу общего представления данных положена единая для всех уровней модели система ASN.1. Эта система служит для описания структуры файлов, а также позволяет решить проблему шифрования данных. На этом уровне может выполняться шифрование и дешифрование данных, благодаря которым секретность обмена данными обеспечивается сразу для всех прикладных сервисов. Примером такого протокола является протокол **Secure Socket Layer (SSL)**, который обеспечивает секретный обмен сообщениями для протоколов прикладного уровня стека TCP/IP.

Представительский уровень выполняет следующие основные функции:

– генерация запросов на установление сеансов взаимодействия прикладных процессов;

– согласование представления данных между прикладными процессами;

– реализация форм представления данных;

– представление графического материала (чертежей, рисунков, схем);

– засекречивание данных;

– передача запросов на прекращение сеансов.

Протоколы уровня представления данных обычно являются составной частью протоколов трех верхних уровней модели.

3.3.8. Прикладной уровень

Прикладной уровень (Application layer) обеспечивает прикладным процессам средства доступа к области взаимодействия, является верхним (седьмым) уровнем и непосредственно примыкает к прикладным процессам. В действительности прикладной уровень – это 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, например, с помощью протокола электронной почты. Специальные элементы прикладного сервиса обеспечивают сервис для конкретных прикладных программ, таких как программы пересылки файлов и эмуляции терминалов. Если, например, программе необходимо переслать файлы, то обязательно будет использован ***протокол передачи, доступа и управления файлами*** (File Transfer Access and Management, FTAM). В модели OSI прикладная программа, которой нужно выполнить конкретную задачу (например, обновить базу данных на компьютере), посылает конкретные данные в виде **дейтаграммы** (datagram) на прикладной уровень. Одна из основных задач этого уровня – определить, как следует обрабатывать запрос прикладной программы. Другими словами, какой вид должен принять данный запрос.

Единица данных, которой оперирует прикладной уровень, обычно называется **сообщением** (message).

Прикладной уровень выполняет следующие функции:

– описание форм и методов взаимодействия прикладных процессов;

– выполнение различных видов работ;

– передача файлов;

– управление заданиями;

– управление системой;

– идентификация пользователей по их паролям, адресам, электронным подписям;

– определение функционирующих абонентов и возможности доступа к новым прикладным процессам;

– определение достаточности имеющихся ресурсов;

– организация запросов на соединение с другими прикладными процессами;

– передача заявок представительскому уровню на необходимые методы описания информации;

– выбор процедур планируемого диалога процессов;

– управление данными, которыми обмениваются прикладные процессы и синхронизация взаимодействия прикладных процессов;

– определение качества обслуживания (время доставки блоков данных, допустимой частоты ошибок);

– соглашение об исправлении ошибок и определении достоверности данных;

– согласование ограничений, накладываемых на синтаксис (наборы символов, структура данных).

Указанные функции определяют виды сервиса, которые прикладной уровень предоставляет прикладным процессам. Кроме этого, прикладной уровень передает прикладным процессам сервис, предоставляемый физическим, канальным, сетевым, транспортным, сеансовым и представительским уровнями.

На прикладном уровне необходимо предоставить в распоряжение пользователей уже переработанную информацию. С этим может справиться системное и пользовательское программное обеспечение.

Прикладной уровень отвечает за доступ приложений в сеть. Задачами этого уровня является перенос файлов, обмен почтовыми сообщениями и управление сетью.

К числу наиболее распространенных протоколов верхних трех уровней относятся:

– FTP (File Transfer Protocol) – протокол передачи файлов;

– TFTP (Trivial File Transfer Protocol) – простейший протокол пересылки файлов;

– X.400 – электронная почта;

– Telnet – работа с удаленным терминалом;

– SMTP (Simple Mail Transfer Protocol) – простой протокол почтового обмена;

– CMIP (Common Management Information Protocol) – общий протокол управления информацией;

– SLIP (Serial Line IP) – IP для последовательных линий. Протокол последовательной посимвольной передачи данных;

– SNMP (Simple Network Management Protocol) – простой протокол сетевого управления;

– FTAM (File Transfer, Access, and Management) – протокол передачи, доступа и управления файлами.

Выводы

1. В компьютерных сетях идеологической основой стандартизации является многоуровневый подход к разработке средств сетевого взаимодействия.

2. Формализованные правила, определяющие последовательность и формат сообщений, которыми обмениваются сетевые компоненты, лежащие на одном уровне, но в разных узлах, называются протоколом.

3. Формализованные правила, определяющие взаимодействие сетевых компонентов соседних уровней одного узла, называются интерфейсом. Интерфейс определяет набор сервисов, предоставляемый данным уровнем соседнему уровню.

4. Иерархически организованный набор протоколов, достаточный для организации взаимодействия узлов в сети, называется стеком коммуникационных протоколов.

5. Открытой системой может быть названа любая система, которая построена в соответствии с общедоступными спецификациями, соответствующими стандартам и принятыми в результате публичного обсуждения всеми заинтересованными сторонами.

6. Модель OSI стандартизует взаимодействие открытых систем. Она определяет семь уровней взаимодействия: прикладной, представительский, сеансовый, транспортный, сетевой, канальный и физический.

7. Три нижних уровня физический, канальный и сетевой являются сетезависимыми – протоколы этих уровней тесно связаны с технической реализацией сети, с используемым коммуникационным оборудованием.

8. Важнейшим направлением стандартизации в области вычислительных сетей является стандартизация коммуникационных протоколов. Наиболее популярными являются стеки: TCP/IP, IPX/SPX, NetBIOS/SMB, DECnet, SNA и OSI.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Дайте определение пакета.
2. В чем заключаются преимущества использования пакетов?
3. Дайте определение времени доступа.
4. Опишите типичную стуктуру пакета.
5. Для чего предназначена преамбула в пакете?
6. Для чего предназначена служебная информация в пакете?
7. Что такое инкапсуляция пакетов?

8. Что такое «метод доступа» и как он влияет на передачу данных в сети?

9. Какие существуют методы доступа?

10. Охарактеризуйте метод доступа с прослушиванием несущей и разрешением коллизий.

11. При каком методе доступа обе станции могут одновременно начать передачу и войти в конфликт?

12. В каких сетевых технологиях используется метод CSMA/CD?

13. Охарактеризуйте метод доступа с разделением во времени и перечислите, в каких случаях используется данный метод.

14. Что такое маркер?

15. В каком случае рабочая станция может начать передачу данных при использовании метода доступа с передачей полномочия?

16. Охарактеризуйте метод доступа с передачей полномочия.

17. Охарактеризуйте метод множественного доступа с разделением частоты.

18. Какие существуют варианты использования множественного доступа с разделением во времени?

19. Что такое OSI?

20. Каково назначение базовой модели взаимодействия открытых систем?

21. На какие уровни разбивается базовая модель OSI?

22. Что обеспечивает горизонтальная составляющая модели взаимодействия открытых систем?

23. Какие элементы являются основными элементами для базовой модели взаимодействия открытых систем?

24. Какие функции выполняются на физическом уровне?

25. Какие вопросы решаются на физическом уровне?

26. Какой уровень модели OSI преобразует данные в общий формат для передачи по сети?

27. Какое оборудование используется на физическом уровне?

28. Какие известны спецификации физического уровня?

29. Перечислите функции канального уровня.

30. Каковы функции канального уровня?

31. На какие подуровни разделяется канальный уровень? Опишите их функции.

32. Какие протоколы используются на канальном уровне?
33. Какое оборудование используется на канальном уровне?
34. Какие функции выполняются, какие протоколы используются на сетевом уровне?
35. Какое оборудование используется на сетевом уровне?
36. Перечислите функции транспортного уровня.
37. Какие протоколы используются на транспортном уровне?
38. Перечислите оборудование транспортного уровня.
39. Дайте определение сеансового уровня.
40. Какой уровень отвечает за доступ приложений в сеть?
41. Перечислите задачи уровня представления данных.
42. Перечислите функции прикладного уровня.
43. Перечислите протоколы верхних уровней.

4. ПОНЯТИЕ ПРОТОКОЛА. СТЕК ПРОТОКОЛОВ TCP/IP

4.1. Спецификации стандартов

Спецификации института инженеров по электротехнике и электронике (Institute of Electrical and Electronics Engineers, IEEE) IEEE 802 определяют стандарты для физических компонентов сети. Эти компоненты – ***сетевая карта*** (Network Interface Card, NIC) и ***сетевой носитель*** (network media) – относятся к физическому и канальному уровням модели OSI. Спецификации IEEE 802 определяют механизм доступа адаптера к каналу связи и механизм передачи данных. Стандарты IEEE 802 подразделяют канальный уровень на подуровни:

– Logical Link Control (LLC) – подуровень управления логической связью;

– Media Access Control (MAC) – подуровень управления доступом к устройствам.

Существует более двадцати спецификаций IEEE 802.

Стандарт IEEE 802.1 (Internetworking – *объединение сетей*) задает механизмы управления сетью на MAC-уровне. В разделе 802.1 приводятся основные понятия и определения, общие характеристики и требования к локальным сетям, а также поведение маршрутизации на канальном уровне, где логические адреса должны быть преобразованы в их физические адреса, и наоборот.

Стандарт IEEE 802.2 (Logical Link Control – *управление логической связью*) определяет функционирование подуровня LLC на канальном уровне модели OSI. LLC обеспечивает интерфейс между методами доступа к среде и сетевым уровнем.

Стандарт IEEE 802.3 (Ethernet Carrier Sense Multiple Access with Collision Detection, *CSMA/CD* LANs Ethernet – *множественный доступ к сетям Ethernet с проверкой несущей и обнаружением конфликтов*) описывает физический уровень и подуровень MAC для сетей, использующих шинную топологию и коллективный доступ с прослушиванием несущей и обнаружением конфликтов. Прототипом этого метода является метод доступа стандарта Ethernet (10BaseT, 10Base2, 10Base5).

Данный стандарт включает также технологии Fast Ethernet (100BaseTX, 100BaseFX, 100BaseFX):

– 100Base-TX – двухпарная витая пара; использует метод MLT-3 для передачи сигналов 5-битовых порций кода 4B/5B по витой паре, а также имеется функция автопереговоров (Auto-negotiation) для выбора режима работы порта;

– 100Base-T4 – четырехпарная витая пара; вместо кодирования 4B/5B в этом методе используется кодирование 8B/6T;

– 100BaseFX – многомодовое оптоволокно. Эта спецификация определяет работу протокола Fast Ethernet по многомодовому оптоволокну в полудуплексном и полнодуплексном режимах на основе хорошо проверенной схемы кодирования и передачи оптических сигналов, использующейся уже на протяжении ряда лет в стандарте FDDI. Как и в стандарте FDDI, каждый узел соединяется с сетью двумя оптическими волокнами, идущими от приемника (Rx) и от передатчика (TX).

Этот метод доступа используется в сетях с общей шиной (к которым относятся и радиосети, породившие этот метод). Все компьютеры такой сети имеют непосредственный доступ к общей шине, поэтому она может быть использована для передачи данных между любыми двумя узлами сети. Простота схемы подключения – это один из факторов, определивших успех стандарта Ethernet. Говорят, что кабель, к которому подключены все станции, работает в режиме **коллективного доступа** (Multiply Access, MA).

Метод доступа *CSMA/CD* определяет основные временные и логические соотношения, гарантирующие корректную работу всех станций в сети.

Все данные, передаваемые по сети, помещаются в кадры определенной структуры и снабжаются уникальным адресом станции назначения. Затем кадр передается по кабелю. Все станции, подключенные к кабелю, могут распознать факт передачи кадра, и та станция, которая узнает собственный адрес в заголовках кадра, записывает его содержимое в свой внутренний буфер, обрабатывает полученные данные и посылает по кабелю кадр-ответ. Адрес станции-источника также включен в исходный кадр, поэтому станция-получатель знает, кому нужно послать ответ.

Стандарт IEEE 802.4 (Token Bus LAN – *локальные сети Token Bus*) определяет метод доступа к шине с передачей маркера, прототип ArcNet.

При подключении устройств в ArcNet применяют топологию шина или звезда. Адаптеры ArcNet поддерживают метод доступа Token Bus (маркерная шина) и обеспечивают производительность 2,5 Мбит/с. Этот метод предусматривает следующие правила:

– все устройства, подключенные к сети, могут передавать данные, только получив разрешение на передачу (маркер);

– в любой момент времени только одна станция в сети обладает таким правом;

– кадр, передаваемый одной станцией, одновременно анализируется всеми остальными станциями сети.

В сетях ArcNet используется асинхронный метод передачи данных (в сетях Ethernet и Token Ring применяется синхронный метод), т. е. передача каждого байта в ArcNet выполняется посылкой ISU (Information Symbol Unit – единица передачи информации), состоящей из трех служебных старт/стоповых битов и восьми битов данных.

Стандарт IEEE 802.5 (Token Ring LAN – *локальные сети Token Ring*) описывает метод доступа к кольцу с передачей маркера, прототип – Token Ring.

Сети стандарта Token Ring, как и сети Ethernet, используют разделяемую среду передачи данных, которая состоит из отрезков кабеля, соединяющих все станции сети в кольцо. Кольцо рассматривается как общий разделяемый ресурс, и для доступа к нему используется алгоритм, основанный на передаче станциями права на использование кольца в определенном порядке. Право на использование кольца передается с помощью маркера, или токена.

Стандарт IEEE 802.6 (Metropolitan Area Network – *городские или муниципальные сети*) описывает рекомендации для региональных сетей.

Стандарт IEEE 802.7 (Broadband Technical Advisory Group – *техническая консультационная группа по широковещательной передаче*) описывает рекомендации по широкополосным сетевым технологиям, носителям, интерфейсу и оборудованию.

Стандарт IEEE 802.8 (Fiber Technical Advisory Group – *техническая консультационная группа по оптоволоконным сетям*) содержит обсуждение использования оптических кабелей в сетях со стандартом 802.3 – 802.6, а также рекомендации по оптоволоконным сетевым технологиям, носителям, интерфейсу и оборудованию, прототип – сеть *FDDI* (Fiber Distributed Data Interface).

Стандарт FDDI использует оптоволоконный кабель и доступ с применением *маркера*. Сеть FDDI строится на основе двух оптоволоконных колец, которые образуют основной и резервный пути передачи данных между узлами сети. Использование двух колец – это основной способ повышения отказоустойчивости в сети FDDI, и узлы, которые хотят им воспользоваться, должны быть подключены к обоим кольцам. Скорость сети – до 100 Мбит/с. Данная технология позволяет включать до 500 узлов на расстоянии 100 км.

Стандарт IEEE 802.9 (Integrated Voice and Data Network – *интегрированные сети передачи голоса и данных*) задает архитектуру и интерфейсы устройств одновременной передачи данных и голоса по одной линии, а также содержит рекомендации по гибридным сетям, в которых объединяют голосовой трафик и трафик данных в одной и той же сетевой среде.

В ***стандарте IEEE 802.10*** (Network Security – *сетевая безопасность*) рассмотрены вопросы обмена данными, *шифрования* (на основе криптографического преобразования информации), управления сетями и безопасности в сетевых архитектурах, совместимых с моделью OSI.

Стандарт IEEE 802.11 (Wireless Network – *беспроводные сети*) описывает рекомендации по использованию беспроводных сетей.

Стандарт IEEE 802.12 описывает *рекомендации по использованию сетей 100VG* – AnyLAN со скоростью100 Мбит/с и методом доступа по очереди запросов и по приоритету (Demand Priority Queuing, DPQ, Demand Priority Access, DPA).

Технология *100VG* – это комбинация Ethernet и Token Ring со скоростью передачи 100 Мбит/с, работающая на *неэкранированных витых парах*. В проекте 100Base-VG усовершенствован метод доступа с учетом потребности мультимедийных приложений. В спецификации *100VG* предусматривается поддержка волоконно-оптических кабельных систем. Технология 100VG использует метод доступа – *обработка запросов по приоритету* (*demand priority access*). В этом случае узлам сети предоставляется право равного доступа. Концентратор опрашивает каждый порт и проверяет наличие запроса на передачу, а затем разрешает этот запрос в соответствии с приоритетом. Имеется два уровня приоритетов – высокий и низкий.

Стандарт IEEE 802.14 определяет *функционирование кабельных модемов*.

Стандарт IEEE 802.15 (Personal Area Network, PAN – *персональные сети*) рассматривает вопросы организации персональных сетей. В настоящее время уже существует несколько спецификаций данного стандарта.

1. ***Стандарт IEEE 802.15.1*** базируется на спецификациях Bluetooth v1.x. и предназначен для построения так называемых персональных беспроводных сетей (Wireless Personal Area Network, WPAN). Для работы радиоинтерфейса *Bluetooth* используется так называемый нижний (2,45 ГГц) диапазон ISM (industrial, scientific, medical), предназначенный для работы промышленных, научных и медицинских приборов.

2. ***Стандарт IEEE 802.15.3*** предназначен для *беспроводных частных сетей* и является прямым наследником Bluetooth (частота 2,4 ГГц). IEEE 802.15.3 обеспечивает скорость передачи данных до 55 Мбит/с на расстоянии до 100 метров, одновременно работать в такой сети могут до 245 пользователей. Шифрование данных в сетях IEEE 802.15.3 может осуществлятся по стандарту AES 128.

3. ***Стандарт IEEE 802.15.4*** (ZigBee) ориентирован, главным образом, на использование в качестве средства связи между автономными приборами и оборудованием.

4. ***Стандарт IEEE 802.15.4a*** (Ultra Wideband, UWB) базируется на технологии сверхширокополосной связи (Ultra Wideband, UWB), основаннной на передаче множества закодированных импульсов негармонической формы очень малой мощности и малой длительности в широком диапазоне частот.

Стандарт IEEE 802.16 предназначен для реализации широкополосных каналов в городских сетях (MAN). В отличие от 802.11 он ориентирован на соединение стационарных, а не мобильных объектов. Его задачей является обеспечение сетевого уровня между локальными сетями (IEEE 802.11) и региональными сетями (WAN), где планируется применение разрабатываемого стандарта IEEE 802.20. Эти стандарты совместно со стандартом IEEE 802.15 и 802.17 образуют взаимосогласованную иерархию протоколов беспроводной связи.

Стандарт IEEE 802.17 называется RPR (Resilient Packet Ring – *адаптивное кольцо для пакетов*), и в отличие от FDDI (а также Token Ring или DQDB) пакеты удаляются из кольца

узлом-адресатом, что позволяет осуществлять несколько обменов одновременно.

Стандарт IEEE 802.18 представляет собой требования и рекомендации технической консультативной группы по радиочастотному регулированию – RTAG (*Radio Regulatory Technical Advisory Group*).

Стандарт IEEE 802.19 представляет собой требования и рекомендации технической консультативной группы по сосуществованию – CTAG (*Coexistence Technical Advisory Group*).

Стандарт IEEE 802.20 описывает правила беспроводного мобильного широкополосного доступа MBWA (*Mobile Broadband Wireless Access*) для пакетного интерфейса в беспроводных городских сетях WMAN. Этот стандарт должен поддерживать услуги по передаче данных с IP в качестве транспортного протокола и дополнять стандарт IEEE 802.16 в масштабе WiMAX. Стандарт обеспечивает скорость передачи данных более 1 Мбит/с и позволяет получить мобильный доступ к данным из движущихся транспортных средств (если скорость их не превышает 250 км/ч). Для беспроводного интерфейса HPI (Highspeed Portable Internet) устанавливаются уровни скорости передачи и безопасности. Быстродействие HPI выше, чем универсальной системы мобильной связи UMTS, которая ориентирована на передачу голоса. Стандарт обеспечивает подключение ПК в небольших и домашних офисах (SOHO) как альтернативу сетей «последней мили» по медным или оптическим кабелям, использующим технологии DSL.

Стандарт IEEE 802.21 – это стандарт независимой от среды эстафетной передачи соединений – MIHS (*Media Independent Handover Services*).

Стандарт IEEE 802.22 определяет функционирование беспроводных региональных сетей WRAN (*Wireless Regional Area Network*), использующих для передачи данных телевизионные частотные диапазоны.

4.2. Протоколы и стеки протоколов

Согласованный набор протоколов разных уровней, достаточный для организации межсетевого взаимодействия, называется **стеком протоколов**.

Для каждого уровня определяется набор функций-запросов для взаимодействия с вышележащим уровнем, который называется **интерфейсом**.

Правила взаимодействия двух машин могут быть описаны в виде набора процедур для каждого из уровней, которые называются **протоколами**.

Существует достаточно много стеков протоколов, широко применяемых в сетях. Это и стеки, являющиеся международными и национальными стандартами, и фирменные стеки, получившие распространение благодаря распространенности оборудования той или иной фирмы. Примерами популярных стеков протоколов могут служить стек IPX/SPX фирмы Novell, стек TCP/IP, используемый в сети Internet и во многих сетях на основе операционной системы UNIX, стек OSI международной организации по стандартизации, стек DECnet корпорации Digital Equipment и некоторые другие.

Стеки протоколов разбиваются на три уровня:

– сетевые;
– транспортные;
– прикладные.

4.2.1. Протоколы сетевого уровня

Сетевые протоколы предоставляют следующие услуги: адресацию и маршрутизацию информации, проверку на наличие ошибок, запрос повторной передачи и установление правил взаимодействия в конкретной сетевой среде. Ниже приведены наиболее популярные сетевые протоколы:

– DDP (Datagram Delivery Protocol – протокол доставки дейтаграмм). *Протокол передачи данных Apple*, используемый в Apple Talk;

– IP (Internet Protocol – протокол Internet). *Протокол стека TCP/IP*, обеспечивающий адресную информацию и информацию о маршрутизации;

– IPX (Internetwork Packet eXchange – межсетевой обмен пакетами) в NWLink. *Протокол Novel NetWare*, используемый для маршрутизации и направления пакетов;

– NetBEUI (NetBIOS Extended User Interface – расширенный пользовательский интерфейс базовой сетевой системы ввода/вывода). Разработан совместно IBM и Microsoft, обеспечивает транспортные услуги для NetBIOS.

4.2.2. Протоколы транспортного уровня

Транспортные протоколы предоставляют услуги надежной транспортировки данных между компьютерами. Ниже приведены наиболее популярные транспортные протоколы:

– ATP (Apple Talk Protocol – транзакционный протокол Apple Talk) и NBP (Name Binding Protocol – *протокол связывания имен*). Сеансовый и транспортный протоколы Apple Talk;

– NetBIOS (Network Basis Input/Output System – *базовая сетевая система ввода/вывода*). NetBIOS устанавливает соединение между компьютерами, а NetBEUI предоставляет услуги передачи данных для этого соединения;

– SPX (Sequenced Packet eXchange – последовательный обмен пакетами) в NWLink. Протокол Novel NetWare, используемый для обеспечения доставки данных;

– TCP (Transmission Control Protocol – протокол управления передачей). Протокол стека TCP/IP отвечает за надежную доставку данных.

4.2.3. Протоколы прикладного уровня

Прикладные протоколы отвечают за взаимодействие приложений. Ниже приведены наиболее популярные прикладные протоколы:

– AFP (Apple Talk File Protocol – файловый протокол Apple Talk). *Протокол удаленного управления файлами Macintosh*;

– FTP (File Transfer Protocol – протокол передачи файлов). *Протокол стека TCP/IP*, используемый для обеспечения услуг по передаче файлов;

– NCP (NetWare Core Protocol – *базовый протокол NetWare*). Оболочка и редиректоры клиента Novel NetWare;

– SNMP (Simple Network Management Protocol – *простой протокол управления сетью*). Протокол стека TCP/IP, используемый для управления и наблюдения за сетевыми устройствами;

– HTTP (Hyper Text Transfer Protocol) – протокол *передачи гипертекста*.

4.3. Стек OSI

Следует различать стек протоколов OSI и модель OSI (*рис. 4.1*). **Стек OSI** – это набор вполне конкретных спецификаций протоко-

лов, образующих согласованный стек протоколов. Этот стек протоколов поддерживает правительство США в своей программе GOSIP. Стек OSI, в отличие от других стандартных стеков, полностью соответствует модели взаимодействия OSI и включает спецификации для всех семи уровней модели взаимодействия открытых систем.

Рис. 4.1. Стек OSI

На физическом и канальном уровнях стек OSI поддерживает спецификации Ethernet, Token Ring, FDDI, а также протоколы LLC, X.25 и ISDN.

На сетевом уровне реализованы протоколы как без установления соединений, так и с установлением соединений. Транспортный протокол стека OSI скрывает различия между сетевыми сервисами с установлением соединения и без установления соединения, так что пользователи получают нужное качество обслуживания независимо от нижележащего сетевого уровня. Для обеспечения этого транспортный уровень требует, чтобы пользователь задал нужное качество обслуживания. Определено 5 классов транспортного сервиса: от низшего класса 0 до высшего класса 4, которые отличаются степенью устойчивости к *ошибкам* и требованиями к восстановлению данных после ошибок.

Сервисы прикладного уровня включают передачу файлов, эмуляцию терминала, службу каталогов и почту. Из них наиболее перспективными являются служба каталогов (стандарт X.500), электронная почта (X.400), протокол виртуального терминала (VT), протокол передачи, доступа и управления файлами (FTAM), протокол пересылки и управления работами (JTM). В последнее время ISO сконцентрировала свои усилия именно на сервисах верхнего уровня.

4.4. Архитектура стека протоколов TCP/IP

Набор многоуровневых протоколов, или, как называют, **стек TCP/IP**, предназначен для использования в различных вариантах сетевого окружения.

Стек TCP/IP с точки зрения системной архитектуры соответствует эталонной модели OSI (Open Systems Interconnection – взаимодействие открытых систем) и позволяет обмениваться данными по сети приложениям и службам, работающим практически на любой платформе, включая Unix, Windows, Macintosh и другие.

Стандартная реализация TCP/IP (например, фирмы Microsoft) соответствует четырехуровневой модели вместо семиуровневой модели, как показано на *рис. 4.2*.

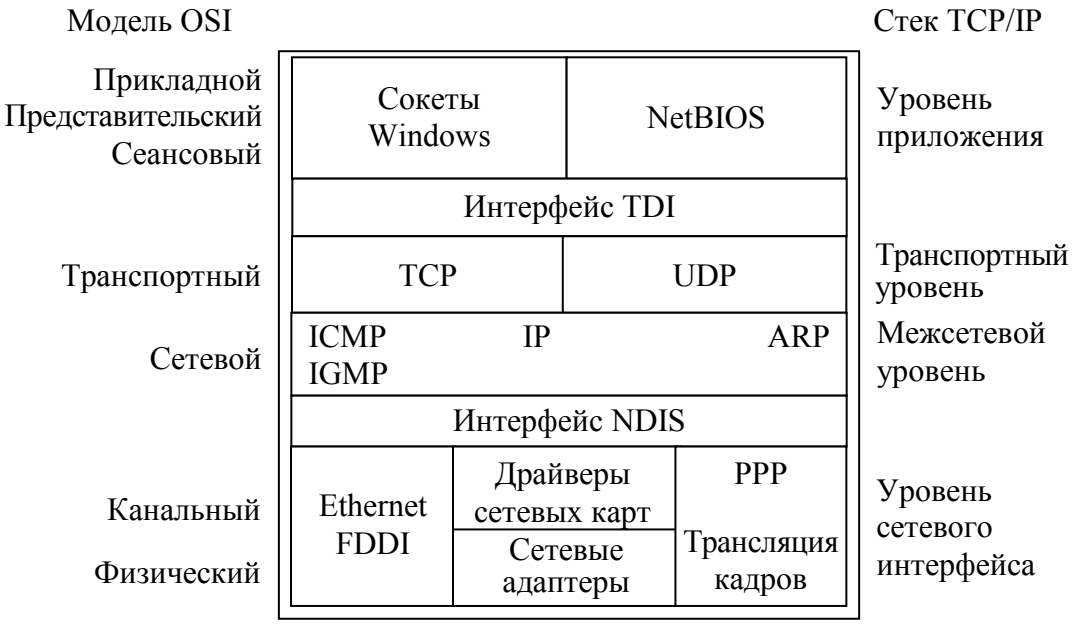


Рис. 4.2. Соответствие семиуровневой модели OSI и четырехуровневой модели TCP/IP

Модель TCP/IP включает большее число функций на один уровень, что приводит к уменьшению числа уровней. В модели используются следующие уровни:

– уровень *Приложения* модели TCP/IP соответствует *Прикладному*, *Представительскому* и *Сеансовому* уровням модели OSI;

– *Транспортный уровень* модели TCP/IP соответствует аналогичному уровню модели OSI;

– *Межсетевой* уровень модели TCP/IP выполняет те же функции, что и *Сетевой уровень* модели OSI;

– уровень С*етевого интерфейса* модели TCP/IP соответствует *Канальному* и *Физическому* уровням модели OSI.

4.4.1. Уровень Приложения

Через уровень *Приложения* модели TCP/IP приложения и службы получают доступ к сети. Доступ к протоколам TCP/IP осуществляется посредством двух программных интерфейсов API: сокеты Windows и NetBIOS.

Интерфейс сокетов Windows, или, как его называют, *WinSock*, является сетевым программным интерфейсом, предназначенным для облегчения взаимодействия между различными TCP/IP – приложениями и семействами протоколов.

Интерфейс NetBIOS используется для связи между процессами (IPC – Interposes Communications) служб и приложений ОС Windows. NetBIOS выполняет три основных функции:

– определение имен NetBIOS;

– служба дейтаграмм NetBIOS;

– служба сеанса NetBIOS.

В *табл. 4.1* приведено семейство протоколов TCP/IP.

Таблица 4.1

Назначение протоколов TCP/IP

Название протокола	Описание протокола
WinSock	Сетевой программный интерфейс
NetBIOS	Связь с приложениями ОС Windows
TDI	Интерфейс транспортного драйвера (Transport Driver Interface); позволяет создавать компоненты сеансового уровня
TCP	Протокол управления передачей (Transmission Control Protocol)
UDP	Протокол пользовательских дейтаграмм (User Datagram Protocol)

Окончание табл. 4.1

Название протокола	Описание протокола
ARP	Протокол разрешения адресов (Address Resolution Protocol)
RARP	Протокол обратного разрешения адресов (Reverse Address Resolution Protocol)
IP	Протокол Internet (Internet Protocol)
ICMP	Протокол управляющих сообщений Internet (Internet Control Message Protocol)
IGMP	Протокол управления группами Интернета (Internet Group Management Protocol)
NDIS	Интерфейс взаимодействия между драйверами транспортных протоколов
FTP	Протокол пересылки файлов (File Transfer Protocol)
TFTP	Простой протокол пересылки файлов (Trivial File Transfer Protocol)

4.4.2. Транспортный уровень

Транспортный уровень TCP/IP отвечает за установление и поддержание соединения между двумя узлами. Основные функции уровня:

- подтверждение получения информации;
- управление потоком данных;
- упорядочение и ретрансляция пакетов.

В зависимости от типа службы могут быть использованы два протокола:

– TCP (Transmission Control Protocol – *протокол управления передачей*);

– UDP (User Datagram Protocol – *пользовательский протокол дейтаграмм*).

TCP обычно используют в тех случаях, когда приложению требуется передать большой объем информации и убедиться, что данные своевременно получены адресатом. Приложения и службы, отправляющие небольшие объемы данных и не нуждающиеся в получении подтверждения, используют протокол UDP, который является протоколом без установления соединения.

Протокол управления передачей TCP отвечает за надежную передачу данных от одного узла сети к другому. Он создает сеанс с установлением соединения, иначе говоря, виртуальный канал между машинами. Установление соединения происходит в три шага.

1. Клиент, запрашивающий соединение, отправляет серверу пакет, указывающий номер порта, который клиент желает использовать, а также код (определенное число) ISN (Initial Sequence number).

2. Сервер отвечает пакетом, содержащим ISN сервера, а также ISN клиента, увеличенный на 1.

3. Клиент должен подтвердить установление соединения, вернув ISN сервера, увеличенный на 1.

Трехступенчатое открытие соединения устанавливает номер порта, а также ISN клиента и сервера. Каждый отправляемый TCP-пакет содержит номера TCP-портов отправителя и получателя, номер фрагмента для сообщений, разбитых на меньшие части, а также контрольную сумму, позволяющую убедиться, что при передаче не произошло ошибок.

В отличие от TCP **пользовательский протокол дейтаграмм UDP** не устанавливает соединения. Протокол UDP предназначен для отправки небольших объемов данных без установки соединения и используется приложениями, которые не нуждаются в подтверждении адресатом их получения. UDP также использует номера портов для определения конкретного процесса по указанному IP-адресу. Однако UDP-порты отличаются от TCP-портов и, следовательно, могут использовать те же номера портов, что и TCP, без конфликта между службами.

4.4.3. Межсетевой уровень

Межсетевой уровень отвечает за маршрутизацию данных внутри сети и между различными сетями. На этом уровне работают маршрутизаторы, которые зависят от используемого протокола и используются для отправки пакетов из одной сети (или ее сегмента) в другую (или другой сегмент сети). В стеке TCP/IP на этом уровне используется протокол IP.

Протокол Интернета IP обеспечивает обмен дейтаграммами между узлами сети и является протоколом, не устанавливающим соединения и использующим дейтаграммы для отправки данных из одной сети в другую. Данный протокол не ожидает получение подтверждения (ASK, Acknowledgment) отправленных пакетов от узла адресата. Подтверждения, а также повторные отправки пакетов осуществляются протоколами и процессами, работающими на верхних уровнях модели.

К функциям протокола относится фрагментация дейтаграмм и межсетевая адресация. Протокол IP предоставляет управляющую информацию для сборки фрагментированных дейтаграмм. Главной функцией протокола является межсетевая и глобальная адресация. В зависимости от размера сети, по которой будет маршрутизироваться дейтаграмма или пакет, применяется одна из трех схем адресации.

Протокол IP действует на сетевом уровне модели OSI, поэтому *IP-адреса называются сетевыми*. Они предназначены для передачи сообщений в составных сетях, связывающих подсети, построенные на различных локальных или глобальных сетевых технологиях, например, Ethernet или ATM. Однако для непосредственной передачи сообщения в рамках одной подсети вместо IP-адреса нужно использовать локальный (аппаратный) адрес технологии канального уровня, чаще всего MAC-адрес. При этом к IP-пакету добавляются заголовок и концевик кадра канального уровня, в заголовке указываются MAC-адреса источника и приемника кадра (*рис. 4.3*).

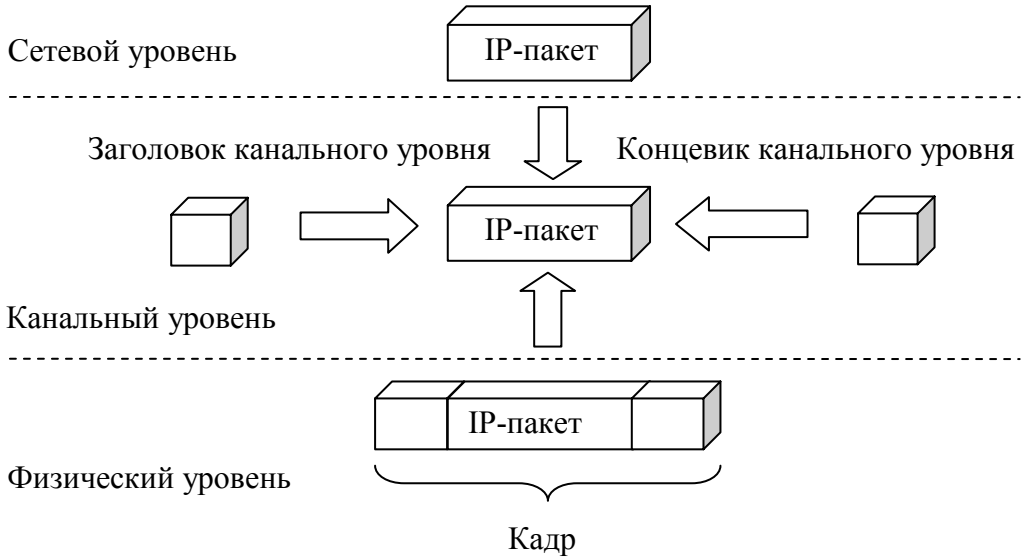


Рис. 4.3. Формирование кадра на канальном уровне

При формировании кадра канального уровня возникает проблема: каким образом по известному IP-адресу определить соответствующий MAC-адрес. Указанная проблема решается при помощи протокола ARP (Address Resolution Protocol – протокол разрешения адресов).

Протокол сопоставления адреса ARP определяет MAC-адреса следующим образом. Осуществляется рассылка всем узлам сети специального кадра, который называется **ARP-запрос** (***ARP Request***).

В кадре содержится IP-адрес компьютера, у которого требуется узнать MAC-адрес. Каждый узел сети принимает ARP-запрос и сравнивает IP-адрес из запроса со своим IP-адресом. Если адреса совпадают, узел высылает **ARP-ответ** (***ARP Reply***), содержащий требуемый MAC-адрес.

Результаты своей работы протокол ARP сохраняет в специальной таблице, хранящейся в *оперативной памяти*, которая называется **ARP-кэш**. При необходимости разрешения IP-адреса, протокол ARP сначала ищет IP-адрес в ARP-кэше и только в случае отсутствия нужной записи производит рассылку ARP-запроса.

Записи в ARP-кэше могут быть двух типов: статические и динамические. Статические записи заносятся в кэш администратором при помощи утилиты arp с ключом /s. Динамические записи помещаются в кэш после полученного ARP-ответа и по истечении двух минут удаляются.

ARP-кэш имеет структуру, представленную в *табл. 4.2*.

Таблица 4.2

Внешний вид таблицы ARP-кэш

IP-адрес	MAC-адрес	Тип записи
192.168.1.1	03-E8-48-A1-57-7B	статический
192.168.1.2	03-E8-48-A1-43-88	динамический
192.168.1.3	03-E8-48-A1-F8-D9	динамический

Процесс получения по известному IP-адресу MAC-адреса называется **разрешением IP-адреса**.

Удаление происходит для того, чтобы при перемещении в другую подсеть компьютера с MAC-адресом, занесенным в таблицу, кадры не отправлялись бесполезно в сеть.

Иногда требуется по известному MAC-адресу найти IP-адрес (например, при начале работы компьютеров без жесткого диска, у которых есть MAC-адрес сетевого адаптера и им нужно определить свой IP-адрес). В этом случае используется реверсивный протокол RARP (Reverse ARP).

Протокол управления сообщениями Интернета (Internet Control Message Protocol, ICMP) используется IP и другими протоколами высокого уровня для отправки и получения отчетов о состоянии переданной информации. Этот протокол используется для контроля скорости передачи информации между двумя системами. Если маршрутизатор, соединяющий две системы, перегружен трафиком, он может отправить специальное сообщение ICMP – ошибку для уменьшения скорости отправления сообщений.

Узлы локальной сети используют **протокол управления группами Интернета (Internet Group Management Protocol, IGMP)**, чтобы зарегистрировать себя в группе. Информация о группах содержится на маршрутизаторах локальной сети. Маршрутизаторы используют эту информацию для передачи групповых сообщений.

Групповое сообщение, как и широковещательное, используется для отправки данных сразу нескольким узлам.

NDIS (Network Device Interface Specification) – спецификация интерфейса сетевого устройства, программный интерфейс, обеспечивающий взаимодействие между драйверами транспортных протоколов и соответствующими драйверами сетевых интерфейсов. Позволяет использовать несколько протоколов, даже если установлена только одна сетевая карта.

4.4.4. Уровень сетевого интерфейса

Этот уровень модели TCP/IP отвечает за распределение IP-дейтаграмм. Он работает с ARP для определения информации, которая должна быть помещена в заголовок каждого кадра. Затем на этом уровне создается кадр, подходящий для используемого типа сети, такого как Ethernet, Token Ring или ATM, затем IP-дейтаграмма помещается в область данных этого кадра, и он отправляется в сеть.

ВЫВОДЫ

1. Стандарты семейства IEEE 802.X охватывают только два нижних уровня семиуровневой модели OSI – физический и канальный. Это связано с тем, что именно эти уровни в наибольшей

степени отражают специфику локальных сетей. Старшие же уровни, начиная с сетевого, в значительной степени имеют общие черты как для локальных, так и для глобальных сетей.

2. Согласованный набор протоколов разных уровней, достаточный для организации межсетевого взаимодействия, называется стеком протоколов. Для каждого уровня определяется набор функций-запросов для взаимодействия с вышележащим уровнем, который называется интерфейсом. Правила взаимодействия двух машин могут быть описаны в виде набора процедур для каждого из уровней, которые называются протоколами.

3. Наибольшее распространение для построения составных сетей в последнее время получил стек TCP/IP, характеризующийся 4 уровнями: прикладной, основной, уровень межсетевого взаимодействия и уровень сетевых интерфейсов. Необходимо отметить, что хоть стек TCP/IP в общем и соответсвует модели OSI, соответствие уровней стека TCP/IP уровням модели OSI достаточно условно.

4. Прикладной уровень объединяет все службы, предоставляемые системой пользовательским приложениям: традиционные сетевые службы типа Telnet, FTP, TFTP, DNS, SNMP, а также сравнительно новые, такие, например, как протокол передачи гипертекстовой информации HTTP.

5. На основном уровне стека TCP/IP, называемом также транспортным, функционируют протоколы TCP и UDP. Протокол управления передачей TCP решает задачу обеспечения надежной информационной связи между двумя конечными узлами. Дейтаграммный протокол UDP используется как экономичное средство связи уровня межсетевого взаимодействия с прикладным уровнем.

6. Уровень межсетевого взаимодействия реализует концепцию коммутации пакетов в режиме без установления соединений. Основными протоколами этого уровня являются дейтаграммный протокол IP и протоколы маршрутизации (RIP, OSPF, BGP и др.). Вспомогательную роль выполняет протокол межсетевых управляющих сообщений ICMP, протокол группового управления IGMP и протокол разрешения адресов ARP.

7. Протоколы уровня сетевых интерфейсов обеспечивают интеграцию в составную сеть других сетей. Этот уровень не регламентируется, но поддерживает все популярные стандарты физического и канального уровней: для локальных сетей – Ethernet,

Token Ring, FDDI и т. д., для глобальных сетей – X.25, Frame relay, PPP, ISDN и т. д.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Назначение спецификации стандартов IEEE 802.
2. Какой стандарт описывает сетевую технологию Ethernet?
3. Какой стандарт определяет задачи управления логической связью?
4. Какой стандарт задает механизмы управления сетью?
5. Какой стандарт описывает сетевую технологию ArcNet?
6. Какой стандарт описывает сетевую технологию Token Ring?
7. Какой стандарт содержит рекомендации по оптоволоконным сетевым технологиям?
8. Что такое интерфейс уровня базовой модели OSI?
9. Что такое протокол уровня базовой модели OSI?
10. Дайте определение стека протоколов.
11. На какие уровни разбиваются стеки протоколов?
12. Назовите наиболее популярные сетевые протоколы.
13. Назовите наиболее популярные транспортные протоколы.
14. Назовите наиболее популярные прикладные протоколы.
15. Перечислите наиболее популярные стеки протоколов.
16. Назначение программных интерфейсов сокетов Windows и NetBIOS.
17. Чем отличается протокол TCP от UDP?
18. Функции протокола IP.
19. Какие существуют виды адресации в IP-сетях?
20. Какой протокол используется для определения локального адреса по IP-адресу?
21. Какой протокол используется для определения IP-адреса по локальному адресу?
22. Какой протокол используется для управления сообщениями Интернета?
23. Назначение уровня сетевого интерфейса стека TCP/IP.

5. АДРЕСАЦИЯ И МАРШРУТИЗАЦИЯ В IP-СЕТЯХ

Каждый компьютер в сетях TCP/IP имеет адреса трех уровней: физический (MAC-адрес), сетевой (IP-адрес) и символьный (DNS-имя).

5.1. Физический адрес

Физический, или **локальный**, **адрес узла** определяется технологией, с помощью которой построена сеть, в которую входит узел. Для узлов, входящих в локальные сети, это MAC-адрес сетевого адаптера или порта маршрутизатора.

В качестве стандартного выбран 48-битный формат адреса, что соответствует примерно 280 триллионам различных адресов. Понятно, что столько сетевых адаптеров никогда не будет выпущено.

С тем чтобы распределить возможные диапазоны адресов между многочисленными изготовителями сетевых адаптеров, была предложена следующая структура адреса (*рис. 5.1*).

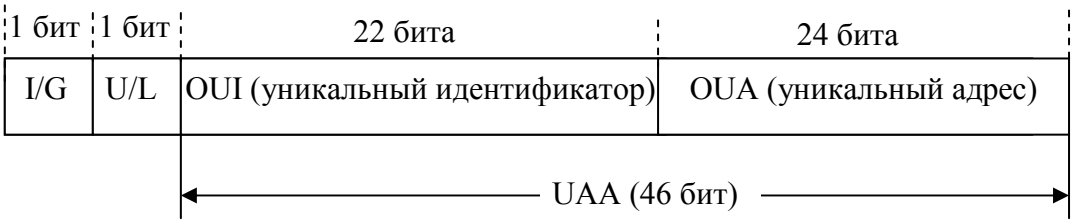


Рис. 5.1. Структура 48-битного стандартного MAC-адреса

Младшие 24 разряда кода адреса называются OUA (Organizationally Unique Address) – ***уникальный адрес***. Именно их присваивает каждый из зарегистрированных производителей сетевых адаптеров. Всего возможно свыше 16 миллионов комбинаций, это значит, что каждый изготовитель может выпустить 16 миллионов сетевых адаптеров. Следующие 22 разряда кода называются OUI (Organizationally Unique Identifier) – ***уникальный идентификатор***. IEEE присваивает один или несколько OUI каждому производителю сетевых адаптеров. Это позволяет исключить совпадения

адресов адаптеров от разных производителей. Всего возможно свыше 4 миллионов разных OUI, это означает, что теоретически может быть зарегистрировано 4 миллиона производителей. Вместе OUA и OUI называются UAA (Universally Administered Address) – универсально управляемый адрес, или IEEE-адрес.

Два старших разряда адреса управляющие, они определяют тип адреса, способ интерпретации остальных 46 разрядов. Старший бит I/G (Individual/Group) указывает на тип адреса. Если он установлен в 0, то индивидуальный, если в 1, то групповой (многопунктовый или функциональный). Пакеты с групповым адресом получат все имеющие этот групповой адрес сетевые адаптеры. Причем групповой адрес определяется 46 младшими разрядами. Второй управляющий бит U/L (Universal/ Local) называется флажком универсального/местного управления и определяет, как был присвоен адрес данному сетевому адаптеру. Обычно он установлен в 0. Установка бита U/L в 1 означает, что адрес задан не производителем сетевого адаптера, а организацией, использующей данную сеть. Это случается довольно редко.

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

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

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

5.2. Сетевой адрес

5.2.1. Представление IP-адреса

IP-адрес представляет собой 32-разрядное двоичное число, разделенное на группы по 8 бит, называемые **октетами**. Например, 00010001.11101111.00101111.01011110.

Обычно IP-адреса записываются в виде четырех десятичных октетов и разделяются точками. Таким образом, приведенный выше IP-адрес можно записать в следующей форме: 17.239.47.94.

Следует заметить, что максимальное значение октета равно 11111111_2 (двоичная система счисления), что соответствует в десятичной системе 255_{10}. Поэтому IP-адреса, в которых хотя бы один октет превышает это число, являются недействительными. Пример: 172.16.123.1 – действительный адрес, а 172.16.123.256 – несуществующий адрес, поскольку 256 выходит за пределы допустимого диапазона: от 0 до 255.

IP-адрес состоит из двух логических частей – **номера подсети** (ID подсети) и **номера узла** (ID хоста) в этой подсети. При передаче пакета из одной подсети в другую используется ID подсети. Когда пакет попал в подсеть назначения, ID хоста указывает на конкретный узел в рамках этой подсети.

Чтобы записать ID подсети, в поле номера узла в IP-адресе ставят нули. Чтобы записать ID хоста, в поле номера подсети ставят нули. Например, если в IP-адресе 172.16.123.1 первые два байта отводятся под номер подсети, остальные два байта – под номер узла, то номера записываются следующим образом: ID подсети 172.16.0.0; ID хоста 0.0.123.1.

По числу разрядов, отводимых для представления номера узла (или номера подсети), можно определить общее количество узлов (или подсетей) по простому правилу: если число разрядов для представления номера узла равно N, то общее количество узлов равно $2^N - 2$. Два узла вычитаются вследствие того, что адреса со всеми разрядами, равными нулям или единицам, являются особыми и используются в специальных целях.

Например, если под номер узла в некоторой подсети отводится два байта (16 бит), то общее количество узлов в такой подсети равно $2^{16} - 2 = 65534$ узла.

Для определения того, какая часть IP-адреса отвечает за ID подсети, а какая за ID хоста, применяются два способа: с помощью классов и с помощью масок.

***Общее правило**:* под ID подсети отводятся *первые* несколько бит IP-адреса, оставшиеся биты обозначают ID хоста.

Рассмотрим конфигурирование IP-адресации (v4) в операционных системах типа *Windows*.

Пример 1. Рассмотрим настройку протокола TCP/IP v4.

1. Запустите папку *Сетевые подключения*. Для этого в операционных системах типа Windows Seven необходимо нажать кнопку *Пуск*, ввести в строке поиска начальные буквы слова *Центр*. Из списка выберите пункт *Центр управления сетями и общим доступом* (*рис. 5.2*).

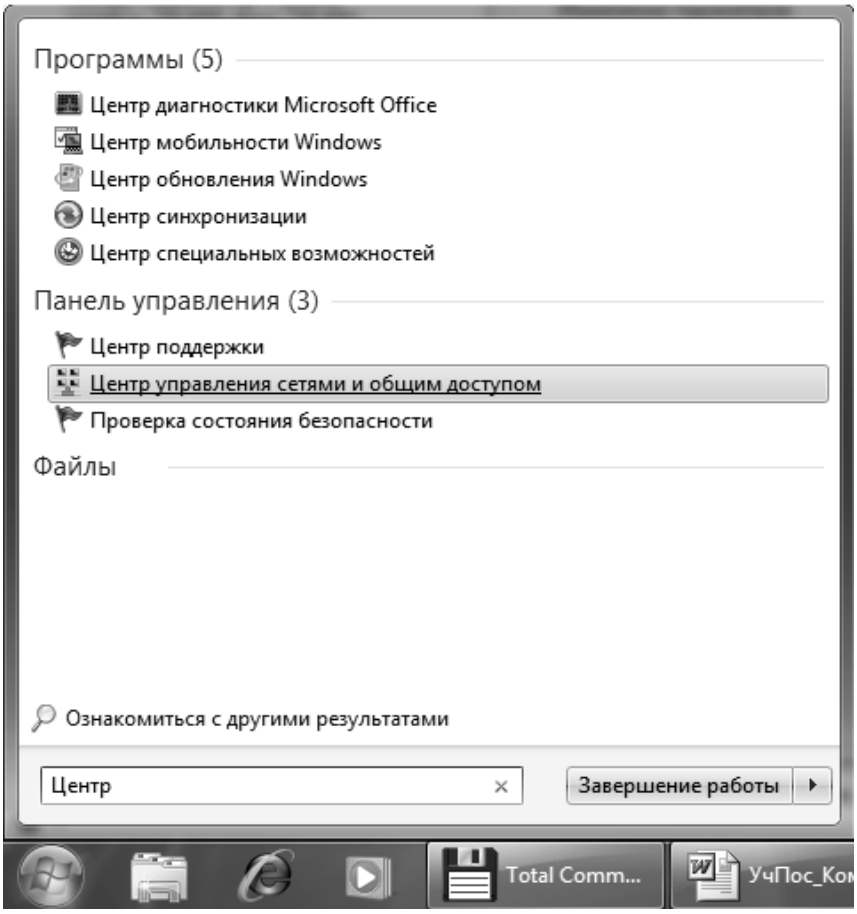


Рис. 5.2. Пример вызова
Центра управления сетями и общим доступом

2. В окне *Центра управления сетями и общим доступом* щелкните по *Изменению параметров адаптера* (*рис. 5.3*). Далее откроется окно сетевых подключений (*рис. 5.4*).

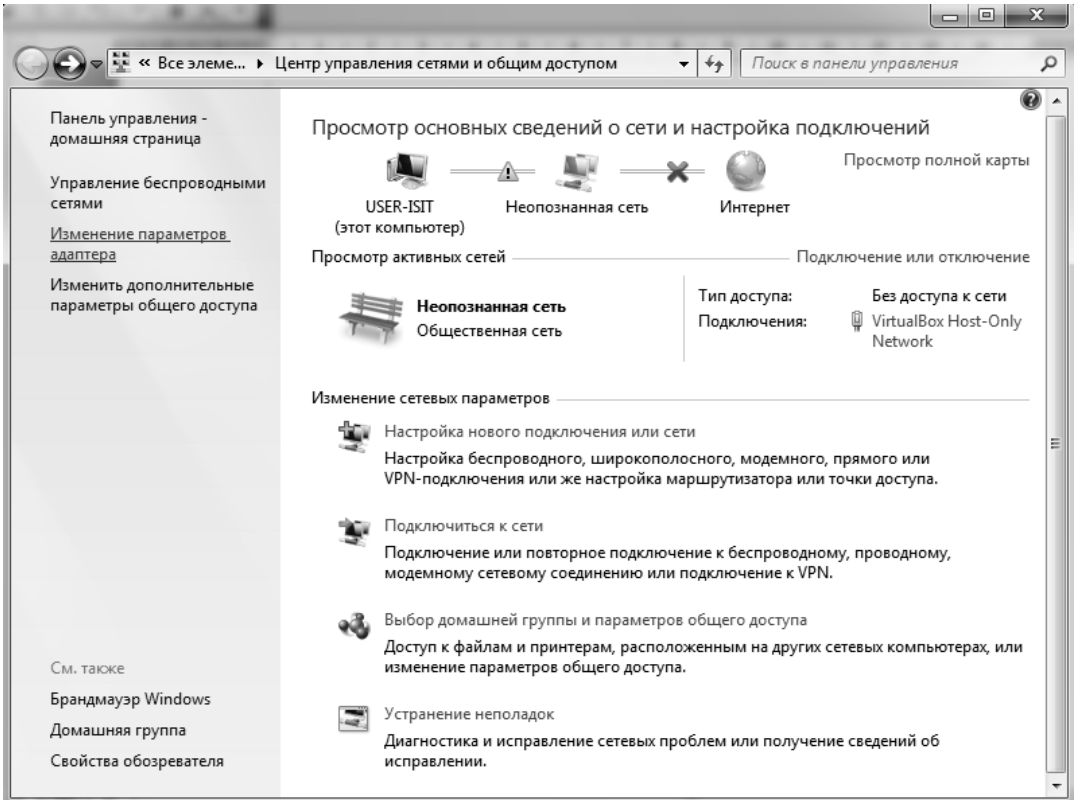


Рис. 5.3. Общий вид Центра управления сетями и общим доступом

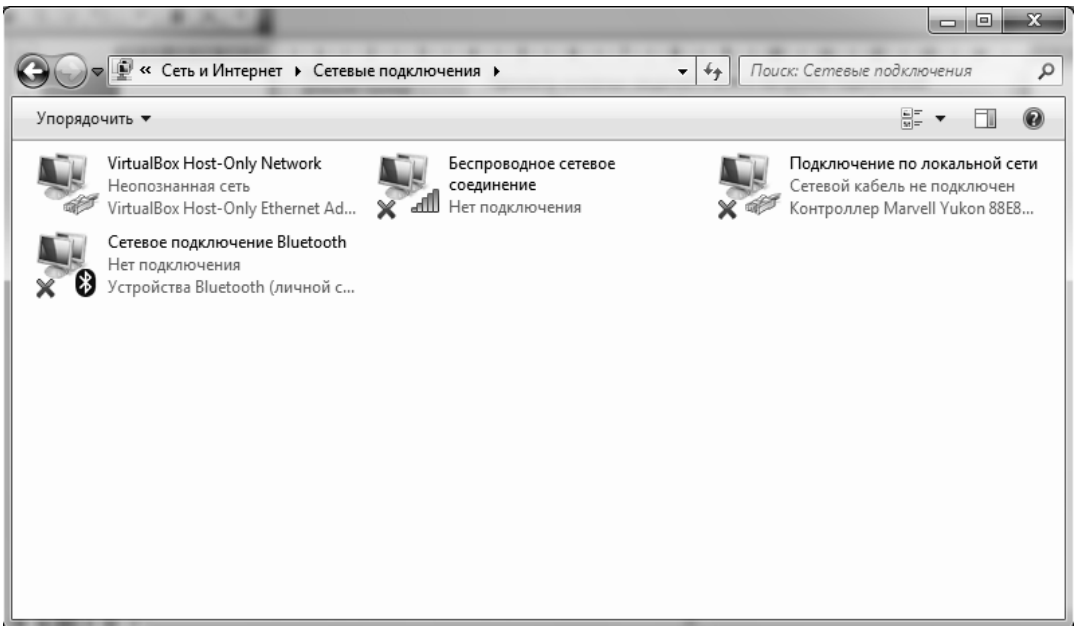


Рис. 5.4. Общий вид папки Сетевые подключения

3. Щелкните правой кнопкой мыши по подключению, которое требуется настроить, а затем выберите команду *Свойства*.

Если появится диалоговое окно *Управление учетной записью пользователя*, убедитесь, что действие, указанное в окне, совпадает с тем, которое вы хотите выполнить, и нажмите *Продолжить*.

4. Далее выполните одно из указанных ниже действий:

– в случае подключения по локальной сети на вкладке *Общие* в списке *Компоненты*, используемые этим подключением, выберите пункт *Протокол Интернета версии 4 (TCP/IPv4)* и нажмите кнопку *Свойства*;

– в случае подключения удаленного доступа, VPN-подключения или высокоскоростного подключения на вкладке *Сеть* в списке *Компоненты*, используемые этим подключением, выберите пункт *Протокол Интернета версии 4 (TCP/IPv4)* и нажмите кнопку *Свойства*. В результате откроется окно с настройками протокола TCP/IP (*рис. 5.5*).

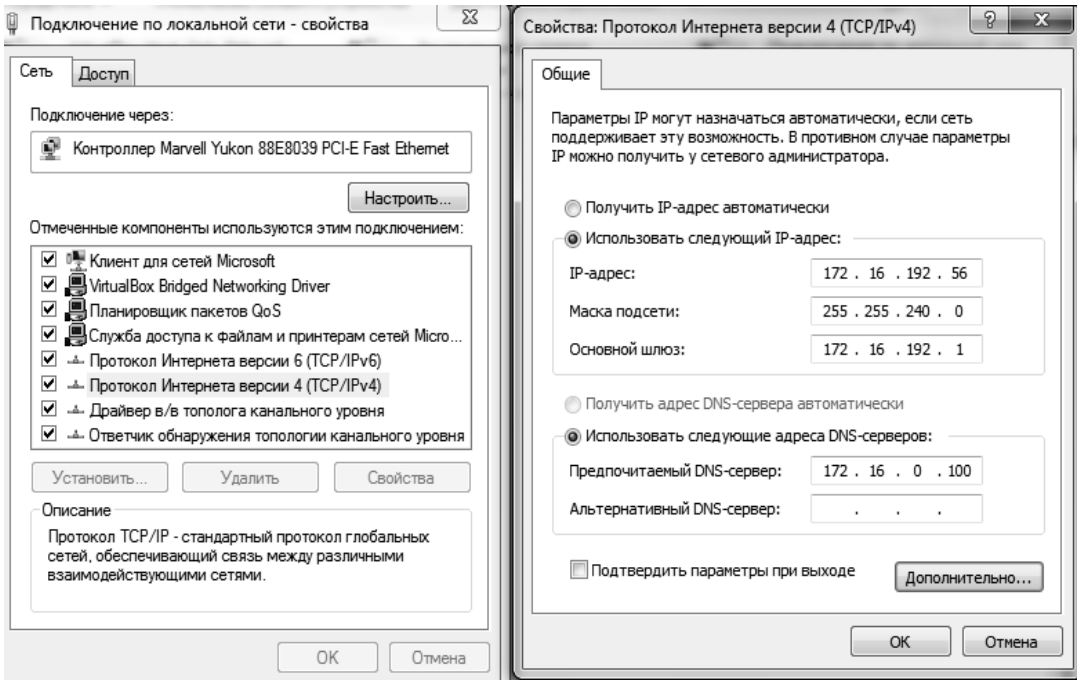


Рис. 5.5. Свойства Протокола Интернета версии 4 (TCP/IPv4)

5. Выполните далее одно из указанных ниже действий:

– если необходимо, чтобы параметры IP-адреса назначались автоматически, выберите пункт *Получить IP-адрес автоматически* и нажмите кнопку *ОК*;

– если необходимо указать IP-адрес IPv4 или адрес DNS-сервера, выполните следующие действия:

a) выберите пункт *Использовать следующий IP-адрес* и в поле *IP-адрес* введите IP-адрес, соответствующую маску подсети и адрес шлюза по умолчанию (в примере на *рис. 5.5* IP адрес: 172.16.192.56; маска подсети: 255.255.240.0; основной шлюз: 172.16.192.1);

b) выберите пункт *Использовать следующие адреса DNS-серверов* и в полях *Предпочитаемый DNS-сервер* и *Альтернативный DNS-сервер* введите адреса основного и дополнительного DNS-сервера (в примере на *рис. 5.5* IP-адрес предпочитаемого DNS-сервера: 172.16.0.100);

c) для настройки параметров DNS, WINS и IP нажмите кнопку *Дополнительно* (*рис. 5.6*).

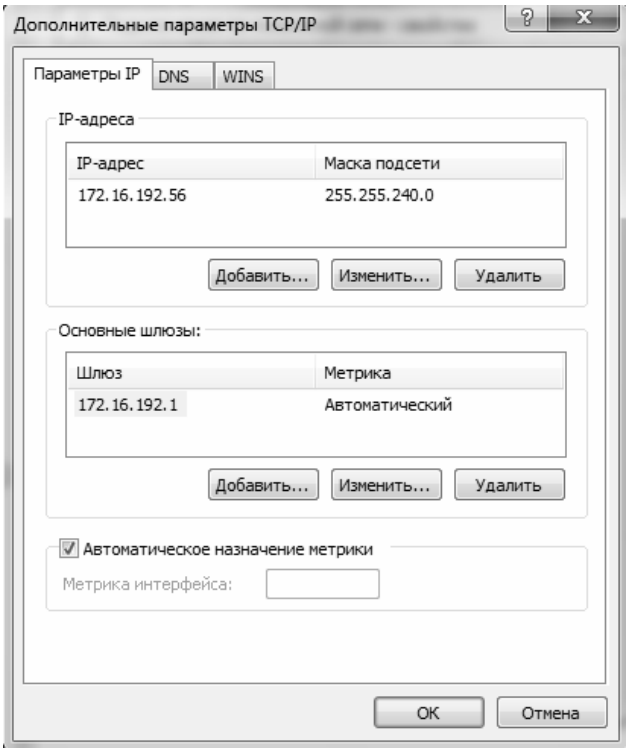


Рис. 5.6. Окно с дополнительными параметрами TCP/IP

6. В подключении по локальной сети при выборе параметра *Получить IP-адрес* автоматически включается вкладка *Альтернативная конфигурация*. Если компьютер используется более чем в одной сети, используйте эту вкладку для ввода альтернативных параметров IP-адреса. Для настройки параметров DNS, WINS и IP откройте вкладку *Настраиваемый пользователем* или *Альтернативная конфигурация*.

Дополнительные рекомендации. Если это возможно, используйте автоматическую настройку параметров протокола IP (DHCP), поскольку при этом устраняется необходимость настройки таких параметров, как IP-адрес, адрес DNS-сервера и адрес WINS-сервера.

Параметры *Альтернативная конфигурация* определяют второй набор параметров протокола IP, который используется при недоступности DHCP-сервера. Это весьма полезно для пользователей портативных компьютеров, которые часто перемещаются между двумя различными сетевыми средами (например, между средой со службой DHCP и средой со статическими IP-адресами).

Отметим, что аналогично осуществляется конфигурирование TCP/IPv6 (используются свойства *Протокол Интернета версии 6* (TCP/IPv6)).

5.2.2. Классы IP-адресов

Существует пять классов IP-адресов: *A*, *B*, *C*, *D* и *E* (*рис. 5.7*).

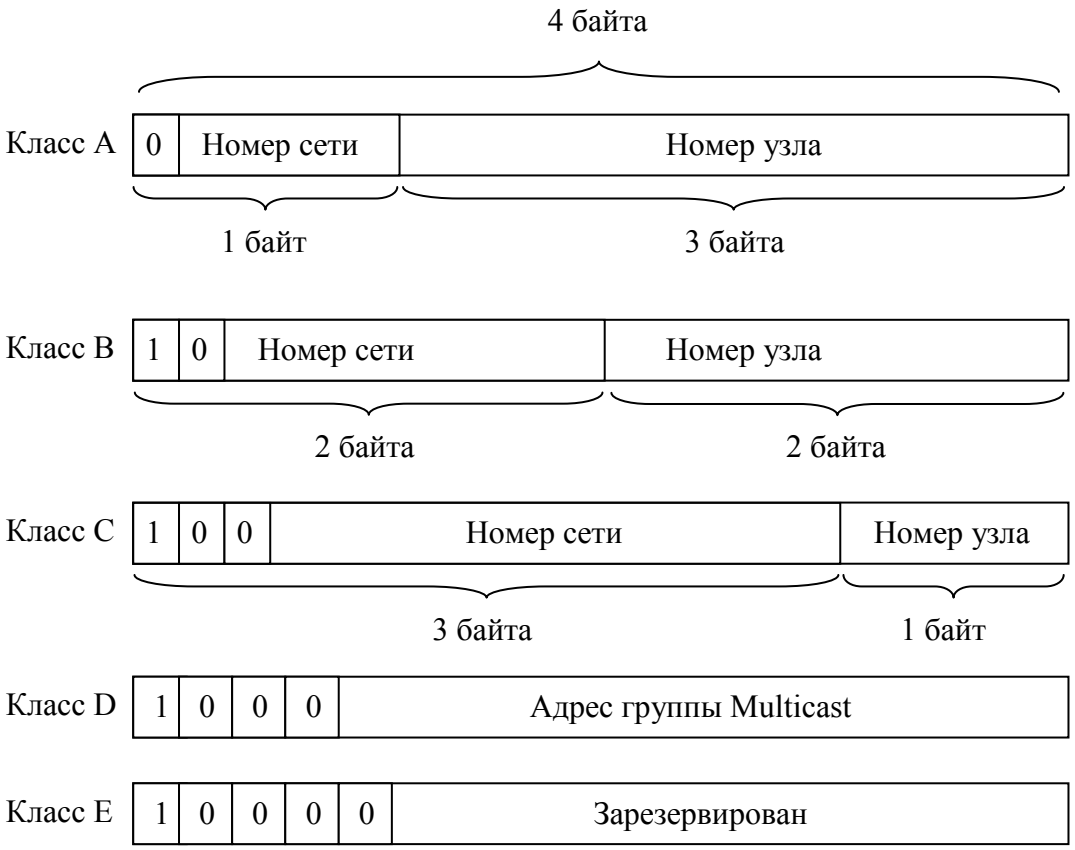


Рис. 5.7. Классы IP-адресов

За принадлежность к тому или иному классу отвечают первые биты IP-адреса. Деление сетей на классы описано в RFC 791 (документ описания протокола IP).

Целью такого деления являлось создание малого числа больших сетей (***класс A***), умеренного числа средних сетей (***класс B***) и большого числа малых сетей (***класс C***).

Если адрес начинается с 0, то сеть относят к *классу A* и номер сети занимает один байт, остальные 3 байта интерпретируются как номер узла в сети. Сети класса A имеют номера в диапазоне от 1 до 126. Сетей класса A немного, зато количество узлов в них может достигать $2^{24} – 2$, то есть 16 777 214 узлов.

Если первые два бита адреса равны 10, то сеть относится к *классу B*. В сетях класса B под номер сети и под номер узла отводится по 16 бит, то есть по 2 байта. Таким образом, сеть класса B является сетью средних размеров с максимальным числом узлов $2^{16} – 2$, что составляет 65 534 узлов.

Если адрес начинается с последовательности 110, то это сеть *класса C*. В этом случае под номер сети отводится 24 бита, а под номер узла – 8 бит. Сети этого класса наиболее распространены, число узлов в них ограничено $2^8 – 2$, то есть 254 узлами.

Адрес, начинающийся с 1110, обозначает особый, **групповой адрес** (multicast). Пакет с таким адресом направляется всем узлам, которым присвоен данный адрес.

Адреса *класса E* в настоящее время не используются (зарезервированы для будущих применений).

Характеристики адресов разных классов представлены в *табл. 5.1*.

Таблица 5.1

Характеристики IP-адресов разных классов

Класс	Первые биты	Наименьший номер сети	Наибольший номер сети	Количество сетей	Максимальное число узлов в сети
A	0	1.0.0.0	126.0.0.0	126	$2^{24} – 2 = 16777214$
B	10	128.0.0.0	191.255.0.0	16384	$2^{16} – 2 = 65534$
C	110	192.0.0.0	223.255.255.0	2097152	$2^8 – 2 = 254$
D	1110	224.0.0.0	239.255.255.255	Групповой адрес	
E	11110	240.0.0.0	247.255.255.255	Зарезервирован	

Применение классов удовлетворительно решало задачу деления на подсети в начале развития Интернета. В 90-е годы с увеличением числа подсетей стал ощущаться дефицит IP-адресов. Это связано с

неэффективностью распределения при классовой схеме адресации. Например, если организации требуется тысяча IP-адресов, ей выделяется сеть класса B, при этом 64 534 адреса не будут использоваться.

Существует два основных способа решения этой проблемы:

– более эффективная схема деления на подсети с использованием масок (RFC 950);

– применение протокола IP-версии 6 (IPv6).

5.2.3. Использование масок

Маска подсети (subnet mask) – это число, которое используется в паре с IP-адресом; двоичная запись маски содержит единицы в тех разрядах, которые должны в IP-адресе интерпретироваться как номер сети.

Для стандартных классов сетей маски имеют следующие значения:

– *класс A* – 11111111.00000000.00000000.00000000 (255.0.0.0);

– *класс B* – 11111111.11111111.00000000.00000000 (255.255.0.0);

– *класс C* – 11111111.11111111.11111111.00000000 (255.255.255.0).

Маска подсети записывается либо в виде, аналогичном записи IP-адреса, например, 255.255.255.0, либо совместно с IP-адресом с помощью указания числа единичных разрядов в записи маски, например, 192.168.1.1/24, т. е. в маске содержится 24 единицы (255.255.255.0).

При использовании масок можно вообще отказаться от понятия классов.

Пример 2. Пусть задан IP-адрес 17.239.47.94, маска подсети 255.255.0.0 (другая форма записи: 17.239.47.94/16).

Требуется определить ID подсети и ID хоста в обеих схемах адресации.

1) *Адресация с использованием классов*. Двоичная запись IP-адреса имеет вид:

00010001.11101111.00101111.01011110.

Так как первый бит равен нулю, адрес относится к *классу A*. Следовательно, первый байт отвечает за ID подсети, остальные три байта – за ID хоста:

ID подсети: 17.0.0.0 ID хоста: 0.239.47.94.

2) *Адресация с использованием масок*. Запишем IP-адрес и маску подсети в двоичном виде:

IP-address: 17.239.47.94 = 00010001.11101111.00101111.01011110;
Subnet mask: 255.255.0.0 = 11111111.11111111.00000000.00000000.

Вспомнив определение маски подсети, можно интерпретировать номер подсети как те биты, которые в маске равны 1, т. е. первые два байта. Оставшаяся часть IP-адреса будет номером узла в данной подсети.

ID подсети: 17.239.0.0. ID хоста: 0.0.47.94.

Номер подсети можно получить другим способом, применив к IP-адресу и маске операцию логического умножения или *конъюнкции* (AND):

$$\begin{array}{ll} \text{AND} & 00010001.\ 11101111.\ 00101111.\ 01011110 \\ & \underline{11111111.\ 11111111.\ 00000000.\ 00000000}\ . \\ & 00010001.\ 11101111.\ 00000000.\ 00000000 \\ & \quad 17 \qquad 239 \qquad 0 \qquad 0 \end{array}$$

В масках количество единиц в последовательности, определяющей границу номера сети, не обязательно должно быть кратным 8.

Пример 3. Задан IP-адрес 192.168.89.16, маска подсети – 255.255.192.0 (другая форма записи: 192.168.89.16/18).

Требуется определить ID подсети и ID хоста. Воспользуемся операцией AND:

$$\begin{array}{lll} \text{IP-address: } 192.168.89.16 = & \text{AND} & 11000000.10101000.01011001.00010000 \\ \text{Subnet mask: } 255.255.0.0 = & & \underline{11111111.11111111.11000000.00000000}. \\ \text{subnet ID:} & & 11000000.10101000.01000000.00000000 \\ & & \quad 192 \qquad 168 \qquad 64 \qquad 0 \end{array}$$

Чтобы получить номер узла, нужно в битах, отвечающих за номер подсети, поставить нули:

Host ID: 00000000.00000000.00011001.00010000 = 0.0.25.16.

Ответ: ID подсети = 192.168.64.0 ID хоста = 0.0.25.16.

Для масок существует важное правило: разрывы в последовательности единиц или нулей недопустимы.

Например, не существует маски подсети, имеющей следующий вид:

11111111.11110111.00000000.00001000 (255.247.0.8),

так как последовательности единиц и нулей не являются непрерывными.

С помощью масок администратор может структурировать свою сеть, не требуя от поставщика услуг дополнительных номеров сетей.

Пример 4. Допустим, организации выделена сеть класса B: 160.95.0.0 (*рис. 5.8*).

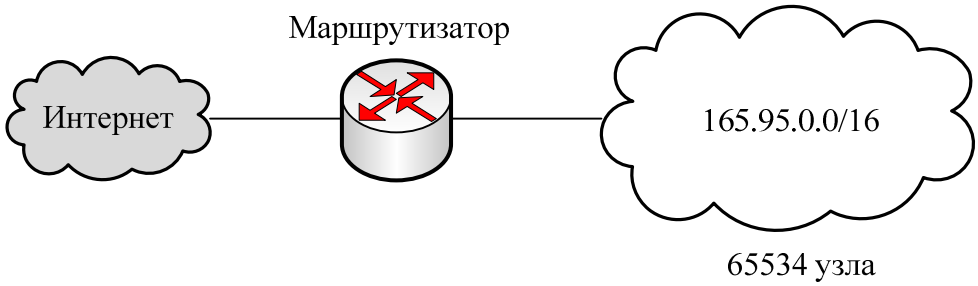


Рис. 5.8. Сеть класса B до деления на подсети

В такой сети может находиться до 65 534 узлов. Однако организации требуется 3 независимые сети с числом узлов в каждой не более 254. В этой ситуации можно применить деление на подсети с помощью масок. Например, при использовании маски 255.255.255.0 третий байт адреса будет определять номер внутренней подсети, а четвертый байт – номер узла (*рис. 5.9*).

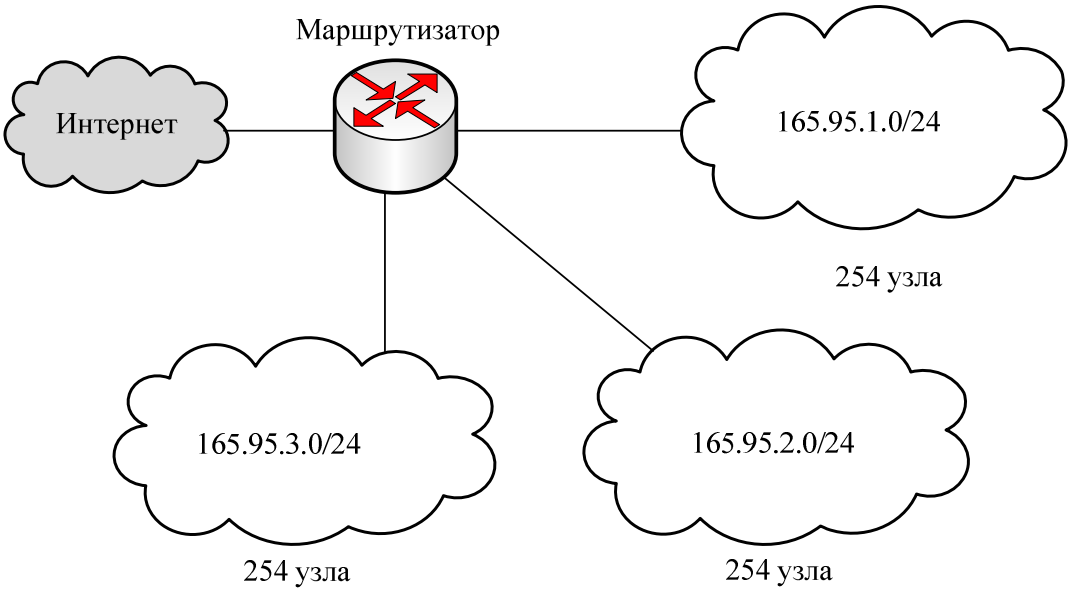


Рис. 5.9. Сеть класса B после деления на подсети

Маршрутизаторы во внешней сети (Интернет) ничего «не знают» о делении сети 160.95.0.0 на подсети, все пакеты направляются на маршрутизатор организации, который переправляет их в требуемую внутреннюю подсеть.

5.2.4. Протокол IPv6

Использование масок является временным решением проблемы дефицита IP-адресов, так как адресное пространство протокола IP не увеличивается, а количество хостов в Интернете растет с каждым днем. Для принципиального решения проблемы требуется существенное увеличение количества IP-адресов. Для преодоления ограничений IPv4 был разработан ***протокол IP 6-й версии*** – ***IPv6*** (RFC 2373, 2460).

Протокол IPv6 имеет следующие основные особенности:

– длина адреса 128 бит – такая длина обеспечивает примерно $3{,}4\times10^{38}$ адресов; такое количество адресов позволит присваивать в обозримом будущем уникальные IP-адреса любым устройствам;

– автоматическая конфигурация – протокол IPv6 предоставляет средства автоматической настройки IP-адреса и других сетевых параметров даже при отсутствии таких служб, как DHCP;

– встроенная безопасность – для передачи данных является обязательным использование *протокола защищенной передачи* IPsec (протокол IPv4 также может использовать IPsec, но не обязан этого делать).

В настоящее время многие производители сетевого оборудования включают поддержку протокола IPv6 в свои продукты, однако преобладающим остается протокол IPv4. Связано это с тем, что IPv6 обратно несовместим с IPv4 и процесс перехода сопряжен с определенными трудностями.

5.2.5. Особые IP-адреса

Некоторые IP-адреса являются особыми, они не должны применяться для идентификации обычных сетей.

1. Если первый октет ID сети начинается с 127, такой адрес считается адресом машины-источника пакета. В этом случае пакет не выходит в сеть, а возвращается на компьютер-отправитель. Такие адреса называются **loopback** (**петля**, замыкание на себя) и используются для проверки функционирования стека TCP/IP.

2. Если все биты IP-адреса равны нулю, адрес обозначает узел-отправитель и используется в некоторых сообщениях ICMP.

3. Если все биты ID сети равны 1, адрес называется ***ограниченным широковещательным*** (limited broadcast). Пакеты, направленные по такому адресу, рассылаются всем узлам той подсети, в которой находится отправитель пакета.

4. Если все биты ID хоста равны 1, адрес называется ***широковещательным*** (broadcast); пакеты, имеющие широковещательный адрес, доставляются всем узлам подсети назначения.

5. Если все биты ID хоста равны 0, адрес считается **идентификатором подсети** (subnet ID).

Наличие особых IP-адресов объясняет, почему из диапазона доступных адресов исключаются два адреса – это случаи, когда все биты ID хоста равны 1 или 0. Например, в сети *класса C* не 256, а 254 узлов.

5.2.6. Автоматизация назначения IP-адресов узлам сети – протокол DHCP

Как уже было сказано, IP-адреса могут назначаться администратором сети вручную. Это представляет для администратора утомительную процедуру. Ситуация усложняется еще тем, что многие пользователи не обладают достаточными знаниями для того, чтобы конфигурировать свои компьютеры для работы в интерсети, и должны поэтому полагаться на администраторов.

Протокол Dynamic Host Configuration Protocol (DHCP) был разработан для того, чтобы освободить администратора от этих проблем. Основным назначением DHCP является динамическое назначение IP-адресов. Однако, кроме динамического, DHCP может поддерживать и более простые способы ручного и автоматического статического назначения адресов.

В ручной процедуре назначения адресов активное участие принимает администратор, который предоставляет DHCP-серверу информацию о соответствии IP-адресов физическим адресам или другим идентификаторам клиентов. Эти адреса сообщаются клиентам в ответ на их запросы к DHCP-серверу.

При автоматическом статическом способе DHCP-сервер присваивает IP-адрес (и, возможно, другие параметры конфигурации клиента) из пула наличных IP-адресов без вмешательства оператора. Границы пула назначаемых адресов задает администратор при кон-

фигурировании DHCP-сервера. Между идентификатором клиента и его IP-адресом по-прежнему, как и при ручном назначении, существует постоянное соответствие. Оно устанавливается в момент первичного назначения сервером DHCP IP-адреса клиенту. При всех последующих запросах сервер возвращает тот же самый IP-адрес.

При динамическом распределении адресов DHCP-сервер выдает адрес клиенту на ограниченное время, что предоставляет возможность впоследствии повторно использовать IP-адреса другими компьютерами. Служба DHCP обеспечивает надежный и простой способ конфигурации сети TCP/IP, гарантируя отсутствие конфликтов адресов за счет централизованного управления их распределением. Администратор управляет процессом назначения адресов с помощью параметра «продолжительности аренды», который определяет, как долго компьютер может использовать назначенный IP-адрес, перед тем как снова запросить его от сервера DHCP в аренду.

Примером работы протокола DHCP может служить ситуация, когда компьютер, являющийся клиентом DHCP, удаляется из подсети. При этом назначенный ему IP-адрес автоматически освобождается. Когда компьютер подключается к другой подсети, то ему автоматически назначается новый адрес. Ни пользователь, ни сетевой администратор не вмешиваются в этот процесс. Это свойство очень важно для мобильных пользователей.

Пример 5. Настройка DHCP-сервера (в ОС Windows 2003 Server).

1. Установка и авторизация сервера DHCP

Установка службы DHCP выполняется так же, как и установка любой другой компоненты Windows Server: *Пуск – Панель управления – Установка и удаление программ – Установка компонентов Windows – Сетевые службы* – кнопка *Состав* – выбрать пункт *DHCP* – кнопки *ОК*, *Далее* и *Готово* (если потребуется, то указать путь к дистрибутиву системы).

Для авторизации сервера DHCP (*рис. 5.10*) необходимо запустить появившуюся в разделе *Администрирование* консоль управления службой DHCP с правами пользователя, являющегося членом группы *Администраторы*. Если текущая рабочая учетная запись не входит в данную группу, то для запуска консоли с соответствующими полномочиями необходимо щелкнуть правой кнопкой мыши на ярлыке консоли и выбрать пункт меню *Запуск от имени…*,

после чего указать имя пользователя, являющегося членом группы *Администраторы*, и ввести его пароль.

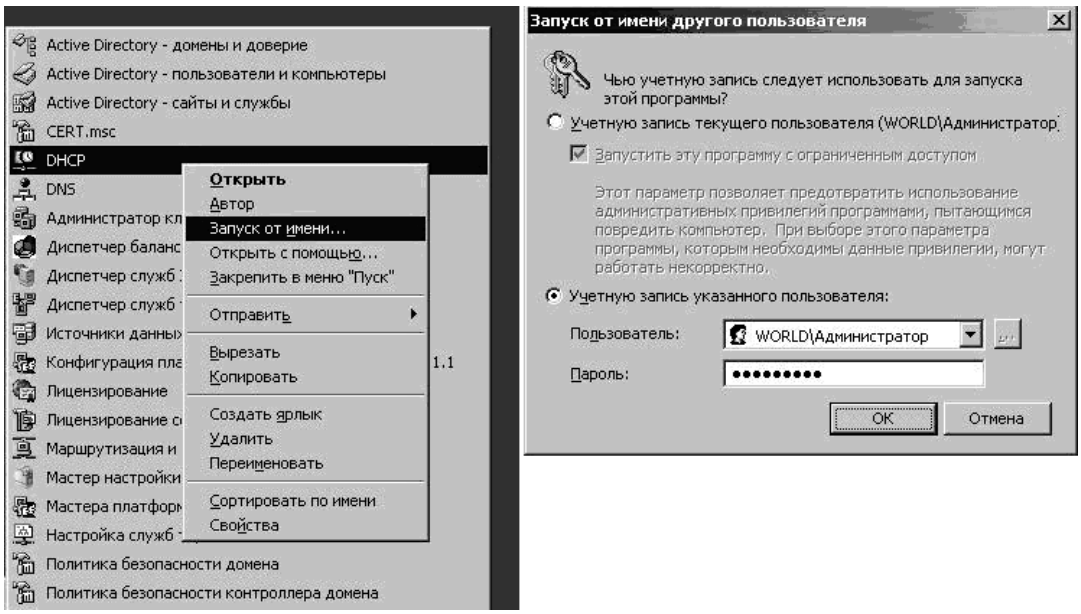


Рис. 5.10. Запуск службы DHCP

Для авторизации сервера необходимо в консоли DHCP выбрать сервер, щелкнуть на имени сервера правой кнопкой мыши и выбрать пункт меню *Авторизовать* (*рис. 5.11*).

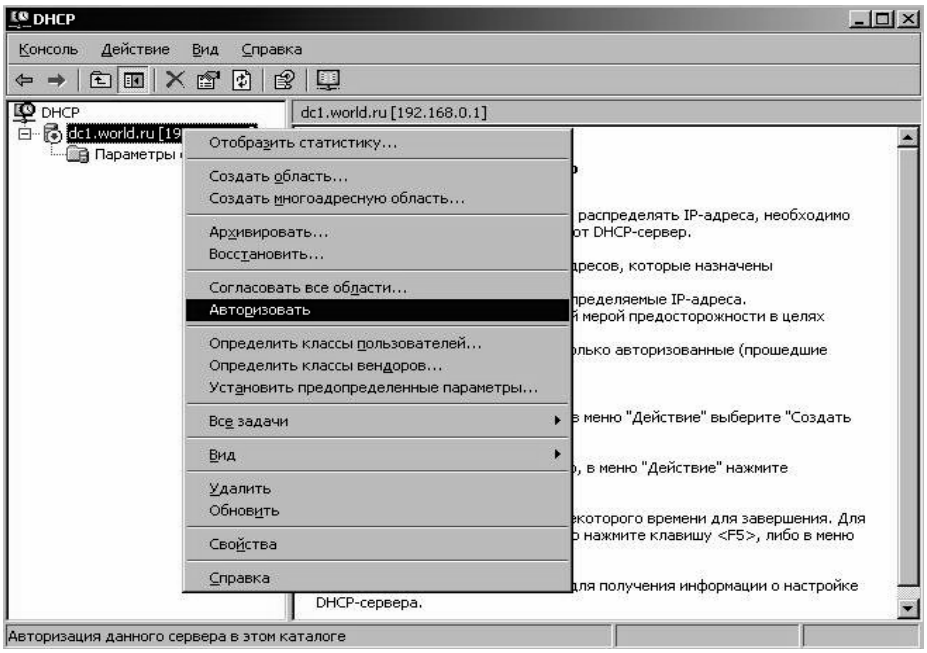


Рис. 5.11. Авторизация DHCP сервера

Когда авторизация будет завершена, значок у имени сервера изменится – вместо красной стрелки, направленной вниз, появится зеленая стрелка, направленная вверх.

2. Настройка параметров DHCP-сервера

Создать область можно, щелкнув правой кнопкой мыши на имени сервера и выбрав пункт меню *Создать область* (или выбрав аналогичный пункт в меню *Действие* консоли DHCP). Консоль запустит *Мастер создания области*, который позволяет по шагам определить все необходимые параметры.

Имя и описание области. В больших сетях именование областей и задание их краткого описания облегчает работу администратора за счет более наглядного отображения в консоли всех созданных областей (*рис. 5.12*).

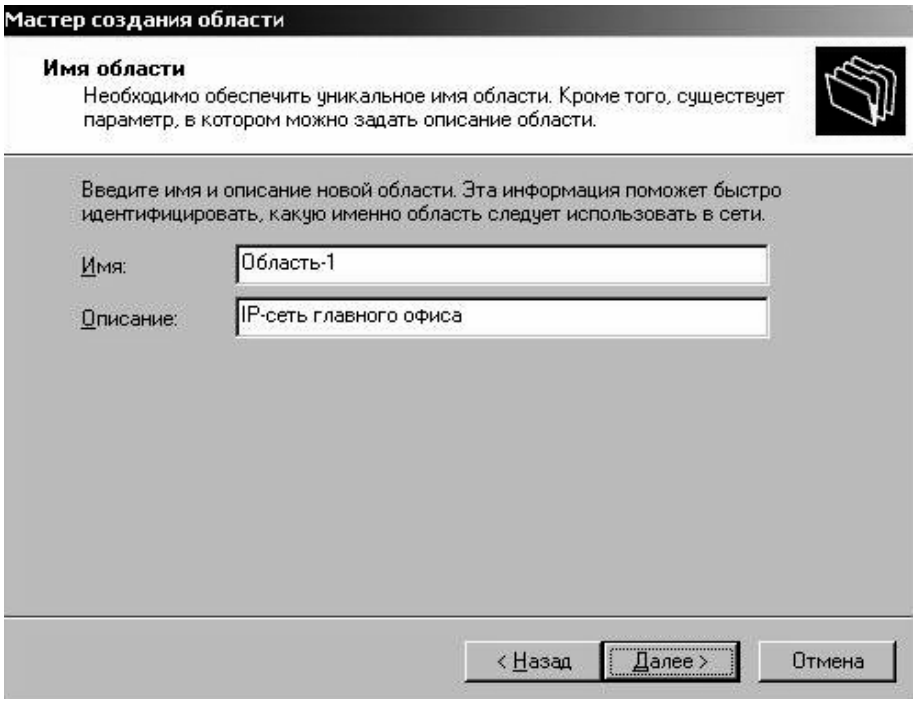


Рис. 5.12. Создание области DHCP-сервера

Определение диапазона IP-адресов и маски подсети (*рис. 5.13*).

Добавление исключений. На данном шаге задаются диапазоны IP-адресов, которые будут исключены из процесса выдачи адресов клиентам.

Срок действия аренды. Стандартный срок действия 8 дней. Если в вашей сети редко происходят изменения (добавление или удаление сетевых узлов, перемещение сетевых узлов из одной

подсети в другую), то срок действия можно увеличить, это сократит количество запросов на обновление аренды. Если же ваша сеть более динамичная, то срок аренды можно сократить, это позволит быстрее возвращать в пул IP-адреса, которые принадлежали компьютерам, уже удаленным из данной подсети.

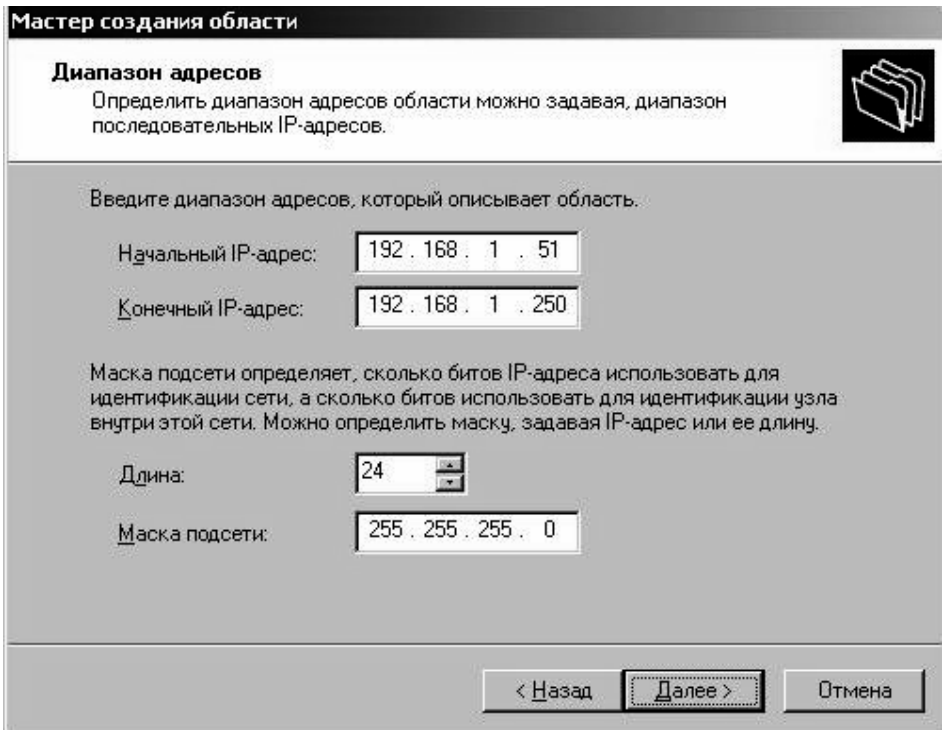


Рис. 5.13. Создание диапазона адресов области

Далее мастер предложит настроить параметры, специфичные для узлов IP-сети, относящихся к данной области: маршрутизатор (основной шлюз; *рис. 5.14*); адрес DNS-сервера (можно назначить несколько адресов; *рис. 5.15*); адрес WINS-сервера (аналогично серверу DNS; можно также назначить несколько адресов).

Запрос на активацию области. IP-адреса, заданные в созданной области, не будут выдаваться клиентам, пока область не будет активирована (*рис. 5.16*).

Нажимаем кнопку *Готово* и завершаем работу мастера. Область готова к использованию. Если какие-либо параметры (например, адреса серверов DNS или WINS) являются общими для всех областей, управляемых данным DHCP-сервером, то такие параметры лучше определить не в разделе параметров каждой области, а в разделе параметров самого сервера (*рис. 5.17*).

Нажимаем кнопку *Готово* и завершаем работу мастера. Область готова к использованию.

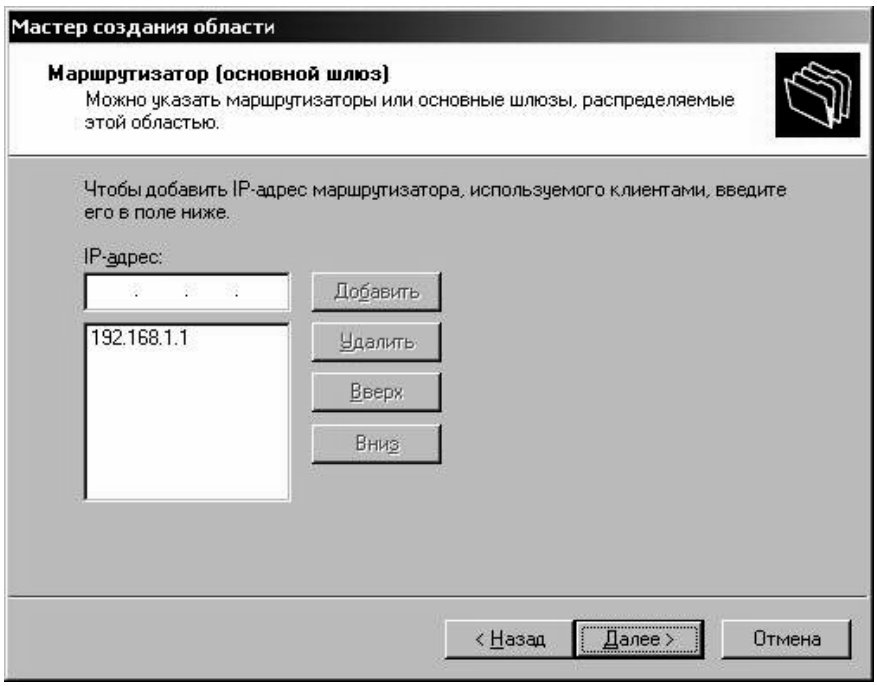


Рис. 5.14. Добавление адреса шлюза, распределяемого областью

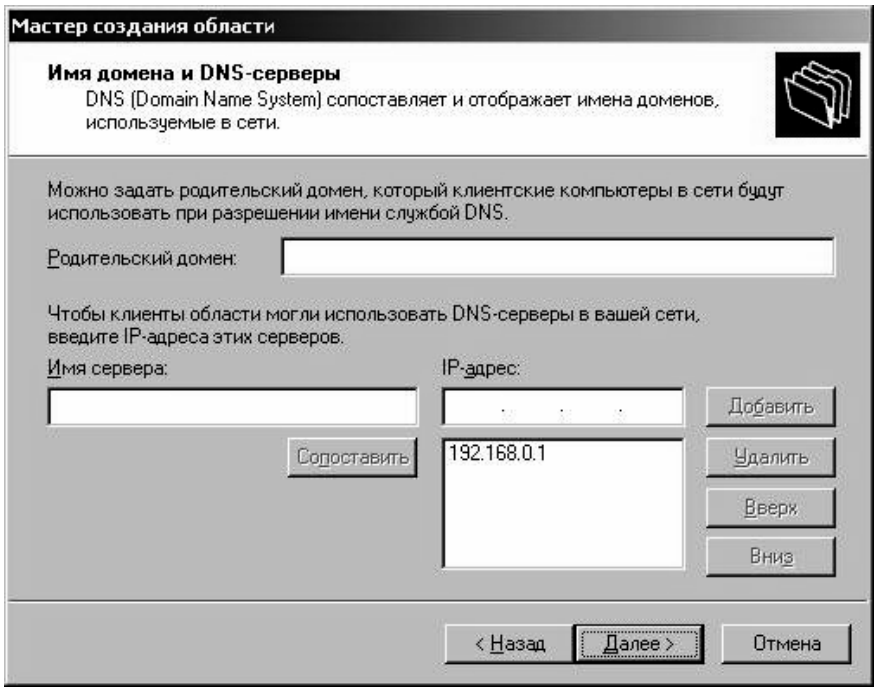


Рис. 5.15. Добавление адреса DNS-сервера, распределяемого областью

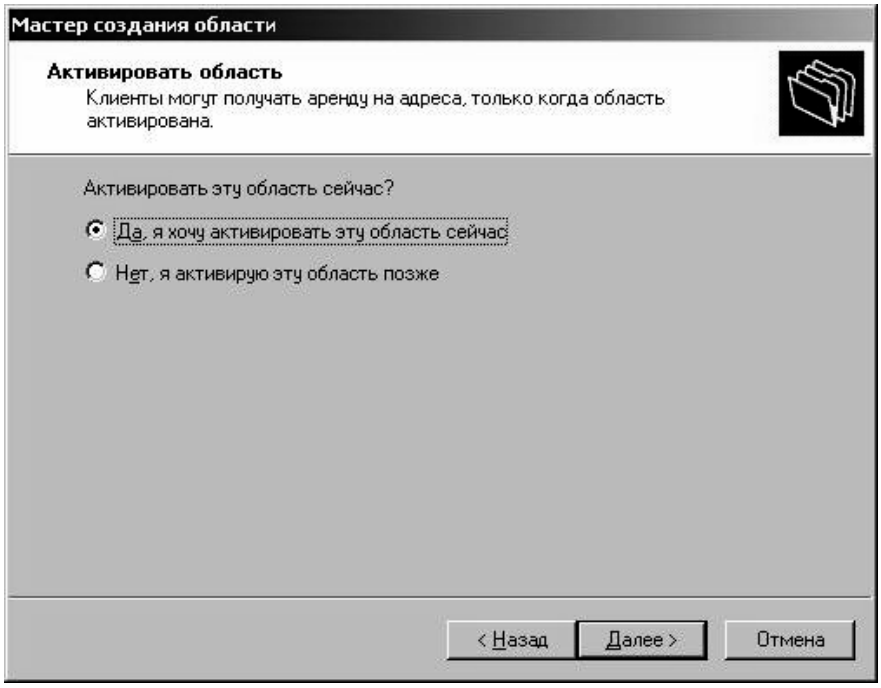


Рис. 5.16. Запрос на активацию области DHCP-сервера

Если какие-либо параметры (например, адреса серверов DNS или WINS) являются общими для всех областей, управляемых данным DHCP-сервером, то такие параметры лучше определить не в разделе параметров каждой области, а в разделе параметров самого сервера (*рис. 5.17*).

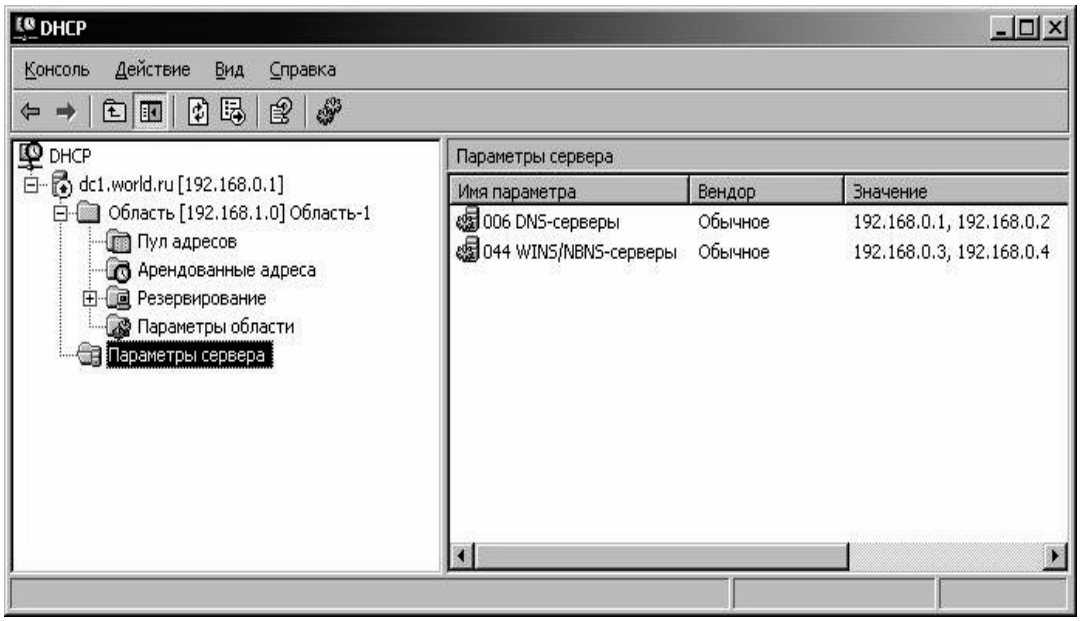


Рис. 5.17. Общие параметры DHCP-сервера

Протокол DHCP использует модель клиент – сервер. Во время старта системы компьютер – клиент DHCP, находящийся в состоянии «инициализация», посылает сообщение *discover* (исследовать), которое широковещательно распространяется по локальной сети и передается всем DHCP-серверам частной интерсети. Каждый DHCP-сервер, получивший это сообщение, отвечает на него сообщением *offer* (предложение), которое содержит IP-адрес и конфигурационную информацию.

Компьютер-клиент DHCP переходит в состояние «выбор» и собирает конфигурационные предложения от DHCP-серверов. Затем он выбирает одно из этих предложений, переходит в состояние «запрос» и отправляет сообщение *request* (запрос) тому DHCP-серверу, чье предложение было выбрано.

Выбранный DHCP-сервер посылает сообщение DHCP-*acknowledgment* (подтверждение), содержащее тот же IP-адрес, который уже был послан ранее на стадии исследования, а также параметр аренды для этого адреса. Кроме того, DHCP-сервер посылает параметры сетевой конфигурации. После того, как клиент получит это подтверждение, он переходит в состояние «связь», находясь в котором он может принимать участие в работе сети TCP/IP. Компьютеры-клиенты, которые имеют локальные диски, сохраняют полученный адрес для использования при последующих стартах системы. При приближении момента истечения *срока аренды адреса* компьютер пытается обновить параметры аренды у DHCP-сервера, а если этот IP-адрес не может быть выделен снова, то ему возвращается другой IP-адрес.

Однако использование DHCP несет в себе и некоторые проблемы. Во-первых, это проблема согласования информационной адресной базы в службах DHCP и DNS. Как известно, DNS служит для преобразования символьных имен в IP-адреса. Если IP-адреса будут динамически изменятся сервером DHCP, то эти изменения необходимо также динамически вносить в базу данных сервера DNS.

Во-вторых, нестабильность IP-адресов усложняет процесс управления сетью. Системы управления, основанные на протоколе SNMP, разработаны с расчетом на статичность IP-адресов. Аналогичные проблемы возникают и при конфигурировании фильтров маршрутизаторов, которые оперируют с IP-адресами.

Наконец, централизация процедуры назначения адресов снижает надежность системы: при отказе DHCP-сервера все его клиенты

оказываются не в состоянии получить IP-адрес и другую информацию о конфигурации. Последствия такого отказа могут быть уменьшены путем использовании в сети нескольких серверов DHCP, каждый из которых имеет свой пул IP-адресов.

5.2.7. Распределение IP-адресов

Поскольку каждый узел сети Интернет должен обладать уникальным IP-адресом, то, безусловно, важной является задача координации распределения адресов отдельным сетям и узлам. Такую координирующую роль выполняет Интернет-корпорация по распределению адресов и имен (The Internet Corporation for Assigned Names and Numbers, ICANN).

Естественно, что ICANN не решает задач выделения IP-адресов конечным пользователям и организациям, а занимается распределением диапазонов адресов между крупными организациями-поставщиками услуг по доступу к сети Интернет (Internet Service Provider), которые, в свою очередь, могут взаимодействовать как с более мелкими поставщиками, так и с конечными пользователями. Так, например, функции по распределению IP-адресов в Европе ICANN делегировал Координационному Центру RIPE (RIPE NCC, The RIPE Network Coordination Centre, RIPE – Reseaux IP Europeens). В свою очередь, этот центр делегирует часть своих функций региональным организациям.

5.2.8. Частные адреса

Служба распределения номеров IANA (Internet Assigned Numbers Authority) зарезервировала для частных сетей три блока адресов:

10.0.0.0 – 10.255.255.255 (префикс 10/8);

172.16.0.0 – 172.31.255.255 (префикс 172.16/12);

192.168.0.0 – 192.168.255.255 (префикс 192.168/16).

Будем называть первый блок 24-битовым, второй – 20-битовым, а третий – 16-битовым. Отметим, что первый блок представляет собой не что иное, как одну сеть класса A, второй блок – 16 последовательных сетей класса B, а третий блок – 256 последовательных сетей класса C.

Любая организация может использовать IP-адреса из этих блоков без согласования с ICANA или Internet-регистраторами. В результате эти адреса используются во множестве организаций. Таким образом, уникальность адресов сохраняется только

в масштабе одной или нескольких организаций, согласованно использующих общий блок адресов. В такой сети каждая рабочая станция может обмениваться информацией с любой другой рабочей станцией частной сети.

Если организации требуются уникальные адреса для связи с внешними сетями, такие адреса следует получать обычным путем через регистраторов Internet. Такие адреса никогда не будут входить ни в один из указанных выше блоков частных адресов.

Перед распределением адресов из частного и публичного блоков следует определить, какие из рабочих станций сети должны иметь связь с внешними системами на сетевом уровне. Для таких рабочих станций следует использовать публичные адреса, остальным же можно присваивать адреса из частных блоков, это не помешает им взаимодействовать со всеми рабочими станция частной сети организации, независимо от того, какие адреса используются (частные или публичные). Однако прямой доступ во внешние сети для рабочих станций с адресами из частного блока невозможен. Для организации их доступа во внешние шлюзы придется использовать прокси-серверы.

Перемещение рабочей станции из частной сети в публичную (и обратное) связано со сменой IP-адреса, соответствующих записей DNS и изменением конфигурационных файлов на других рабочих станциях, которые их идентифицируют по IP-адресам. Поскольку частные адреса не имеют глобального значения, маршрутная информация о частных сетях не должна выходить за пределы этих сетей, а пакеты с частными адресами отправителей или получателей не должны передаваться через межсетевые каналы. Предполагается, что маршрутизаторы в публичных сетях (особенно маршрутизаторы провайдеров Internet) будут отбрасывать маршрутную информацию из частных сетей. Если маршрутизатор публичной сети получает такую информацию, ее отбрасывание не должно трактоваться как ошибка протокола маршрутизации.

5.3. Символьный адрес

5.3.1. DNS-имена

DNS (Domain Name System) – это распределенная база данных, поддерживающая иерархическую систему имен для идентификации узлов в сети Internet.

Служба DNS предназначена для автоматического поиска IP-адреса по известному символьному имени узла. Спецификация DNS определяется стандартами RFC 1034 и 1035. DNS требует статической конфигурации своих таблиц, разрешающих имена компьютеров в IP-адреса.

Протокол DNS является служебным протоколом прикладного уровня. Этот протокол несимметричен – в нем определены DNS-серверы и DNS-клиенты.

DNS-серверы хранят часть распределенной базы данных о соответствии символьных имен и IP-адресов. Эта база данных распределена по административным доменам сети Internet. Клиенты сервера DNS знают IP-адрес сервера DNS своего административного домена и по протоколу IP передают запрос, в котором сообщают известное символьное имя и просят вернуть соответствующий ему IP-адрес. Если данные о запрошенном соответствии хранятся в базе данного DNS-сервера, то он сразу посылает ответ клиенту, если же нет – то он посылает запрос DNS-серверу другого домена, который может сам обработать запрос либо передать его другому DNS-серверу. Все DNS-серверы соединены иерархически в соответствии с иерархией доменов сети Internet. Клиент опрашивает эти серверы имен, пока не найдет нужные отображения. Этот процесс ускоряется из-за того, что серверы имен постоянно кэшируют информацию, предоставляемую по запросам. Клиентские компьютеры могут использовать в своей работе IP-адреса нескольких DNS-серверов для повышения надежности своей работы.

База данных DNS имеет структуру дерева, называемого **доменным пространством имен**, в котором каждый домен (узел дерева) имеет имя и может содержать поддомены.

Имя домена идентифицирует его положение в этой базе данных по отношению к родительскому домену, причем точки в имени отделяют части, соответствующие узлам домена.

Корень базы данных DNS управляется центром Internet Network Information Center. Домены верхнего уровня назначаются для каждой страны, а также на организационной основе. Имена этих доменов должны отвечать международному стандарту ISO 3166. Для обозначения стран используются трехбуквенные и двухбуквенные аббревиатуры, а для различных типов организаций используются следующие аббревиатуры:

– **com** – коммерческие организации (например, microsoft.com);
– **edu** – образовательные (например, mit.edu);
– **gov** – правительственные организации (например, nsf.gov);
– **org** – некоммерческие организации (например, fidonet.org);
– **net** – организации, поддерживающие сети (например, nsf.net).

Каждый домен DNS администрируется отдельной организацией, которая обычно разбивает свой ***домен*** на ***поддомены*** и передает функции администрирования этих поддоменов другим организациям. Каждый домен имеет уникальное имя, а каждый из поддоменов имеет уникальное имя внутри своего домена. Имя домена может содержать до 63 символов. Каждый хост в сети Internet однозначно определяется своим полным доменным именем (fully qualified domain name, FQDN), которое включает имена всех доменов по направлению от хоста к корню.

Рассмотрим пример организации DNS-адресации в локальной сети.

Пример 6. Для организации DNS-адресации необходимо выполнить определенные действия на двух серверах (с именами DC1 и DC2) и клиенте.

1. Установка DNS-сервера

Установка службы DNS производится достаточно просто с помощью мастера установки компонент Windows:

– откройте *Панель управления*;
– выберите пункт *Установка и удаление программ*;
– нажмите кнопку *Установка компонентов Windows* (*рис. 5.18*);
– выберите *Сетевые службы* – кнопка *Дополнительно* (ни в коем случае не ставьте галочку у названия *Сетевые службы*);
– отметьте службу DNS;
– кнопка *ОК*, кнопка *Далее*, кнопка *Готово* (если система попросит указать путь к дистрибутиву системы, введите путь к папке с дистрибутивом).

Выполним данные действия на обоих серверах.

2. Создание основной зоны прямого просмотра

На сервере DC1 создадим стандартную основную зону с именем world.ru:

– откройте консоль DNS;
– выберите раздел *Зоны прямого просмотра*;

– запустите мастер создания зоны (тип зоны – *Основная*, динамические обновления – *разрешить*, остальные параметры – по умолчанию);

– введите имя зоны – world.ru;

– разрешите передачу данной зоны на любой сервер DNS (*Консоль DNS* – зона world.ru – *Свойства* – Закладка *Передачи зон* – отметьте *Разрешить передачи* и *На любой сервер*).

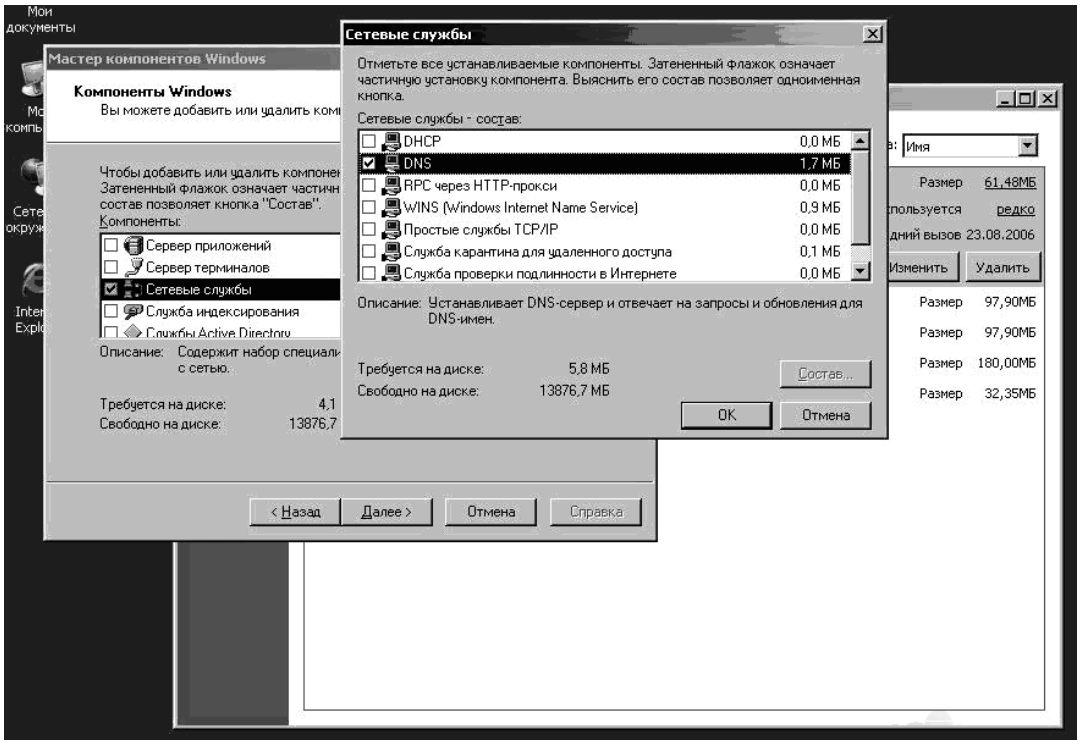


Рис. 5.18. Установка службы DNS

3. Создание дополнительной зоны прямого просмотра

На сервере DC2 создадим стандартную дополнительную зону с именем world.ru:

– откройте консоль DNS.;

– выберите раздел *Зоны прямого просмотра*;

– запустите мастер создания зоны (выберите: тип зоны – *Дополнительная*, IP-адрес master-сервера (с которого будет копироваться зона) – *адрес сервера DC1*, остальные параметры – по умолчанию);

– введите имя зоны – world.ru.

4. Настройка узлов для выполнения динамической регистрации на сервер DNS

Для выполнения данной задачи нужно выполнить ряд действий как на сервере DNS, так и в настройках клиента DNS.

На сервере *DNS* необходимо:

– создать соответствующую зону;

– разрешить динамические обновления.

На клиенте *DNS* необходимо сделать следующее:

– указать в настройках протокола TCP/IP адрес предпочитаемого DNS-сервера – тот сервер, на котором разрешены динамические обновления (в нашем примере – сервер DC1);

– в полном имени компьютера указать соответствующий DNS-суффикс (*рис. 5.19*) (в нашем примере – world.ru). Для этого последовательно инициировать: *Мой компьютер – Свойства* – закладка *Имя компьютера* – кнопка *Изменить* – кнопка *Дополнительно* – в пустом текстовом поле вписать название домена world.ru – кнопка *ОК* (3 раза)).

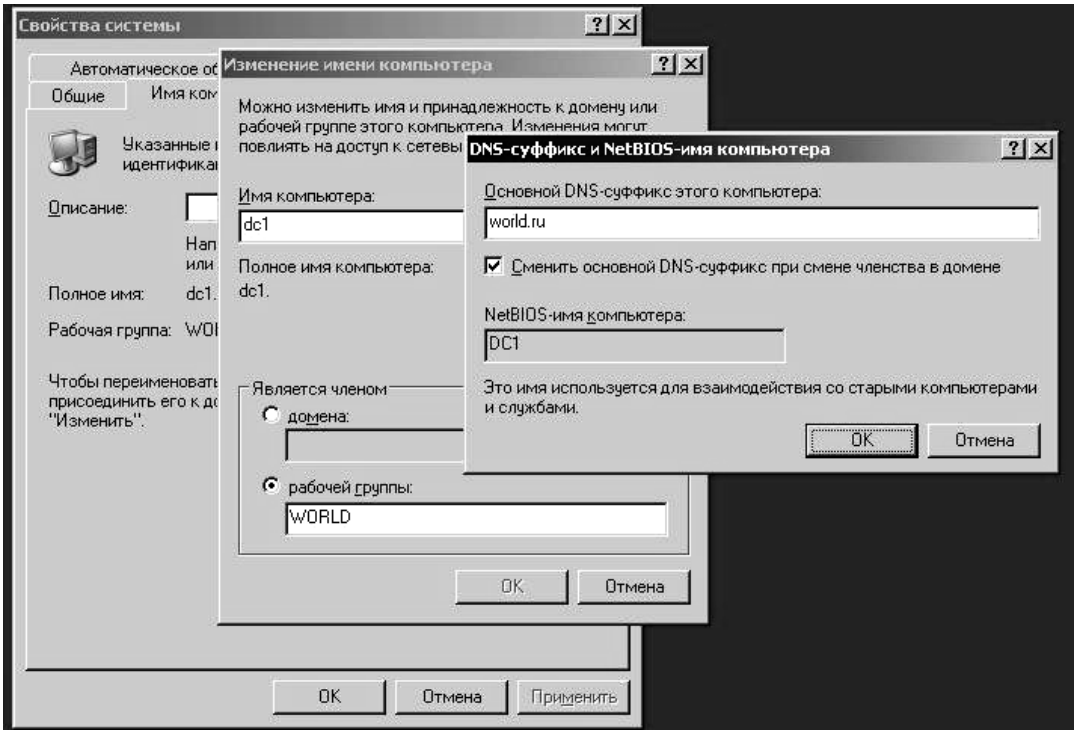


Рис. 5.19. Установка DNS-суффикса
в полном имени компьютера

После этого система предложит перезагрузить компьютер. После выполнения перезагрузки на сервер DNS в зоне world.ru автоматически создадутся записи типа A для наших серверов (*рис. 5.20*).

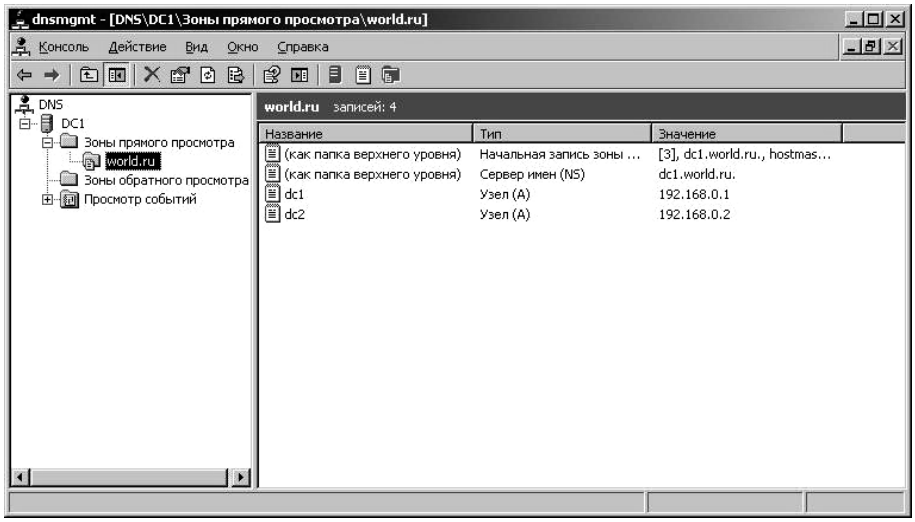


Рис. 5.20. Консоль DNS-сервера с зоной прямого просмотра

5. Создание зоны обратного просмотра выполняется по следующим шагам:

– откройте консоль DNS;

– выберите раздел *Зоны обратного просмотра*;

– запустите мастер создания зоны (выберите: тип зоны – *Основная*, динамические обновления – разрешить, остальные параметры – по умолчанию);

– в поле *Код сети* (*ID*) введите параметры идентификатора сети – 192.168.0, а затем выполните команду принудительной регистрации клиента на сервере DNS – ipconfig/registerdns.

В итоге серверы зарегистрируются в обратной зоне DNS (*рис. 5.21*).

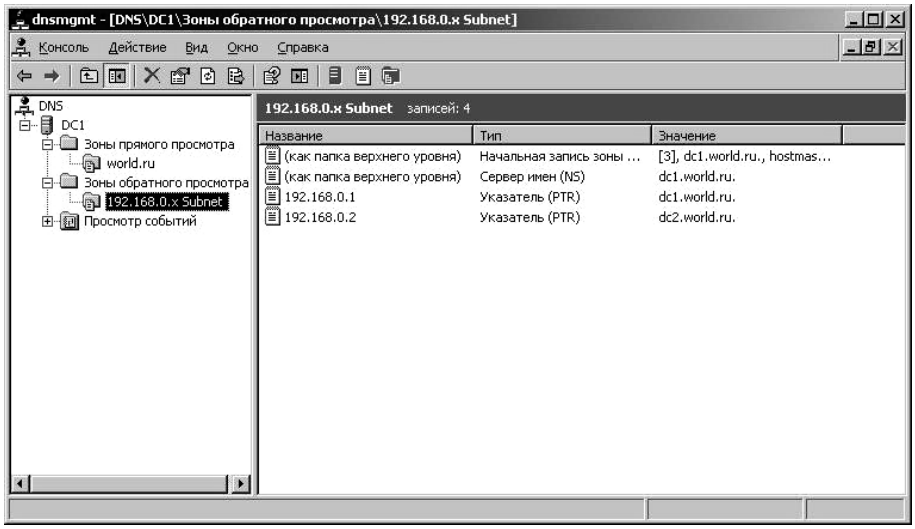


Рис. 5.21. Консоль DNS-сервера с зоной обратного просмотра

5.3.2. Имена NetBIOS

Протокол *NetBIOS* (Network Basic Input/Output System – сетевая базовая система ввода/вывода) был разработан в 1984 году для корпорации IBM как сетевое дополнение стандартной BIOS на компьютерах IBM PC. В операционных системах Microsoft Windows NT, а также в Windows 98 протокол и имена NetBIOS являлись основными сетевыми компонентами. Начиная с Windows 2000, операционные системы Microsoft ориентируются на глобальную сеть Интернет, в этой связи фундаментом сетевых решений стали протоколы TCP/IP и доменные имена. Однако поддержка имен NetBIOS осталась и в операционной системе Windows Server 2008.

Система имен NetBIOS представляет собой простое неиерархическое пространство, т. е. в имени NetBIOS отсутствует структура, деление на уровни, как в DNS-именах. Длина имени не более 15 символов (плюс один служебный).

Для преобразования NetBIOS-имен в IP-адреса в операционной системе Windows Server используется служба WINS – Windows Internet Naming Service (служба имен в Интернете для Windows).

Служба WINS работает, как и служба DNS, по модели клиент – сервер. WINS-клиенты используют WINS-сервер для регистрации своего NetBIOS-имени и преобразования неизвестного NetBIOS-имени в IP-адрес. Функции сервера NetBIOS-имен описаны в RFC 1001 и 1002.

5.4. Утилиты диагностики TCP/IP и DNS

Любая операционная система имеет набор диагностических утилит для тестирования сетевых настроек и функционирования коммуникаций. Большой набор диагностических средств есть и в системах семейства Windows (как графических, так и в режиме командной строки).

Утилиты командной строки, являющиеся инструментами первой необходимости для проверки настроек протокола TCP/IP и работы сетей и коммуникаций, представлены в *табл. 5.2*. Подробное описание данных утилит содержится в системе интерактивной помощи Windows (вызывается нажатием кнопки F1). В *табл. 5.2* указаны основные и наиболее часто используемые параметры этих команд, а также дано их краткое описание.

Таблица 5.2

Утилиты диагностики TCP/IP и DNS

Название утилиты	Параметры	Комментарии
ipconfig	**/?** – отобразить справку по команде **/all** – отобразить полную информацию о настройке параметров всех адаптеров **/release** – освободить динамическую IP-конфигурацию **/renew** – обновить динамическую IP-конфигурацию с DHCP-сервера **/flushdns** – очистить кэш разрешений DNS **/registerdns** – обновить регистрацию на DNS-сервере **/displaydns** – отобразить содержимое кэша разрешений DNS	Служит для отображения всех текущих параметров сети TCP/IP и обновления параметров DHCP и DNS. При вызове команды ipconfig без параметров выводятся IP-адрес, маска подсети и основной шлюз для каждого сетевого адаптера
arp	**-a** – отображает текущие ARP-записи	Отображение и изменение ARP-таблиц
ping	Формат команды: **ping <*сетевой узел*> параметры** Параметры: **-t** – бесконечная (до нажатия клавиш <Ctrl>+<Break>) отправка пакетов на указанный узел **-a** – определение имени узла по IP-адресу **-n <число>** – число отправляемых запросов **-l <размер>** – размер буфера отправки **-w <таймаут>** – таймаут ожидания каждого ответа в миллисекундах	Мощный инструмент диагностики (с помощью протокола ICMP). Команда ping позволяет проверить: работоспособность IP-соединения; правильность настройки протокола TCP/IP на узле; работоспособность маршрутизаторов; работоспособность системы разрешения имен FQDN или NetBIOS; доступность и работоспособность какого-либо сетевого ресурса
tracert	**-d** – без разрешения IP-адресов в имена узлов **-h <максЧисло>** – максимальное число прыжков при поиске узла **-w <таймаут>** – таймаут каждого ответа в миллисекундах	Служебная программа для трассировки маршрутов, используемая для определения пути, по которому IP-дейтаграмма доставляется по месту назначения

Окончание табл. 5.2

Название утилиты	Параметры	Комментарии
pathping	**-n** – без разрешения IP-адресов в имена узлов **-h максЧисло** – максимальное число прыжков при поиске узла **-q <число_запросов>** – число запросов при каждом прыжке **-w <таймаут>** – таймаут каждого ответа в миллисекундах	Средство трассировки маршрута, сочетающее функции программ *ping* и *tracert* и обладающее дополнительными возможностями. Эта команда показывает степень потери пакетов на любом маршрутизаторе или канале, с ее помощью легко определить, какие маршрутизаторы или каналы вызывают неполадки в работе сети
netstat	**-a** – отображение *всех* подключений и ожидающих (слушающих) портов **-n** – отображение адресов и номеров портов в числовом формате **-o** – отображение кода (ID) процесса каждого подключения **-r** – отображение содержимого локальной таблицы маршрутов	Используется для отображения статистики протокола и текущих TCP/IP-соединений
nbtstat	**-n** – выводит имена пространства имен NetBIOS, зарегистрированные локальными процессами **-c** – отображает кэш имен NetBIOS (разрешение NetBIOS-имен в IP-адреса) **-R** – очищает кэш имен и перезагружает его из файла Lmhosts **-RR** – освобождает имена NetBIOS, зарегистрированные на WINS-сервере, а затем обновляет их регистрацию	Средство диагностики разрешения имен NetBIOS
hostname	Никаких ключей для данной утилиты не предусмотрено	Это самая простая утилита – она выводит на экран имя компьютера

Рассмотрим примеры использования утилит командной строки для диагностики протокола TCP/IP и символьной адресации (DNS).

Пример 7. Использование команды **ipconfig** (без параметров и с параметром /all) представлено на *рис. 5.22*.

```
C:\>ipconfig

Настройка протокола IP для Windows

Подключение по локальной сети - Ethernet адаптер:

   DNS-суффикс этого подключения . . :
   IP-адрес  . . . . . . . . . . . . : 192.168.0.1
   Маска подсети . . . . . . . . . . : 255.255.255.0
   Основной шлюз . . . . . . . . . . :

C:\> ipconfig /all

Настройка протокола IP для Windows

   Имя компьютера  . . . . . . . . . : dc1
   Основной DNS-суффикс  . . . . . . : world.ru
   Тип узла. . . . . . . . . . . . . : неизвестный
   IP-маршрутизация включена . . . . : нет
   WINS-прокси включен . . . . . . . : нет
   Порядок просмотра суффиксов DNS . : world.ru

Подключение по локальной сети - Ethernet адаптер:

   DNS-суффикс этого подключения . . :
   Описание  . . . . . . . . . . . . : Realtek RTL8139 Family
PCI Fast Ethernet NIC
   Физический адрес. . . . . . . . . : 00-11-D8-E7-14-F4
   DHCP включен. . . . . . . . . . . : нет
   IP-адрес  . . . . . . . . . . . . : 192.168.0.1
   Маска подсети . . . . . . . . . . : 255.255.255.0
   Основной шлюз . . . . . . . . . . :
   DNS-серверы . . . . . . . . . . . : 192.168.0.1
```

Рис. 5.22. Использование команды **ipconfig**

Пример 8. Рассмотрим использование команды **arp**. Пусть в сети только два узла (сервер DC1 и сервер DC2). Тогда в кэше сервера DC1 будет только одна запись – отображение IP-адреса сервера DC2 на MAC-адрес сетевого адаптера (*рис. 5.23*).

```
C:\>arp -a
Интерфейс: 192.168.0.1 --- 0x10003
  IP-адрес              Физический адрес      Тип
  192.168.0.2           00-03-ff-e7-14-f4     динамический
```

Рис. 5.23. Использование команды **arp**

Пример 9. Рассмотрим использование команды **ping**.

Существуют различные варианты использования данной утилиты (в сети существуют два компьютера с именами DC1 и DC2, настроена DNS-адресация):

– ping <IP-адрес> (*рис. 5.24*);

– ping <NetBIOS-имя узла>, когда в зоне сервера DNS нет записи для сервера DC2 (поиск IP-адреса производится широковещательным запросом) (*рис. 5.25*);

– ping <NetBIOS-имя узла>, когда в зоне сервера DNS есть запись для сервера DC2 (надо обратить внимание на подстановку клиентом DNS суффикса домена в запросе на имя узла, т. е. в команде используется краткое NetBIOS-имя сервера, а в статистике команды выводится полное имя) (*рис. 5.26*);

– ping <FQDN-имя узла>, когда в зоне сервера DNS нет записи для сервера DC2 (узел DC2 не будет найдет в сети) (*рис. 5.27*);

– ping <FQDN-имя узла>, когда в зоне сервера DNS есть запись для сервера DC2 (узел успешно найден) (*рис. 5.28*);

– ping -a <IP-адрес> (обратное разрешение IP-адреса в имя узла) (*рис. 5.29*).

```
C:\>ping 192.168.0.2

Обмен пакетами с 192.168.0.2 по с 32 байт данных:

Ответ от 192.168.0.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.0.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.0.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.0.2: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.0.2:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
```

Рис. 5.24. Использование команды **ping** с заданным IP-адресом

```
C:\>ping dc2

Обмен пакетами с dc2 [192.168.0.2] с 32 байт данных:

Ответ от 192.168.0.2: число байт=32 время=16мс TTL=128
Ответ от 192.168.0.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.0.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.0.2: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.0.2:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 16 мсек, Среднее = 4 мсек
```

Рис. 5.25. Использование команды **ping** с заданным NetBIOS-именем узла (с широковещательным запросом)

```
C:\>ping dc2

Обмен пакетами с dc2.world.ru [192.168.0.2] с 32 байт данных:

Ответ от 192.168.0.2: число байт=32 время=16мс TTL=128
Ответ от 192.168.0.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.0.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.0.2: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.0.2:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 16 мсек, Среднее = 4 мсек
```

Рис. 5.26. Использование команды **ping** с заданным NetBIOS-именем узла (при условии существования записи на DNS-сервере)

```
C:\>ping dc2.world.ru

При проверке связи не удалось обнаружить узел dc2.world.ru.
Проверьте имя узла и повторите попытку.
```

Рис. 5.27. Использование команды **ping** с заданным FQDN-именем узла (при условии отсутствия записи на DNS-сервере)

```
C:\>ping dc2.world.ru

Обмен пакетами с dc2.world.ru [192.168.0.2] с 32 байт данных:

Ответ от 192.168.0.2: число байт=32 время=16мс TTL=128
Ответ от 192.168.0.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.0.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.0.2: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.0.2:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 16 мсек, Среднее = 4 мсек
```

Рис. 5.28. Использование команды **ping** с заданным FQDN-именем узла (при условии существования записи на DNS-сервере)

```
C:\>ping -a 192.168.0.2

Обмен пакетами с dc2.world.ru [192.168.0.2] с 32 байт данных:

Ответ от 192.168.0.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.0.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.0.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.0.2: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.0.2:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
```

Рис. 5.29. Использование команды **ping** с обратным разрешением IP-адреса в имя узла

Пример 10. Рассмотрим использование команды **tracert**. На *рис. 5.30* приведен пример трассировки маршрута до узла www.ru (если в распоряжении только одна IP-сеть, изучить работу данной команды будет невозможно).

```
C:\>tracert -d www.ru

Трассировка маршрута к www.ru [194.87.0.50]
с максимальным числом прыжков 30:

  1  17 ms  <1 мс  <1 мс  192.168.0.1
  2   1 ms  <1 мс   1 ms  217.1.1.33
  3   3 ms   3 ms   3 ms  217.1.10.1
  4   *      *      *     Превышен интервал ожидания для запро-
са.
  5   *      *      *     Превышен интервал ожидания для запро-
са.
  6  10 ms  11 ms  10 ms  217.150.36.190
  7   *      *      *     Превышен интервал ожидания для запро-
са.
  8  13 ms  13 ms  15 ms  194.87.0.83
  9  17 ms  12 ms  12 ms  194.87.0.50

Трассировка завершена.
```

Рис. 5.30. Использование команды **tracert**

Пример 11. Рассмотрим пример использования команды **pathping**. Пусть поставлена задача, аналогичная предыдущему примеру (трассировка маршрута до узла www.ru). Выполним ее командой **pathping** (*рис. 5.31*).

Пример 12. Рассмотрим пример использования команды **netstat** (с параметром -an – комбинация -a и -n) – отображение в числовой форме списка активных подключений и слушающих портов) (*рис. 5.32*).

```
C:\> pathping -n www.ru

Трассировка маршрута к www.ru [194.87.0.50]
с максимальным числом прыжков 30:
  0  192.168.0.1
  1  217.1.1.33
  2  217.1.10.1
  3     *        *        *
Подсчет статистики за: 100 сек. ...
           Исходный узел     Маршрутный узел
Прыжок  RTT   Утер./Отпр.   %   Утер./Отпр.  %   Адрес
  0    0мс     0/ 100 =  0%     0/ 100 =  0%  192.168.0.1
                                0/ 100 =  0%   |
  1    2мс     0/ 100 =  0%     0/ 100 =  0%  217.1.1.33
                                0/ 100 =  0%   |
  2    5мс     0/ 100 =  0%     0/ 100 =  0%  217.1.10.1
                               100/ 100 =100%   |
  3  ---     100/ 100 =100%     0/ 100 =  0%  0.0.0.0

Трассировка завершена.
```

Рис. 5.31. Использование команды **pathping**

```
C:\> netstat -an

Активные подключения

  Имя    Локальный адрес         Внешний адрес          Состояние
  TCP    0.0.0.0:53              0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1029            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1030            0.0.0.0:0              LISTENING
  TCP    192.168.0.1:139      0.0.0.0:0              LISTENING
  UDP    0.0.0.0:445             *:*
  UDP    0.0.0.0:500             *:*
  UDP    0.0.0.0:1025            *:*
  UDP    0.0.0.0:1028            *:*
  UDP    0.0.0.0:1035            *:*
  UDP    0.0.0.0:4500            *:*
  UDP    127.0.0.1:53            *:*
  UDP    127.0.0.1:123           *:*
  UDP    127.0.0.1:1026          *:*
  UDP    127.0.0.1:1027          *:*
  UDP    192.168.0.1:53       *:*
  UDP    192.168.0.1:123      *:*
  UDP    192.168.0.1:137      *:*
  UDP    192.168.0.1:138      *:*
```

Рис. 5.32. Использование команды **netstat**

Пример 13. Рассмотрим пример диагностики имен NetBIOS при помощи команды **nbtstat** (с параметром -n – отображение локальных имен NetBIOS) (*рис. 5.33*).

```
C:\> nbtstat -n

Подключение по локальной сети:
Адрес IP узла: [192.168.0.1] Код области: []

                Локальная таблица NetBIOS-имен

      Имя                 Тип          Состояние
    ---------------------------------------------------
    DC1             <00>  Уникальный  Зарегистрирован
    DC1             <20>  Уникальный  Зарегистрирован
    WORLD           <00>  Группа      Зарегистрирован
    WORLD           <1E>  Группа      Зарегистрирован
```

Рис. 5.33. Диагностика имен NetBIOS при помощи команды **nbtstat**

5.5. Маршрутизация в IP-сетях

5.5.1. Задача маршрутизации

Раскроем суть задачи *маршрутизации*. Пусть имеется составная сеть, задача состоит в том, чтобы доставить пакет из одной подсети в другую подсеть. Известны IP-адрес и маска подсети узла-отправителя (иными словами, ID подсети и ID хоста), IP-адрес узла-получателя. Сложность заключается в многочисленности возможных путей передачи пакета. Например, даже в простой сети, показанной на *рис. 5.34*, для передачи сообщения из подсети 1 в подсеть 3 существует несколько способов.

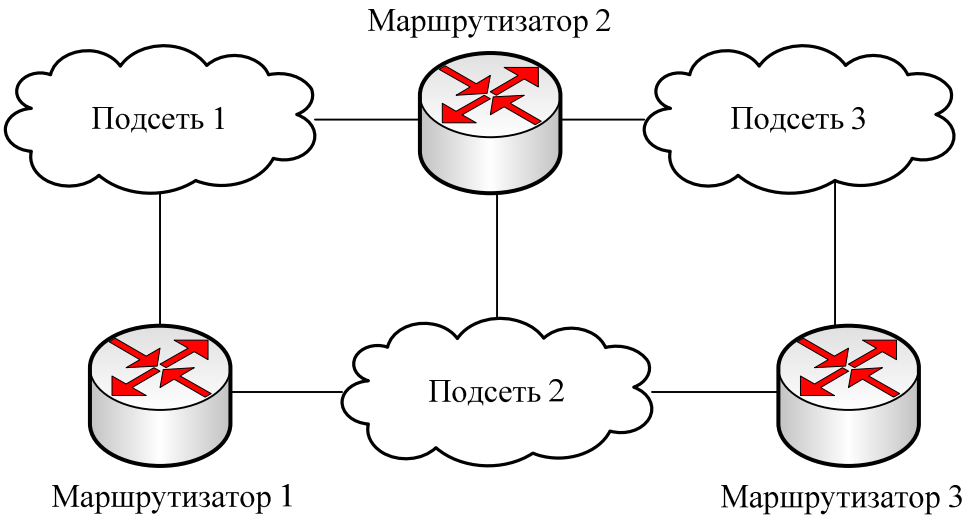


Рис. 5.34. Пример составной сети

Еще одной проблемой является то, что из существующих путей требуется выбрать оптимальный (по времени или по надежности).

В сетях TCP/IP задача маршрутизации решается с помощью специальных устройств – *маршрутизаторов*, которые содержат **таблицы маршрутизации** (routing table). Компьютер с операционной системой Windows Server также может выступать в роли маршрутизатора. Вообще говоря, любой хост, на котором действует стек TCP/IP, имеет свою таблицу маршрутизации (естественно, гораздо меньших размеров, чем на маршрутизаторе).

5.5.2. Таблица маршрутизации

Таблица маршрутизации, создаваемая по умолчанию на компьютере с Windows Server 2003 (одна сетевая карта, IP-адрес: 192.168.1.1, маска подсети: 255.255.255.0), имеет вид, соответствующий *табл. 5.3*.

Таблица 5.3

Таблица маршрутизации

Адрес назначения (Network Destination)	Маска подсети (Netmask)	Шлюз (Gateway)	Интерфейс (Interface)	Метрика (Metric)
0.0.0.0	0.0.0.0	192.168.1.2	192.168.1.1	20
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.1.0	255.255.255.0	192.168.1.1	192.168.1.1	20
192.168.1.1	255.255.255.255	127.0.0.1	127.0.0.1	20
192.168.1.255	255.255.255.255	192.168.1.1	192.168.1.1	20
224.0.0.0	240.0.0.0	192.168.1.1	192.168.1.1	20
255.255.255.255	255.255.255.255	192.168.1.1	192.168.1.1	1

В приведенной таблице имеются следующие поля:

– *адрес назначения* (Network Destination) – адрес хоста или подсети, для которых задан маршрут в таблице;

– *маска подсети* (Netmask) – маска подсети для адреса назначения;

– *шлюз*, *маршрутизатор* (Gateway) – адрес для передачи пакета;

– *интерфейс* (Interface) – адрес собственного порта маршрутизатора (сетевой карты), на который следует передать пакет, при

этом любой маршрутизатор содержит не менее двух портов (в компьютере в роли маршрутизатора с Windows Server портами являются сетевые карты);

– *метрика* (Metric) – число маршрутизаторов (число хопов), которые необходимо пройти для достижения хоста назначения. Для двух маршрутов с одинаковыми адресами назначения выбирается маршрут с наименьшей метрикой. Значение 20 в таблице соответствует 100-мегабитной сети Ethernet.

Кратко опишем записи в таблице по умолчанию:

– 0.0.0.0 – *маршрут по умолчанию* (default route). Эта запись выбирается в случае отсутствия совпадений с адресом назначения. В приведенной таблице маршруту по умолчанию соответствует шлюз 192.168.1.2 – это адрес порта маршрутизатора, который связывает данную подсеть с другими подсетями;

– 127.0.0.0 – *маршрут обратной связи* (loopback address), все пакеты с адресом, начинающимся на 127, возвращаются на узел-источник;

– 192.168.1.0 – адрес собственной подсети узла;

– 192.168.1.1 – собственный адрес узла (совпадает с маршрутом обратной связи);

– 192.168.1.255 – адрес широковещательной рассылки (пакет с таким адресом попадает всем узлам данной подсети);

– 224.0.0.0 – маршрут для групповых адресов;

– 255.255.255.255 – адрес ограниченной широковещательной рассылки.

5.5.3. Принципы маршрутизации в TCP/IP

Рассмотрим, каким образом решается задача *маршрутизации* на примере *составной сети*, показанной на *рис. 5.34*, добавив некоторые подробности – IP-адреса и MAC-адреса узлов (*рис. 5.35*).

Рассмотрим пример выбора маршрутов.

Пример 14. Предположим, что роль маршрутизатора будет выполнять компьютер с ОС Windows Server, который содержит четыре сетевые карты (четыре порта). Каждая карта имеет собственные MAC-адрес и IP-адрес, принадлежащий той подсети, к которой порт подключен.

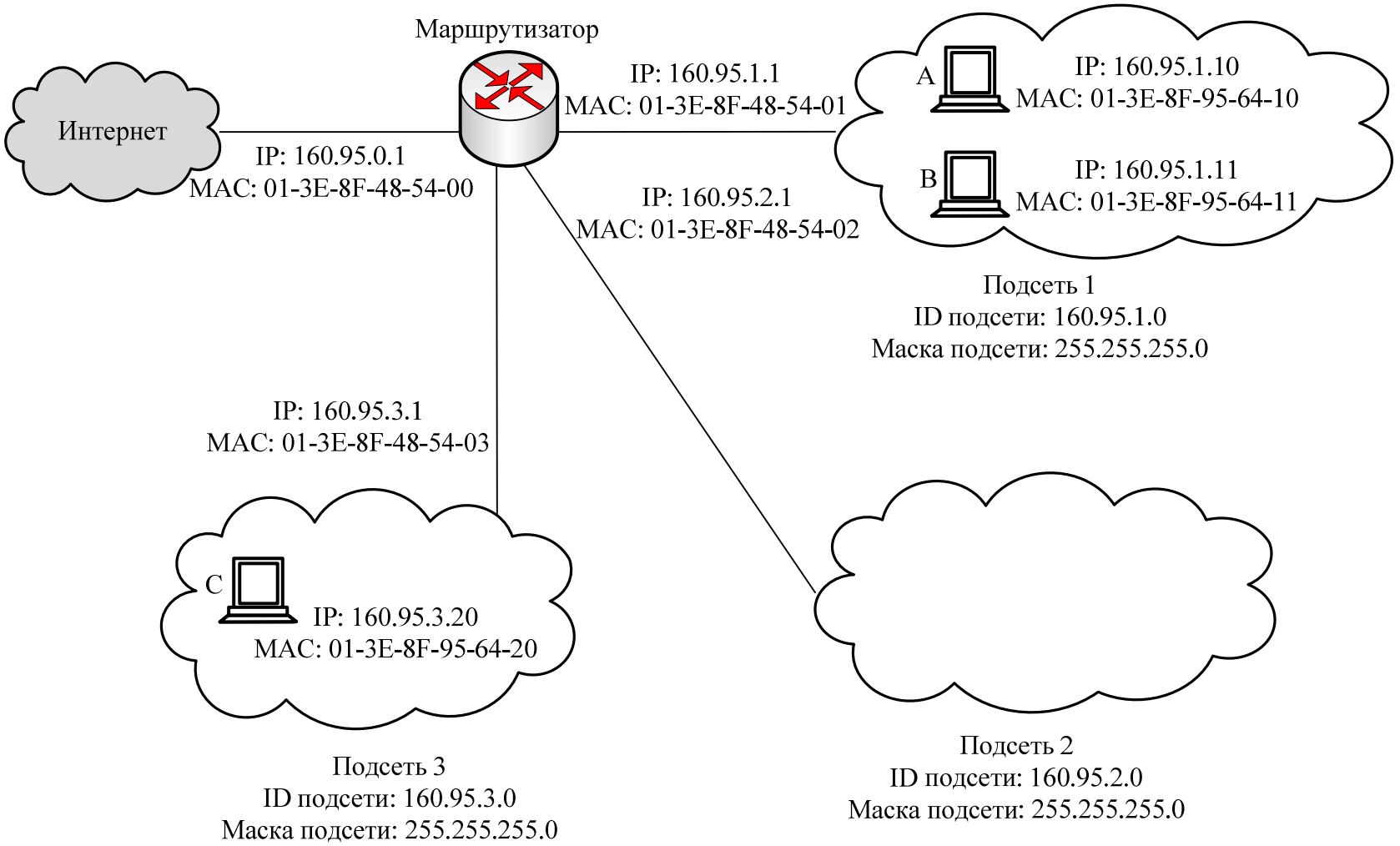


Рис. 5.35. Пример составной сети

Приведем часть таблицы маршрутизации для этого компьютера (*табл. 5.4*).

Таблица 5.4

Таблица маршрутизации сервера с четырьмя сетевыми картами

Адрес назначения (Network Destination)	Маска подсети (Netmask)	Шлюз (Gateway)	Интерфейс (Interface)	Метрика (Metric)
0.0.0.0	0.0.0.0	160.95.0.2	160.95.0.1	20
160.95.0.0	255.255.255.0	160.95.0.1	160.95.0.1	20
160.95.0.1	255.255.255.255	127.0.0.1	127.0.0.1	20
160.95.0.255	255.255.255.255	160.95.0.1	160.95.0.1	20
160.95.1.0	255.255.255.0	160.95.1.1	160.95.1.1	20
160.95.1.1	255.255.255.255	127.0.0.1	127.0.0.1	20
160.95.1.255	255.255.255.255	160.95.1.1	160.95.1.1	20
160.95.2.0	255.255.255.0	160.95.2.1	160.95.2.1	20
160.95.2.1	255.255.255.255	127.0.0.1	127.0.0.1	20
160.95.2.255	255.255.255.255	160.95.2.1	160.95.2.1	20
160.95.3.0	255.255.255.0	160.95.3.1	160.95.3.1	20
160.95.3.1	255.255.255.255	127.0.0.1	127.0.0.1	20
160.95.3.255	255.255.255.255	160.95.3.1	160.95.3.1	20

Будем считать, что пакеты передает хост А. Его таблица маршрутизации может иметь следующий вид (*табл. 5.5*).

Таблица 5.5

Таблица маршрутизации хоста А

Адрес назначения (Network Destination)	Маска подсети (Netmask)	Шлюз (Gateway)	Интерфейс (Interface)	Метрика (Metric)
0.0.0.0	0.0.0.0	160.95.1.1	160.95.1.10	20
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
160.95.1.0	255.255.255.0	160.95.1.10	160.95.1.10	20
160.95.1.10	255.255.255.255	127.0.0.1	127.0.0.1	20
160.95.1.255	255.255.255.255	160.95.1.10	160.95.1.10	20
224.0.0.0	240.0.0.0	160.95.1.10	160.95.1.10	20
255.255.255.255	255.255.255.255	160.95.1.10	160.95.1.10	1

Проанализируем, каким образом будет происходить передача пакетов от хоста А. Возможны три варианта местонахождения получателя:

– подсеть 1 (хост А – хост В);
– подсеть 2 или подсеть 3 (хост А – хост С);
– внешняя сеть (хост А – Интернет).

Если узлом назначения является хост В, пакет не должен попадать на маршрутизатор, так как получатель находится в той же сети, что и отправитель. Хост А ищет в своей таблице маршрутизации подходящий маршрут. При этом для каждой строки на адрес назначения (IP хоста В: 160.95.1.11) накладывается *маска подсети* (операция логического умножения AND) и результат сравнивается с полем Network Destination. Подходящими оказываются два маршрута: 0.0.0.0 и 160.95.1.0. Из них выбирается маршрут с наибольшим числом двоичных единиц – 160.95.1.0, т. е. пакет отправляется непосредственно хосту В. IP-адрес хоста В разрешается с помощью протокола ARP в MAC-адрес. В пересылаемом пакете будет указана следующая информация:

IP-адрес отправителя:	160.95.1.10
MAC-адрес отправителя:	01-3E-8F-95-64-10
IP-адрес получателя:	160.95.1.11
MAC-адрес получателя:	01-3E-8F-95-64-11

Если окажется, что количество единиц совпадает, выбирается маршрут с наименьшей метрикой. Предположим теперь, что узел А отправляет пакет узлу С (подсеть 3). Поиск в собственной таблице маршрутизации не дает подходящих результатов, кроме маршрута по умолчанию – 0.0.0.0. Для этого маршрута указан адрес порта маршрутизатора 160.95.1.1 (default gateway – шлюз по умолчанию). Протокол ARP помогает определить MAC-адрес порта. Именно на него отправляется пакет сначала, причем указывается IP-адрес конечного получателя (узла С):

IP-адрес отправителя:	160.95.1.10
MAC-адрес отправителя:	01-3E-8F-95-64-10
IP-адрес получателя:	160.95.3.20
MAC-адрес получателя:	01-3E-8F-48-54-01

Модуль маршрутизации Windows Server анализирует полученный пакет, выделяет из него адрес узла С, осуществляет поиск в своей таблице маршрутизации (поиск происходит так же, как на хосте А). Находятся две подходящие записи: 160.95.3.0 и 0.0.0.0. Выбирается первый маршрут, так как в нем больше двоичных единиц. Пакет в подсеть 3 отправляется с порта 160.95.3.1:

IP-адрес отправителя:	160.95.1.10
MAC-адрес отправителя:	01-3E-8F-48-54-03
IP-адрес получателя:	160.95.3.20
MAC-адрес получателя:	01-3E-8F-95-64-20

Наконец, в случае, когда хост А осуществляет передачу во внешнюю сеть, пакет сначала попадает на маршрутизатор. Поиск в таблице маршрутизации дает единственный подходящий результат: 0.0.0.0. Поэтому пакет отправляется на порт внешнего маршрутизатора 160.95.0.2. Дальнейшее продвижение пакета выполняют маршрутизаторы Интернета.

5.5.4. Настройка таблиц маршрутизации

Для построения таблиц маршрутизации существует два метода: статический и динамический. *Статический метод* заключается в том, что администратор вручную создает и удаляет записи в таблице. В состав операционной системы Windows Server входит **утилита route**. Она может использоваться с четырьмя командами:

– *print* – печать текущего содержимого таблицы;
– *add* – добавление новой записи;
– *delete* – удаление устаревшей записи;
– *change* – редактирование существующей записи.

Запись должна определяться следующим образом: *<destination> MASK <netmask> <gateway> METRIC <metric> IF <interface>*.

Например, *route add 160.95.1.0 mask 255.255.255.0 160.95.1.1 metric 20 IF 1*.

Кроме того, можно использовать два ключа:

– f – удаление из таблицы всех записей, кроме записей по умолчанию;

– p – создание постоянной записи (т. е. не исчезающей после перезагрузки). По умолчанию создаются временные записи.

Достоинством статического метода является простота. С другой стороны, для сетей с быстро меняющейся конфигурацией этот метод не подходит, так как администратор может не успевать отслеживать все изменения. В этом случае применяют *динамический метод* построения таблицы маршрутизации, основанный на протоколах маршрутизации. В Windows Server реализовано два таких протокола – RIP и OSPF.

5.5.5. Протоколы маршрутизации

Протокол маршрутизации RIP. Маршрутизаторы, работающие по *протоколу RIP* (Routing Information Protocol – *протокол маршрутной информации*), обмениваются содержимым своих таблиц путем групповых рассылок через каждые 30 секунд. Если за 3 минуты не получено никаких сообщений от соседнего маршрутизатора, линия связи между маршрутизаторами считается недоступной. Максимальное число маршрутизаторов, определенное в протоколе RIP – 15. Узлы, находящиеся на большем расстоянии, считаются недоступными.

Так как обмен происходит целыми таблицами, при увеличении числа маршрутизаторов объем трафика сильно возрастает. Поэтому протокол RIP не применяется в крупных сетях.

В Windows Server 2003 реализована вторая версия протокола – RIPv2 (описана в RFC 1723).

Протокол маршрутизации OSPF. Протокол OSPF (Open Shortest Path First – первыми открываются кратчайшие маршруты, описан в RFC 2328) в отличие от RIP может применяться в крупных сетях, так как, во-первых, в процессе обмена информацией о маршрутах передаются не таблицы маршрутизации целиком, а лишь их изменения. Во-вторых, в таблице содержится информация не обо всей сети, а лишь о некоторой ее области. Если адрес назначения отсутствует в таблице, пакет направляется на специальный *пограничный маршрутизатор*, находящийся между областями.

Свое название протокол OSPF получил по алгоритму Дейкстры, лежащему в основе протокола и позволяющему найти наиболее короткий маршрут между двумя узлами сети.

ВЫВОДЫ

1. В стеке TCP/IP используются три типа адресов: физические (MAC-адреса), сетевые (IP-адреса) и символьные имена.

2. Физический, или локальный, адрес узла определяется технологией, с помощью которой построена сеть, в которую входит узел. Для узлов, входящих в локальные сети – это MAC-адрес сетевого адаптера или порта маршрутизатора.

3. IP-адрес действует на сетевом уровне и позволяет объединять разнородные локальные и глобальную сети в единую состав-

ную сеть. Он состоит из 4 байт (октетов), разделенных точками. В его структуре выделяют две части – номер подсети и номер узла. Определение того, какая часть адреса отводится под номер подсети, осуществляется двумя способами – с помощью классов и с помощью масок. В схеме классовой адресации существует пять классов, основными являются классы A, B и C. Поле номера подсети определяется по первым битам адреса. При использовании масок номер подсети находится при помощи логического умножения маски на IP-адрес. Адресация с применением масок является более гибкой по сравнению с классами. Некоторые IP-адреса являются особыми и не используются при адресации конкретных узлов. Это нужно учитывать при назначении IP-адресов.

4. Необходимо отметить, что уже довольно давно возникла проблема дефицита IP-адресов. Решение данной проблемы с помощью масок является временным. Принципиально другой подход заключается в существенном расширении адресного пространства и реализуется в протоколе IPv6.

5. Для преобразования IP-адресов в аппаратные MAC-адреса применяется протокол ARP, для обратного преобразования – протокол RARP. Для диагностики и управления стеком TCP/IP в операционной системе Microsoft Windows Server существуют специальные утилиты – *IPconfig*, *ping*, *tracert*, *netstat*, *arp*, *hostname* и др.

6. В сетях TCP/IP важнейшую задачу выбора наилучшего пути следования пакета данных решают маршрутизаторы на основе таблиц маршрутизации. В таблицы маршрутизации входит информация о номерах и масках подсетей назначения, адресах шлюзов и собственных портов маршрутизатора, а также о метриках. Для адресов, отсутствующих в таблице, применяется специальный адрес – адрес шлюза по умолчанию.

7. Для создания таблиц маршрутизации в Windows Server используют два метода – статический, с помощью утилиты route, и динамический, с применением протоколов маршрутизации RIP и OSPF.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что такое хост?
2. Опишите структуру MAC-адреса.

3. Перечислите виды и приведите примеры адресов, используемых в стеке TCP/IP.
4. Из каких частей состоит IP-адрес?
5. Как определяется номер подсети в IP-адресе?
6. Каков диапазон возможных адресов у сети класса C?
7. Определите номер подсети на основе маски: 116.98.04.39/27.
8. Каковы основные особенности протокола IPv6?
9. Поясните принцип работы протокола ARP.
10. В чем заключается задача маршрутизации?
11. Для чего нужна таблица маршрутизации?
12. Назовите основные поля в таблице маршрутизации.
13. Что такое default gateway?
14. Перечислите ключи утилиты route (приведите примеры).
15. Назовите преимущества и недостатки протокола RIP.
16. Назовите преимущества и недостатки протокола OSPF.
17. Поясните принцип работы утилиты ping (на примерах).
18. Поясните принцип работы утилиты tracert (на примерах).

6. БАЗОВЫЕ ТЕХНОЛОГИИ ЛОКАЛЬНОЙ СЕТИ

За время, прошедшее с появления первых локальных сетей, было разработано несколько сотен самых разных сетевых технологий, однако заметное распространение получили всего несколько сетей, что связано, прежде всего, с поддержкой этих сетей известными фирмами и с высоким уровнем стандартизации принципов их организации.

В настоящее время усиливается тенденция уменьшения числа сетевых технологий. Дело в том, что увеличение скорости передачи в локальных сетях до 100 и даже до 1000 Мбит/с требует применения самых передовых технологий, проведения серьезных и дорогих научных исследований. Естественно, это могут позволить себе только крупнейшие фирмы, которые, конечно же, поддерживают свои стандартные сети и их более совершенные разновидности. К тому же большинство потребителей уже установило у себя какие-то сети и вовсе не желает сразу и полностью заменять все сетевое оборудование на другое, пусть даже в чем-то лучшее. Поэтому в ближайшем будущем вряд ли стоит ожидать принятия принципиально новых стандартов.

В настоящее время стандартные сети обеспечивают широкий диапазон допустимых размеров сети, допустимого количества абонентов сети и, что не менее важно, цен на аппаратуру. Но проблема выбора той или иной сети все равно остается трудноразрешимой.

6.1. Сети Ethernet и Fast Ethernet

6.1.1. Основные характеристики сетей Ethernet

Наибольшее распространение среди стандартных сетей получила сеть **Ethernet**. Впервые она появилась в 1972 году (разработчиком выступила известная фирма Xerox). Сеть оказалась довольно удачной, и вследствие этого в 1980 году ее поддержали такие крупнейшие фирмы, как DEC и Intel (объединение этих фирм, поддерживающих Ethernet, назвали DIX, по первым буквам их

названий). Стараниями этих фирм в 1985 году сеть Ethernet стала международным стандартом, ее приняли крупнейшие международные организации по стандартам: комитет 802 IEEE (Institute of Electrical and Electronic Engineers) и ECMA (European Computer Manufacturers Association).

Стандарт получил название IEEE 802.3. Он определяет *множественный доступ* к моноканалу типа шина с обнаружением конфликтов и контролем передачи, то есть с уже упоминавшимся методом доступа CSMA/CD. Вообще-то надо сказать, что этому стандарту удовлетворяют и некоторые другие сети, так как он не очень сильно детализирован. В результате сети стандарта IEEE 802.3 нередко несовместимы между собой как по конструктивным, так и по электрическим характеристикам.

Основные характеристики стандарта IEEE 802.3: топология – шина; среда передачи – коаксиальный кабель; скорость передачи – 10 Мбит/с; максимальная длина – 5 км; максимальное количество абонентов – до 1024; длина сегмента сети – до 500 м; количество абонентов на одном сегменте – до 100; метод доступа – CSMA/CD; передача узкополосная, то есть без модуляции (моноканал).

Строго говоря, между стандартами IEEE 802.3 и Ethernet существуют небольшие отличия. Сеть Ethernet сейчас наиболее популярна в мире (более 80% рынка), и нет сомнения, что таковой она и останется в ближайшие годы. Этому в немалой степени способствовало то, что с самого начала все характеристики, параметры, протоколы сети были открыты для всех, в результате чего огромное число производителей во всем мире стало выпускать аппаратуру Ethernet, полностью совместимую между собой.

В классической сети Ethernet применяется 50-омный коаксиальный кабель двух видов (толстый и тонкий). Однако с начала 90-х годов XX века все большее распространение получает версия Ethernet, использующая в качестве среды передачи витые пары. Определен также стандарт для применения в сети оптоволоконного кабеля. В стандарты были внесены соответствующие добавления.

В 1995 году появился стандарт на более быструю версию Ethernet, работающую на скорости 100 Мбит/с (так называемый Fast Ethernet, стандарт IEEE 802.3u), использующую в качестве среды передачи витую пару или оптоволоконный кабель. Появилась и версия на скорость 1000 Мбит/с (Gigabit Ethernet, стандарт IEEE 802.3z).

Помимо стандартной топологии шина применяются также топологии типа *пассивная звезда* и *пассивное дерево*. При этом предполагается использование репитеров и пассивных (репитерных) концентраторов, соединяющих между собой различные части (сегменты) сети (*рис. 6.1*).

В качестве сегмента может также выступать единичный абонент. Коаксиальный кабель используется для шинных сегментов, а витая пара и оптоволоконный кабель – для лучей пассивной звезды (для присоединения к концентратору одиночных компьютеров). Главное – чтобы в полученной в результате топологии не было замкнутых путей (*петель*). Фактически получается, что абоненты соединены в физическую шину, так как сигнал от каждого из них распространяется сразу во все стороны и не возвращается назад (как в кольце). Максимальная длина кабеля всей сети в целом (максимальный путь сигнала) теоретически может достигать 6,5 км, но практически не превышает 2,5 км.

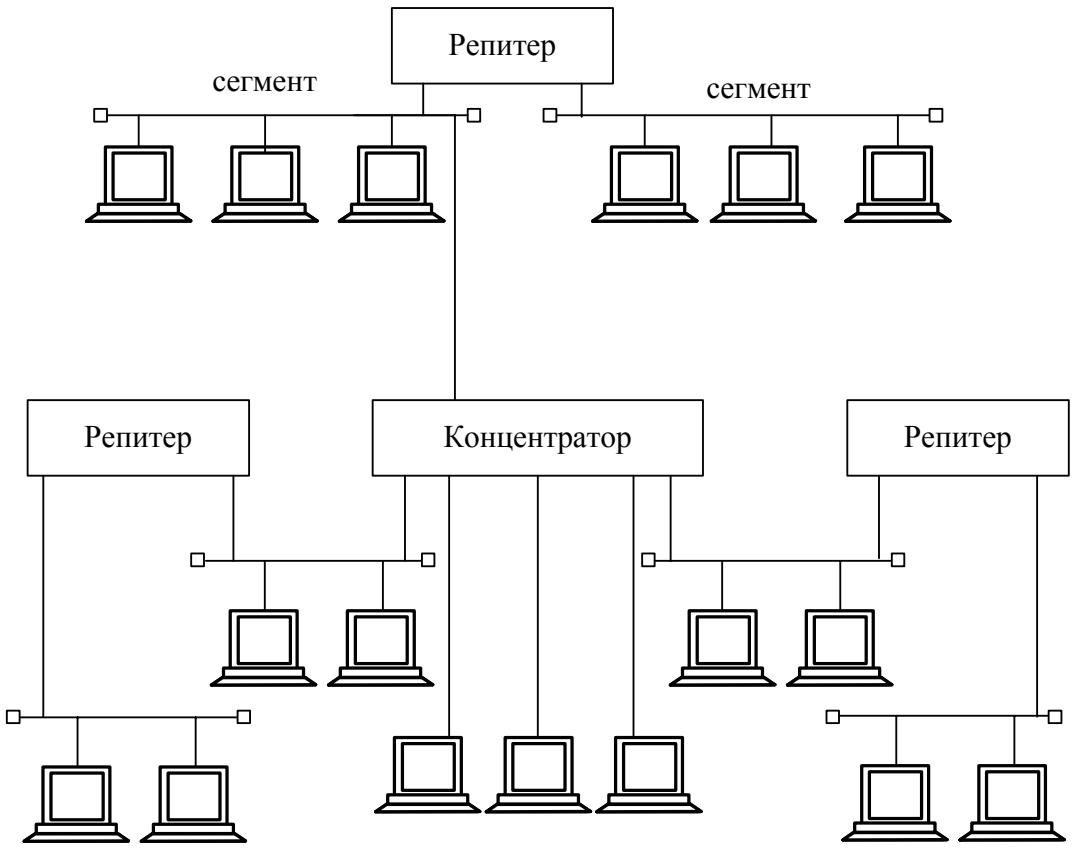


Рис. 6.1. Топология сети Ethernet

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

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

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

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

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

– 100BASE-T4 (счетверенная витая пара);
– 100BASE-TX (сдвоенная витая пара);
– 100BASE-FX (оптоволоконный кабель).

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

Отметим, что сеть Ethernet не отличается ни рекордными характеристиками, ни оптимальными алгоритмами, она уступает по ряду параметров другим стандартным сетям. Но благодаря мощной поддержке, высочайшему уровню стандартизации, огромным объемам выпуска технических средств, Ethernet резко выделяется среди других стандартных сетей, и поэтому любую другую сетевую технологию принято сравнивать именно с Ethernet.

Для передачи информации в сети Ethernet применяется стандартный код Манчестер-II. При этом один уровень сигнала нулевой, а другой – отрицательный, то есть постоянная составляющая сигнала не равна нулю. При отсутствии передачи потенциал в сети нулевой. Гальваническая развязка осуществляется аппаратурой адаптеров, репитеров и концентраторов. При этом приемопередатчик сети гальванически развязан от остальной аппаратуры с помощью трансформаторов и изолированного источника питания, а с кабелем сети соединен напрямую.

6.1.2. Структура пакета в сетях Ethernet

Доступ к сети Ethernet осуществляется по случайному методу CSMA/CD, обеспечивающему полное равноправие абонентов. В сети используются пакеты переменной длины со структурой, представленной на *рис. 6.2*. Длина кадра Ethernet (то есть пакета без преамбулы) должна быть не менее 512 битовых интервалов, или 51,2 мкс (именно такова предельная величина двойного времени прохождения в сети). Предусмотрена *индивидуальная*, *групповая* и *широковещательная адресация*.

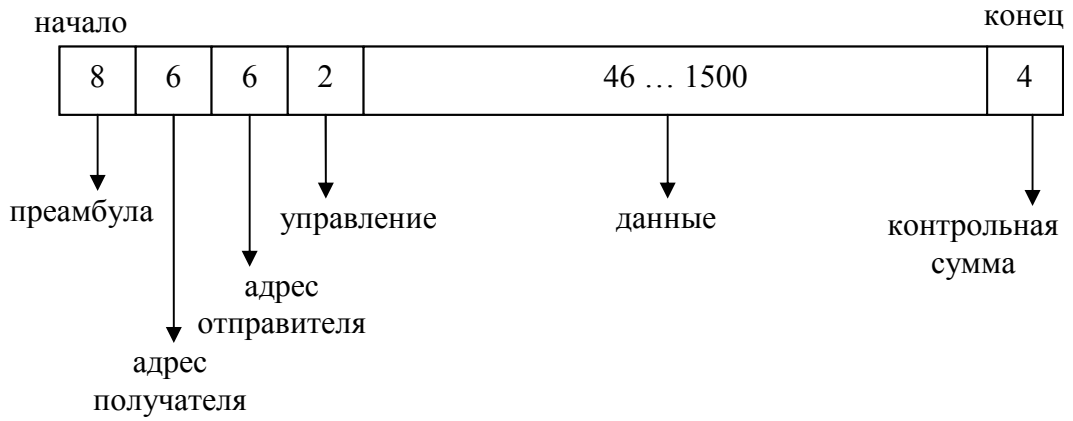


Рис. 6.2. Структура пакета сети Ethernet
(указано число байт каждого поля)

В пакет Ethernet входят следующие поля.

1. *Преамбула* состоит из 8 байт, первые семь из которых представляют собой код 10101010, а последний восьмой – код 10101011. В стандарте IEEE 802.3 этот последний байт называется **признаком начала кадра** (Start of Frame Delimiter, SFD) и образует отдельное поле пакета.

2. *Адрес получателя* (приемника) и *адрес отправителя* (передатчика) включают по 6 байт. Эти адресные поля обрабатываются аппаратурой абонентов.

3. *Поле управления* (L/T – Length/Type) содержит информацию о длине поля данных. Оно может также определять тип используемого протокола. Принято считать, что если значение этого поля не больше 1500, то оно определяет длину поля данных. Если же его значение больше 1500, то оно определяет тип кадра. Поле управления обрабатывается программно.

4. *Поле данных* должно включать в себя от 46 до 1500 байт данных. Если пакет должен содержать менее 46 байт данных, то поле данных дополняется байтами заполнения. Согласно стандарту IEEE 802.3 в структуре пакета выделяется специальное поле заполнения (pad data – незначащие данные), которое может иметь нулевую длину, когда данных достаточно (больше 46 байт).

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

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

На практике в сетях Ethernet на канальном уровне используются кадры 4 различных форматов (типов).

Один и тот же тип кадра может иметь разные названия, поэтому ниже для каждого типа кадра приведено по нескольку наиболее употребительных названий:

– кадр 802.3/LLC (кадр 802.3/802.2 или кадр Novell 802.2);
– кадр Raw 802.3 (или кадр Novell 802.3);
– кадр Ethernet DIX (или кадр Ethernet II);
– кадр Ethernet SNAP.

Выводы

1. Ethernet в настоящее время является самой распространенной технологией локальных сетей. В широком смысле Ethernet – это целое семейство технологий, из которых в наши дни на практике в основном применяются высокоскоростные технологии Fast Ethernet и Gigabit Ethernet. Почти все виды технологий Ethernet используют один и тот же метод разделения среды передачи данных – метод случайного доступа CSMA/CD с прослушиваем несущей, который определяет облик технологии в целом.

2. Важным явлением в сетях Ethernet является коллизия – ситуация, когда две станции одновременно пытаются передать кадр данных по общей среде. Возможность четкого распознавания коллизий обусловлена правильным выбором параметров сети, в частности, соблюдением соотношения между минимальной длиной кадра и максимально возможным размером сети.

3. Практически доказано, что максимально возможная пропускная способность сегмента Ethernet в кадрах в секунду достигается при передаче кадров минимальной длины.

4. Технология Ethernet поддерживает 4 разных типа кадров, которые имеют общий формат адресов узлов. Существуют формальные признаки, по которым сетевые адаптеры автоматически распознают тип кадра.

5. В зависимости от типа физической среды стандарт IEEE 802.3 определяет различные спецификации: 10Base-5, 10Base-2, 10Base-T, 10Base-FL, 10Base-FX и т. д. Для каждой спецификации определяются тип кабеля, максимальные длины непрерывных отрезков кабеля, а также правила использования повторителей для увеличения размера сети.

6.2. Сеть Token Ring

6.2.1. Основные характеристики сетей Token Ring

Сеть **Token Ring** предложена фирмой IBM в 1985 году (первый вариант появился в 1980 году). Назначением сети является объединение в сеть всех типов компьютеров, выпускаемых IBM (от персональных до больших). Уже тот факт, что ее поддерживает фирма IBM, крупнейший производитель компьютерной техники,

говорит о том, что ей необходимо уделить особое внимание. Но не менее важно и то, что Token Ring является в настоящее время международным стандартом IEEE 802.5. Это ставит данную сеть на один уровень по статусу с Ethernet.

По сравнению с аппаратурой Ethernet аппаратура Token Ring оказывается заметно дороже, так как использует более сложные методы управления обменом, поэтому распространена сеть Token Ring значительно меньше. Однако ее применение становится оправданным, когда требуются большие интенсивности обмена (например, при связи с большими компьютерами) и ограниченное время доступа.

Сеть Token Ring имеет топологию кольцо, хотя внешне она больше напоминает звезду. Это связано с тем, что отдельные абоненты (компьютеры) присоединяются к сети не напрямую, а через специальные *концентраторы,* или *многостанционные устройства доступа* (MSAU, или MAU – Multistation Access Unit). Поэтому физически сеть образует *звездно-кольцевую топологию* (*рис. 6.3*).

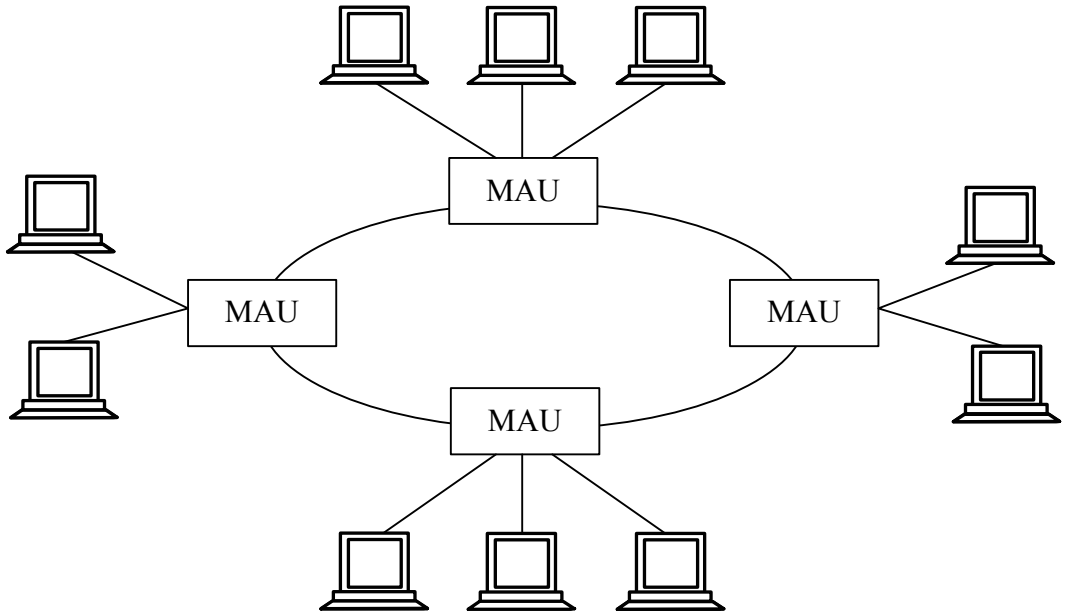


Рис. 6.3. Звездно-кольцевая топология сети Token Ring

В действительности же абоненты объединяются все-таки в кольцо, то есть каждый из них передает информацию одному соседнему абоненту, а принимает информацию от другого соседнего абонента.

Концентратор (MAU) при этом только позволяет централизовать задание конфигурации, отключение неисправных абонентов, контроль за работой сети и т. д. (*рис. 6.4*).

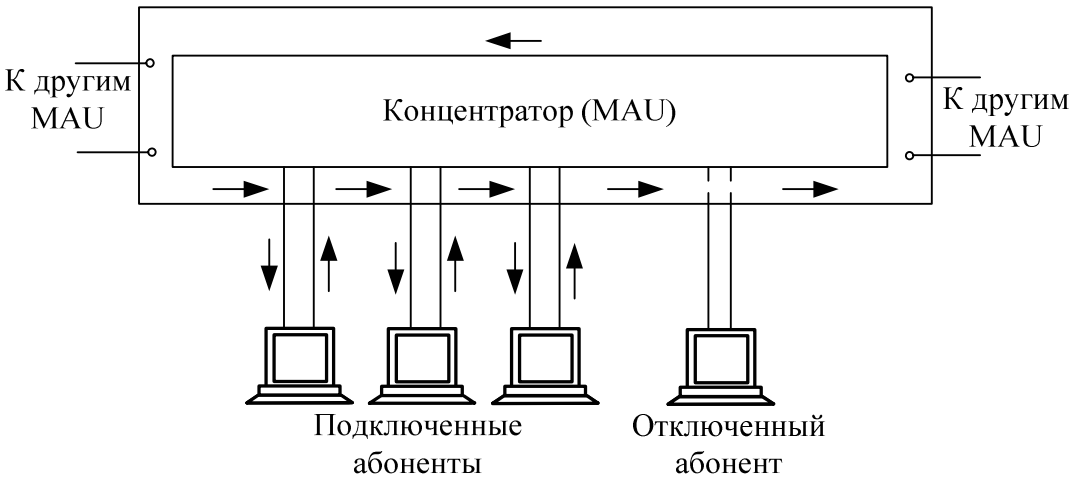


Рис. 6.4. Соединение абонентов сети Token Ring в кольцо с помощью концентратора (MAU)

Для присоединения кабеля к концентратору применяются специальные разъемы, которые обеспечивают постоянство замкнутости кольца даже при отключении абонента от сети. Концентратор в сети может быть и единственным – в кольцо замыкаются только абоненты, подключенные к нему.

В каждом кабеле, соединяющем адаптеры и концентратор (*адаптерные кабели*, adapter cable), находятся на самом деле две разнонаправленные линии связи. Такими же двумя разнонаправленными линиями связи, входящими в *магистральный кабель* (path cable), объединяются между собой в кольцо различные концентраторы (*рис. 6.5*), хотя для этой же цели может также использоваться и единственная однонаправленная линия связи (*рис. 6.6*).

Конструктивно концентратор представляет собой автономный блок с восемью разъемами для подключения абонентов (компьютеров) с помощью адаптерных кабелей и двумя (крайними) разъемами для подключения к другим концентраторам с помощью специальных магистральных кабелей.

Несколько концентраторов могут конструктивно объединяться в группу, ***кластер*** (cluster), внутри которой абоненты также соединены в единое кольцо. Применение кластеров позволяет увеличивать количество абонентов, подключенных к одному центру.

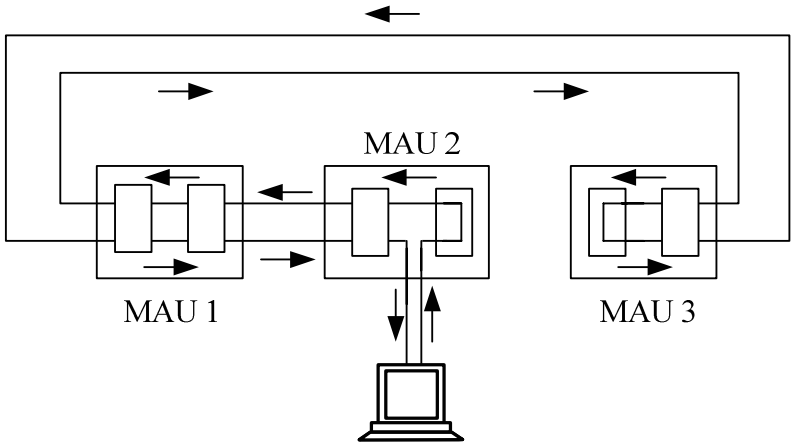


Рис. 6.5. Объединение концентраторов двунаправленной линией связи

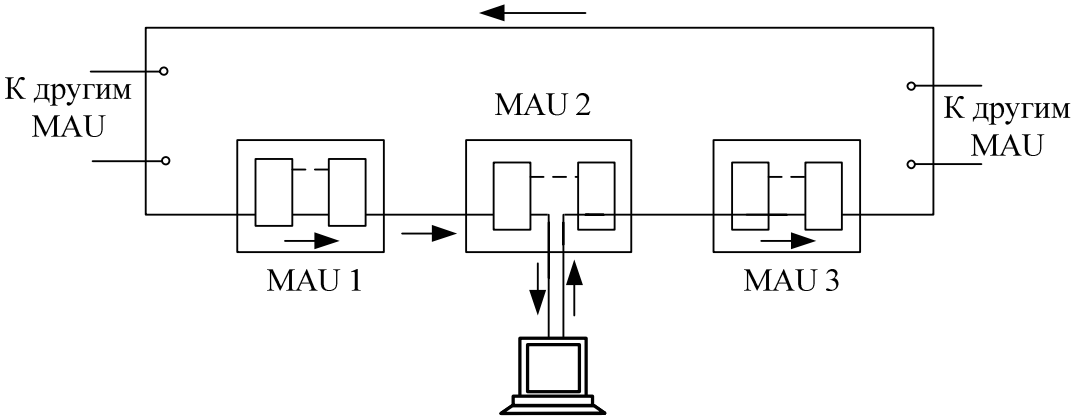


Рис. 6.6. Объединение концентраторов однонаправленной линией связи

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

Основные технические характеристики сети Token Ring следующие:

– максимальное количество концентраторов типа IBM 8228 MAU-12;

– максимальное количество абонентов в сети – 96;

– максимальная длина кабеля между абонентом и концентратором – 45 м;

– максимальная длина кабеля между концентраторами – 45 м;

– максимальная длина кабеля, соединяющего все концентраторы – 120 м;

– скорость передачи данных – 4 Мбит/с и 16 Мбит/с.

Все приведенные характеристики относятся к случаю неэкранированной витой пары. В случае применения другой среды передачи характеристики сети могут отличаться. Например, при использовании экранированной витой пары количество абонентов может быть увеличено до 200 (вместо 96), длина кабеля – до 100 м (вместо 45), количество концентраторов – до 33, а полная длина кольца, соединяющего концентраторы – до 200 м. Оптоволоконный кабель позволяет увеличивать длину кабеля до 1 км.

Как видим, сеть Token Ring уступает сети Ethernet как по допустимому размеру сети, так и по максимальному количеству абонентов. Что касается скорости передачи, то в настоящее время разработаны версии Token Ring со скоростью 100 Мбит/с и 1000 Мбит/с.

Для передачи информации в Token Ring используется вариант кода Манчестер-II. Как и в любой звездообразной топологии, никаких дополнительных мер по электрическому согласованию и внешнему заземлению не требуется.

Для присоединения кабеля к сетевому адаптеру используется внешний 9-контактный разъем типа DIN. Также, как и адаптеры Ethernet, адаптеры Token Ring имеют на своей плате переключатели или перемычки для настройки адресов и прерываний системной шины. Если сеть Ethernet можно построить только на адаптерах и кабеле, то для сети Token Ring обязательно нужно приобретать концентраторы. Это также увеличивает стоимость аппаратуры Token Ring.

В то же время в отличие от Ethernet сеть Token Ring лучше «держит» большую нагрузку (больше 30~40%) и обеспечивает гарантированное время доступа. Это крайне необходимо, например в сетях производственного назначения, в которых задержка реакции на внешнее событие может привести к серьезным последствиям.

В сетях с маркерным методом доступа (а к ним, кроме сетей Token Ring, относятся сети FDDI, а также сети, близкие к стандарту 802.4, ArcNet, сети производственного назначения MAP) право на доступ к среде передается циклически от станции к станции по логическому кольцу.

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. Для обеспечения доступа станций к физической среде по кольцу циркулирует кадр специального формата и назначения – *маркер*. В сети Token Ring любая станция всегда непосредственно получает данные только от одной станции – той, которая является предыдущей в кольце.

Такая станция называется ***ближайшим активным соседом***, расположенным выше по потоку (данных) – Nearest Active Upstream Neighbour, NAUN. Передачу же данных станция всегда осуществляет своему ближайшему соседу вниз по потоку данных.

Получив маркер, станция анализирует его и при отсутствии у нее данных для передачи обеспечивает его продвижение к следующей станции. Станция, которая имеет данные для передачи, при получении маркера изымает его из кольца, что дает ей право доступа к физической среде и передачи своих данных. Затем эта станция выдает в кольцо кадр данных установленного формата последовательно по битам. Переданные данные проходят по кольцу всегда в одном направлении от одной станции к другой. Кадр снабжен адресом назначения и адресом источника.

Все станции кольца ретранслируют кадр побитно, как повторители. Если кадр проходит через станцию назначения, то, распознав свой адрес, эта станция копирует кадр в свой внутренний буфер и вставляет в кадр признак подтверждения приема. Станция, выдавшая кадр данных в кольцо, при обратном его получении с подтверждением приема изымает этот кадр из кольца и передает в сеть новый маркер для обеспечения возможности другим станциям сети передавать данные. Такой алгоритм доступа применяется в сетях Token Ring со скоростью работы 4 Мбит/с, описанных в стандарте 802.5.

Время владения разделяемой средой в сети Token Ring ограничивается временем удержания маркера (token holding time), 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. Обычно время удержания маркера по умолчанию равно 10 мс, а максимальный размер кадра в стандарте 802.5 не определен. Для

сетей 4 Мбит/с он обычно равен 4 Кбайт, а для сетей 16 Мбит/с – 16 Кбайт. Это связано с тем, что за время удержания маркера станция должна успеть передать хотя бы один кадр. При скорости 4 Мбит/с за время 10 мс можно передать 5000 байт, а при скорости 16 Мбит/с – соответственно 20 000 байт. Максимальные размеры кадра выбраны с некоторым запасом.

В сетях Token Ring 16 Мбит/с используется также несколько другой 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, так как по нему одновременно продвигаются кадры нескольких станций. Тем не менее, свои кадры в каждый момент времени может генерировать только одна станция, которая в данный момент владеет маркером доступа. Остальные станции в это время только повторяют чужие кадры, так что принцип разделения кольца во времени сохраняется, ускоряется только процедура передачи владения кольцом.

Для различных видов сообщений могут назначаться различные приоритеты: от 0 (низший) до 7 (высший). Решение о приоритете конкретного кадра принимает передающая станция (протокол Token Ring получает этот параметр через межуровневые интерфейсы от протоколов верхнего уровня, например, прикладного). Маркер также всегда имеет некоторый уровень текущего приоритета. Станция имеет право захватить переданный ей маркер только в том случае, если приоритет кадра, который она хочет передать, выше (или равен) приоритета маркера. В противном случае станция обязана передать маркер следующей по кольцу станции.

За наличие в сети маркера, причем единственной его копии, отвечает *активный монитор*. Если активный монитор не получает маркер в течение длительного времени, он порождает новый маркер.

6.2.2. Форматы кадров Token Ring

В Token Ring существуют три различных формата кадров:

- маркер;
- кадр данных;
- прерывающая последовательность.

Кадр *маркера* состоит из трех полей, каждое длиной в один байт.

Начальный ограничитель (Start Delimiter, SD) появляется в начале маркера, а также в начале любого кадра, проходящего по сети. Поле представляет собой следующую уникальную последовательность символов манчестерского кода: JKOJKOOO. Поэтому начальный ограничитель нельзя спутать ни с какой битовой последовательностью внутри кадра.

Управление доступом (Access Control) состоит из четырех подполей: PPP, T, M и RRR, где PPP – биты приоритета, T – бит маркера, *M* – бит монитора, *RRR* – резервные биты приоритета. Бит T, установленный в 1, указывает на то, что данный кадр является маркером доступа. Бит монитора устанавливается в 1 активным монитором и в 0 любой другой станцией, передающей маркер или кадр. Если активный монитор видит маркер или кадр, содержащий бит монитора со значением 1, то активный монитор «знает», что этот кадр или маркер уже однажды обошел кольцо и не был обработан станциями. Если это кадр, то он удаляется из кольца. Если это маркер, то активный монитор передает его дальше по кольцу. Использование полей приоритетов будет рассмотрено ниже.

Конечный ограничитель (End Delimeter, ED) – последнее поле маркера. Также, как и поле начального ограничителя, это поле содержит уникальную последовательность манчестерских кодов JK1JK1, а также два однобитовых признака: I и E. Признак I (Intermediate) показывает, является ли кадр последним в серии кадров (1-0) или промежуточным (1-1). Признак E (Error) – это признак ошибки. Он устанавливается в 0 станцией-отправителем, и любая станция кольца, через которую проходит кадр, должна установить этот признак в 1, если она обнаружит ошибку по контрольной сумме или другую некорректность кадра.

Кадр данных и прерывающая последовательность. Кадр данных включает те же три поля, что и маркер, и имеет кроме них еще несколько дополнительных полей. Таким образом, кадр данных состоит из следующих полей:

- начальный ограничитель (Start Delimiter, SD);
- управление кадром (Frame Control, PC);
- адрес назначения (Destination Address, DA);
- адрес источника (Source Address, SA);
- данные (INFO);

– контрольная сумма (Frame Check Sequence, PCS);
– конечный ограничитель (End Delimeter, ED);
– статус кадра (Frame Status, FS).

Кадр *данных* может переносить либо служебные данные для управления кольцом (данные MAC-уровня), либо пользовательские данные (LLC-уровня). Стандарт Token Ring определяет 6 типов управляющих кадров MAC-уровня. Поле FC определяет тип кадра (MAC или LLC), и если он определен как MAC, то поле также указывает, какой из шести типов кадров представлен данным кадром.

Чтобы удостовериться, что ее адрес уникальный, станция, когда впервые присоединяется к кольцу, посылает кадр *Тест дублирования адреса* (Duplicate Address Test, DAT).

Чтобы сообщить другим станциям, что он работоспособен, активный монитор периодически посылает в кольцо кадр *Существует активный монитор* (Active Monitor Present, AMP).

Кадр *Существует резервный монитор* (Standby Monitor Present, SMP) отправляется любой станцией, не являющейся активным монитором.

Резервный монитор отправляет кадр *Маркер заявки* (Claim Token, CT), когда подозревает, что активный монитор отказал, затем резервные мониторы «договариваются» между собой, какой из них станет новым активным монитором.

Станция отправляет кадр *Сигнал* (Beacon, BCN) в случае возникновения серьезных сетевых проблем, таких как обрыв кабеля, обнаружение станции, передающей кадры без ожидания маркера, выход станции из строя. Определяя, какая станция отправляет кадр сигнала, диагностирующая программа (ее существование и функции не определяются стандартами Token Ring) может локализовать проблему. Каждая станция периодически передает кадры BCN до тех пор, пока не примет кадр BCN от своего предыдущего (NAUN) соседа. В результате в кольце только одна станция продолжает передавать кадры BCN – та, у которой есть проблемы с предыдущим соседом. В сети Token Ring каждая станция знает MAC-адрес своего предыдущего соседа, поэтому Beacon-процедура приводит к выявлению адреса некорректно работающей станции.

Кадр *Очистка* (Purge, PRG) используется новым активным монитором для того, чтобы перевести все станции в исходное состояние и очистить кольцо от всех ранее посланных кадров.

В стандарте 802.5 используются адреса той же структуры, что и в стандарте 802.3. Адреса назначения и источника могут иметь длину либо 2, либо 6 байт. Первый бит адреса назначения определяет групповой или индивидуальный адрес как для 2-байтовых, так и для 6-байтовых адресов. Второй бит в 6-байтовых адресах говорит о том, назначен адрес локально или глобально. Адрес, состоящий из всех единиц, является широковещательным.

Адрес источника имеет тот же размер и формат, что и адрес назначения. Однако признак группового адреса используется в нем особым способом. Так как адрес источника не может быть групповым, то наличие единицы в этом разряде говорит о том, что в кадре имеется специальное поле маршрутной информации (Routing Information Field, RIF). Эта информация требуется при работе мостов, связывающих несколько колец Token Ring, в режиме маршрутизации от источника.

Поле данных INFO кадра может содержать данные одного из описанных управляющих кадров уровня MAC или пользовательские данные, упакованные в кадр уровня LLC. Это поле, как уже отмечалось, не имеет определенной стандартом максимальной длины, хотя существуют практические ограничения на его размер, основанные на временных соотношениях между временем удержания маркера и временем передачи кадра.

Поле статуса FS имеет длину 1 байт и содержит 4 резервных бита и 2 подполя: бит распознавания адреса A и бит копирования кадра C. Так как это поле не сопровождается вычисляемой суммой CRC, то используемые биты для надежности дублируются: поле статуса FS имеет вид ACxxACxx. Если бит распознавания адреса не установлен во время получения кадра, это означает, что станция назначения больше не присутствует в сети (возможно, вследствие неполадок, а возможно, станция находится в другом кольце, связанном с данным с помощью моста). Если оба бита опознавания адреса и копирования кадра установлены и бит обнаружения ошибки также установлен, то исходная станция знает, что ошибка случилась после того, как этот кадр был корректно получен.

Прерывающая последовательность состоит из двух байтов, содержащих начальный и конечный ограничители. Прерывающая последовательность может появиться в любом месте потока битов и сигнализирует о том, что текущая передача кадра или маркера отменяется.

6.2.3. Приоритетный доступ к кольцу

Каждый кадр данных или маркер имеет приоритет, устанавливаемый битами приоритета (значение от 0 до 7, причем 7 – наивысший приоритет).

Станция может воспользоваться маркером, если только у нее есть кадры для передачи с приоритетом равным или большим, чем приоритет маркера. Сетевой адаптер станции с кадрами, у которых приоритет ниже, чем приоритет маркера, не может захватить маркер, но может поместить наибольший приоритет своих ожидающих передачи кадров в резервные биты маркера, но только в том случае, если записанный в резервных битах приоритет ниже его собственного. В результате в резервных битах приоритета устанавливается наивысший приоритет станции, которая пытается получить доступ к кольцу, но не может этого сделать из-за высокого приоритета маркера.

Станция, сумевшая захватить маркер, передает свои кадры с приоритетом маркера, а затем передает маркер следующему соседу. При этом она переписывает значение резервного приоритета в поле приоритета маркера, а резервный приоритет обнуляется. Поэтому при следующем проходе маркера по кольцу его захватит станция, имеющая наивысший приоритет. При инициализации кольца основной и резервный приоритет маркера устанавливаются в 0. Хотя механизм приоритетов в технологии Token Ring имеется, он начинает работать только в том случае, когда приложение или прикладной протокол решают его использовать. Иначе все станции будут иметь равные права доступа к кольцу, что в основном и происходит на практике, так как большая часть приложений этим механизмом не пользуется. Это связано с тем, что приоритеты кадров поддерживаются не во всех технологиях, например, в сетях Ethernet они отсутствуют, поэтому приложение будет вести себя по-разному, в зависимости от технологии нижнего уровня, что нежелательно. В современных сетях приоритетность обработки кадров обычно обеспечивается коммутаторами или маршрутизаторами, которые поддерживают их независимо от используемых протоколов канального уровня.

6.2.4. Физический уровень технологии Token Ring

Стандарт Token Ring фирмы IBM изначально предусматривал построение связей в сети с помощью концентраторов, называемых

MAU (Multistation Access Unit, активный концентратор) или MSAU (Multistation Access Unit, пассивный концентратор), то есть устройств многостанционного доступа. 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. Ни усиление сигналов, ни их ресинхронизацию пассивный MSAU не выполняет. Такое устройство можно считать простым кроссовым блоком за одним исключением – MSAU обеспечивает обход какого-либо порта, когда присоединенный к этому порту компьютер выключают. Такая функция необходима для обеспечения связности кольца вне зависимости от состояния подключенных компьютеров. Обычно обход порта выполняется за счет релейных схем, которые питаются постоянным током от сетевого адаптера, а при выключении сетевого адаптера нормально замкнутые контакты реле соединяют вход порта с его выходом.

Активный концентратор выполняет функции регенерации сигналов и поэтому иногда называется повторителем, как в стандарте Ethernet.

Возникает вопрос: если концентратор является пассивным устройством, то каким образом обеспечивается качественная передача сигналов на большие расстояния, которые возникают при включении в сеть нескольких сот компьютеров? Ответ состоит в том, что роль усилителя сигналов в этом случае берет на себя каждый сетевой адаптер, а роль ресинхронизирующего блока выполняет сетевой адаптер активного монитора кольца. Каждый сетевой адаптер Token Ring имеет блок повторения, который умеет регенерировать и ресинхронизировать сигналы, однако последнюю функцию выполняет в кольце только блок повторения активного монитора.

Блок ресинхронизации состоит из 30-битного буфера, который принимает манчестерские сигналы с несколько искаженными за время оборота по кольцу интервалами следования. При максимальном количестве станций в кольце (260) вариация задержки циркуляции бита по кольцу может достигать 3-битовых интервалов. Активный монитор «вставляет» свой буфер в кольцо и синхронизирует битовые сигналы, выдавая их на выход с требуемой частотой.

В общем случае сеть Token Ring имеет комбинированную звездно-кольцевую конфигурацию. Конечные узлы подключаются к MSAU по топологии звезды, а сами MSAU объединяются через специальные порты Ring In (RI) и Ring Out (RO) для образования магистрального физического кольца.

Все станции в кольце должны работать на одной скорости – либо 4 Мбит/с, либо 16 Мбит/с. Кабели, соединяющие станцию с концентратором, называются ответвительными (lobe cable), а кабели, соединяющие концентраторы – магистральными (trunk cable).

Технология Token Ring позволяет использовать для соединения конечных станций и концентраторов различные типы кабеля: STP Type I, 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.

Расстояние между пассивными MSAU может достигать 100 м при использовании кабеля STP Type 1 и 45 м при использовании кабеля UTP Type 3. Между активными MSAU максимальное расстояние увеличивается соответственно до 730 м или 365 м в зависимости от типа кабеля.

Максимальная длина кольца Token Ring составляет 4000 м. Ограничения на максимальную длину кольца и количество станций в кольце в технологии Token Ring не являются такими жесткими, как в технологии Ethernet. Здесь эти ограничения во многом связаны со временем оборота маркера по кольцу (но не только – есть и другие соображения, диктующие выбор ограничений). Так, если кольцо состоит из 260 станций, то при времени удержания маркера в 10 мс маркер вернется в активный монитор в худшем случае через 2,6 с, а это время как раз составляет таймаут контроля оборота маркера. В принципе, все значения таймаутов в сетевых адаптерах узлов сети Token Ring можно настраивать, поэтому можно построить сеть Token Ring с большим количеством станций и с большей длиной кольца.

Существует большое разнообразие аппаратуры для сетей Token Ring, которое улучшает некоторые стандартные характеристики

этих сетей: максимальную длину сети, расстояние между концентраторами, надежность (путем использования двойных колец).

Компания IBM предложила новый вариант технологии Token Ring, названный High-Speed Token Ring, HSTR. Эта технология поддерживает битовые скорости в 100 и 155 Мбит/с, сохраняя основные особенности технологии Token Ring 16 Мбит/с.

Выводы

1. В сетях Token Ring используется маркерный метод доступа, который гарантирует каждой станции получение доступа к разделяемому кольцу в течение времени оборота маркера. Из-за этого свойства метод иногда называют детерминированным. Метод доступа основан на приоритетах, причем станция сама определяет приоритет текущего кадра и может захватить кольцо только в том случае, если в сети нет более приоритетных кадров.

2. Современные сети Token Ring работают на скоростях до 1000 Мбит/с и могут использовать в качестве физической среды экранированную и неэкранированную витую пару, а также волоконно-оптический кабель. Максимальное количество станций в кольце – 260, а максимальная длина кольца – 4 км. Максимальный размер поля данных кадра Token Ring зависит от скорости работы кольца. Минимальный размер поля данных кадра не определен.

3. Технология Token Ring обладает элементами отказоустойчивости. За счет обратной связи кольца одна из станций – активный монитор – непрерывно контролирует наличие маркера, а также время оборота маркера и кадров данных. При некорректной работе кольца запускается процедура его повторной инициализации, а если она не помогает, то для локализации неисправного участка кабеля или неисправной станции используется процедура beaconing.

4. В сети Token Ring станции в кольцо объединяют с помощью концентраторов, называемых MSAU. Пассивный концентратор MSAU выполняет роль кроссовой панели, которая соединяет выход предыдущей станции в кольце со входом последующей. Максимальное расстояние от станции до MSAU – 100 м для STP и 45 м для UTP.

5. Сеть Token Ring может строиться на основе нескольких колец, разделенных мостами, маршрутизирующими кадры по принципу «от источника», для чего в кадр Token Ring добавляется специальное поле с маршрутом прохождения колец.

6.3. Сети FDDI

6.3.1. Основные характеристики сетей FDDI

Сеть FDDI (Fiber Distributed Data Interface, *оптоволоконный распределенный интерфейс данных*) – это одна из новейших разработок стандартов локальных сетей. Стандарт FDDI, предложенный Американским национальным институтом стандартов ANSI (спецификация ANSI X3T9.5), изначально ориентировался на высокую скорость передачи (100 Мбит/с) и на применение перспективного оптоволоконного кабеля (длина волны света – 850 нм). Поэтому в данном случае разработчики не были стеснены рамками стандартов, ориентировавшихся на низкие скорости и электрический кабель.

За основу стандарта FDDI был взят метод *маркерного доступа*, предусмотренный международным стандартом IEEE 802.5 Token Ring. Небольшие отличия от этого стандарта определяются необходимостью обеспечить высокую скорость передачи информации на большие расстояния. Топология сети FDDI – это кольцо, причем применяется два разнонаправленных оптоволоконных кабеля, что позволяет в принципе использовать полнодуплексную передачу информации с удвоенной эффективной скоростью в 200 Мбит/с (при этом каждый из двух каналов работает на скорости 100 Мбит/с). Применяется и *звездно-кольцевая* топология с концентраторами, включенными в кольцо.

Основные технические характеристики сети FDDI:

- максимальное количество абонентов сети – 1000;
- максимальная протяженность кольца сети – 20 км;
- максимальное расстояние между абонентами сети – 2 км;
- среда передачи – многомодовый оптоволоконный кабель (возможно применение электрической витой пары);
- метод доступа – маркерный;
- скорость передачи информации – 100 Мбит/с (200 Мбит/с для дуплексного режима передачи).

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

Отметим, что ограничение на общую длину сети в 20 км связано не с затуханием сигналов в кабеле, а с необходимостью ограничения времени полного прохождения сигнала по кольцу для обеспечения предельно допустимого времени доступа. А вот максимальное расстояние между абонентами (2 км при многомодовом кабеле) определяется как раз затуханием сигналов в кабеле (оно не должно превышать 11 дБ). Предусмотрена также возможность применения одномодового кабеля, и в этом случае расстояние между абонентами может достигать 45 км, а полная длина кольца – 100 км.

Существует и реализация FDDI на электрическом кабеле (CDDI – Copper Distributed Data Interface или TPDDI – Twisted Pair Distributed Data Interface). При этом используется кабель категории 5 с разъемами RJ-45. Максимальное расстояние между абонентами в этом случае должно быть не более 100 м.

Для передачи данных в FDDI применяется код 4B/5B (*табл. 6.1*), специально разработанный для этого стандарта.

Таблица 6.1

Схема кода 4B/5B

Информация	Код 4B/5B
0000	11110
0001	01001
0010	10100
0011	10101
0100	01010
0101	01011
0110	01110
0111	01111
1000	10010
1001	10011
1010	10110
1011	10111

Окончание табл. 6.1

Информация	Код 4B/5B
1100	11010
1101	11011
1110	11100
1111	11101

Данный код обеспечивает скорость передачи 100 Мбит/с при пропускной способности кабеля 125 миллионов сигналов в секунду (или 125 МБод), а не 200 МБод, как в случае кода Манчестер-II. При этом каждым четырем битам передаваемой информации (каждому полубайту) ставится в соответствие пять передаваемых по кабелю битов. Это позволяет приемнику восстанавливать синхронизацию приходящих данных один раз на четыре принятых бита, то есть достигается компромисс между простейшим кодом NRZ и самосинхронизирующимся на каждом бите кодом Манчестер-II.

6.3.2. Структура сети FDDI

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

1. Абоненты (станции) класса A (они же абоненты двойного подключения – Dual-Attachment Stations, DAS) подключаются к обоим (внутреннему и внешнему) кольцам сети. При этом реализуется возможность обмена со скоростью до 200 Мбит/с или же возможность резервирования кабеля сети (при повреждении основного кабеля используется резервный). Аппаратура этого класса используется в самых критичных частях сети.

2. Абоненты (станции) класса B (они же абоненты одинарного подключения – Single-Attachment Stations, SAS) подключаются только к одному (внешнему) кольцу сети. Естественно, они могут быть более простыми и дешевыми, чем адаптеры класса A, но не имеют их возможностей. В сеть они могут включаться только через концентратор или обходной коммутатор, отключающий их в случае аварии.

Кроме собственно абонентов (компьютеров, терминалов и т. д.), в сети используются связные концентраторы (Wiring Concentrators), включение которых позволяет собрать в одно место все точки подключения с целью контроля за работой сети, диагностики неисправностей и упрощения реконфигурации. При применении кабелей

разных типов (например, оптоволоконного кабеля и «витой пары») концентратор выполняет также функцию преобразования электрических сигналов в оптические, и наоборот. Концентраторы также бывают двойного подключения (Dual-Attachment Concentrator, DAC) и одинарного подключения (Single-Attachment Concentrator, SAC).

Пример простейшей конфигурации сети FDDI представлен на *рис. 6.7*.

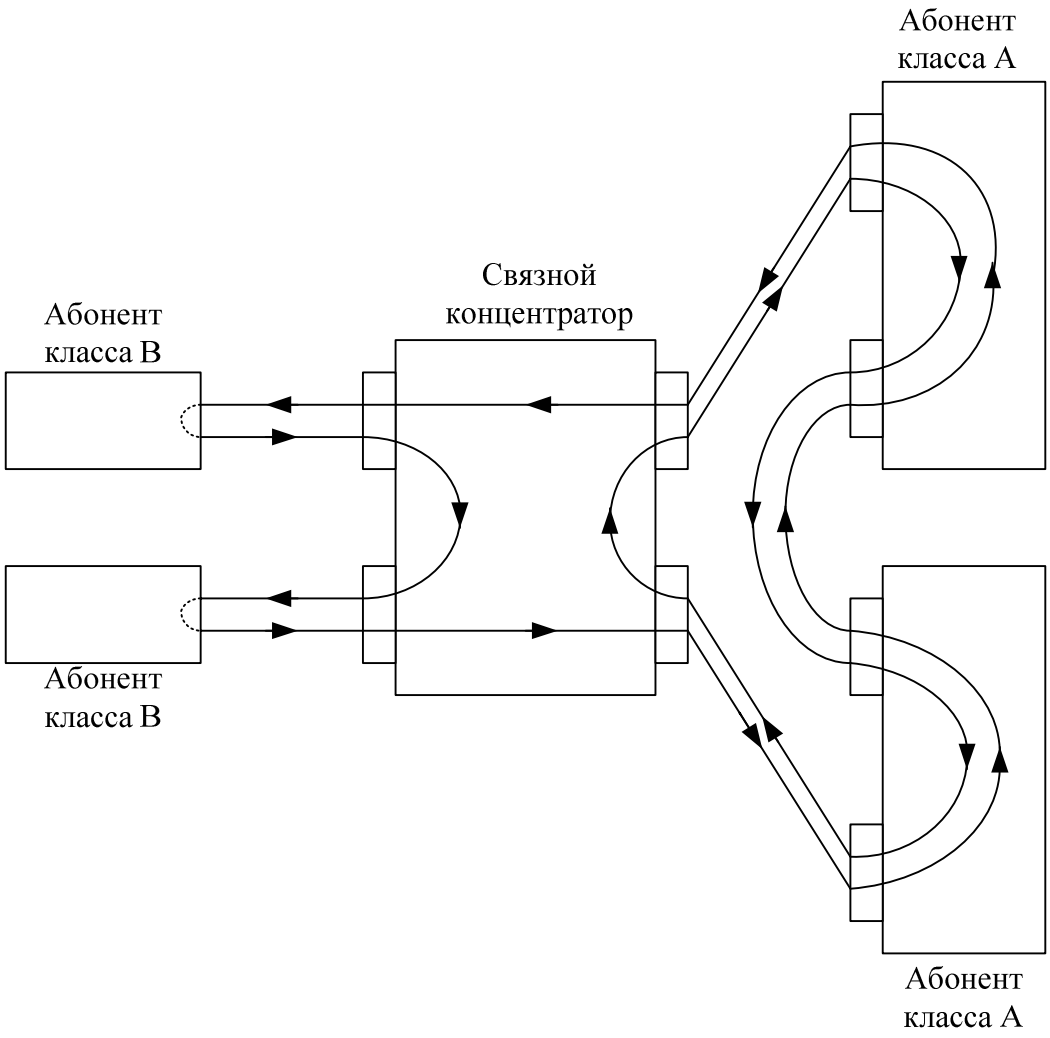


Рис. 6.7. Пример конфигурации сети FDDI

FDDI определяет четыре типа портов абонентов.

1. *Порт А* определен только для устройств двойного подключения, его вход подключается к первичному кольцу, а выход – ко вторичному.

2. *Порт B* определен только для устройств двойного подключения, его вход подключается ко вторичному кольцу, а выход – к первичному.

3. *Порт M* (Master) определен для концентраторов и соединяет два концентратора между собой или концентратор с абонентом.

4. *Порт S* (Slave) определен только для устройств одинарного подключения и используется для соединения двух абонентов или абонента и концентратора.

Стандарт FDDI предусматривает также возможность реконфигурации сети с целью сохранения ее работоспособности в случае повреждения кабеля (*рис. 6.8*). В показанном на рисунке случае поврежденный участок кабеля исключается из кольца, но целостность сети при этом не нарушается вследствие перехода на одно кольцо вместо двух (то есть абоненты класса А начинают работать как абоненты класса В).

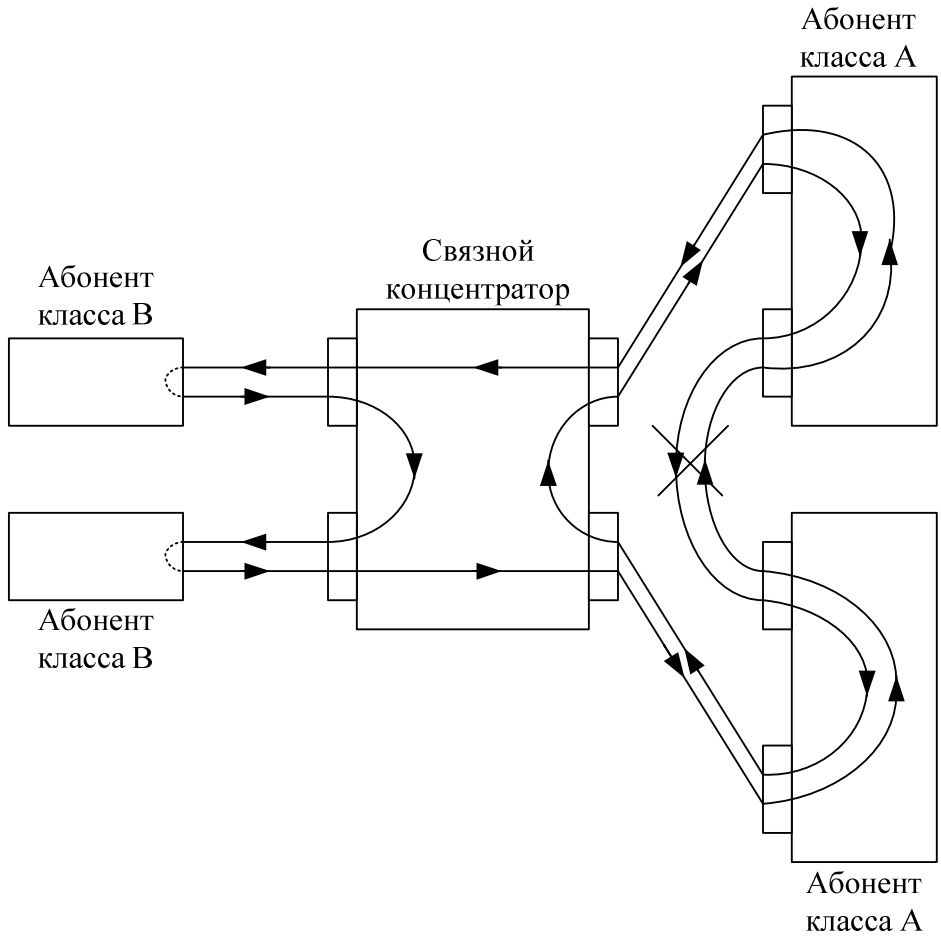


Рис. 6.8. Реконфигурация сети FDDI при повреждении кабеля

В отличие от метода доступа, предлагаемого стандартом IEEE 802.5, в FDDI применяется так называемая ***множественная передача маркера***. Если в случае сети Token Ring новый (свободный) маркер передается абонентом только после возвращения к нему его пакета, то в FDDI новый маркер передается абонентом сразу же после окончания передачи им пакета.

Последовательность действий здесь следующая. Абонент, желающий передавать информацию, ждет маркер, который «идет» за каждым пакетом. Когда маркер пришел, абонент удаляет его из сети и передает свой пакет. Сразу после передачи пакета абонент посылает сгенерированный маркер. Одновременно каждый абонент ведет свой отсчет времени, сравнивая реальное время обращения маркера (TRT) с заранее установленным контрольным временем его прибытия (PTT). Если маркер возвращается раньше, чем установлено PTT, то делается вывод, что сеть загружена мало, и, следовательно, абонент может спокойно передавать всю свою информацию. Если же маркер возвращается позже, чем установлено PTT, то сеть загружена сильно, и абонент может передавать только самую необходимую информацию. При этом величины контрольного времени PTT могут устанавливаться различными для разных абонентов. Такой механизм позволяет абонентам гибко реагировать на загрузку сети и автоматически поддерживать ее на оптимальном уровне.

6.3.3. Структура пакета в сетях FDDI

Стандарт FDDI в отличие от стандарта IEEE 802.5 не предусматривает возможности установки *приоритетов пакетов* и *резервирования*. Вместо этого все абоненты разделяются на две группы: асинхронные и синхронные. ***Асинхронные абоненты*** – это те, для которых время доступа к сети не слишком критично. ***Синхронные*** – это такие абоненты, для которых время доступа должно быть жестко ограничено. В стандарте предусмотрен специальный алгоритм, обслуживающий данные типы абонентов.

Форматы маркера (*рис. 6.9*) и пакета (*рис. 6.10*) сети FDDI несколько отличаются от форматов, используемых в сети Token Ring (на *рис. 6.9* и *рис. 6.10* цифры обозначают количество байт).

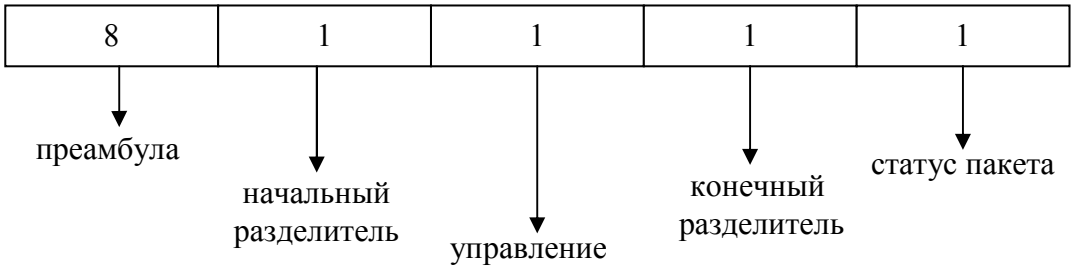


Рис. 6.9. Формат маркера FDDI

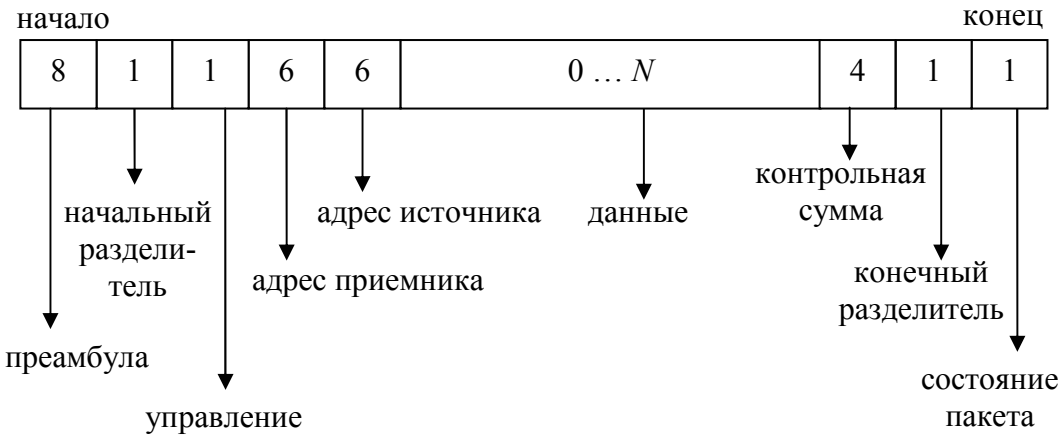


Рис. 6.10. Формат пакета FDDI

Общая длина пакета не может превышать 4500 байт. Рассмотрим назначение каждого из полей.

1. *Преамбула* используется для синхронизации. Первоначально она содержит 64 бита, но абоненты, через которых проходит пакет, могут менять ее размер.

2. *Начальный разделитель* выполняет функцию признака начала кадра.

3. *Адреса приемника и источника* могут быть 6-байтовыми (аналогично Ethernet и Token Ring) или 2-байтовыми.

4. *Поле данных* может быть переменной длины, но суммарная длина пакета не должна превышать 4500 байт.

5. *Поле контрольной суммы* содержит 32-битную циклическую контрольную сумму пакета.

6. *Конечный разделитель* определяет конец кадра.

7. *Байт состояния пакета* включает в себя бит обнаружения ошибки, бит распознавания адреса и бит копирования (все аналогично Token Ring).

Формат байта управления сети FDDI, представленный на *рис. 6.11*, имеет следующую структуру.

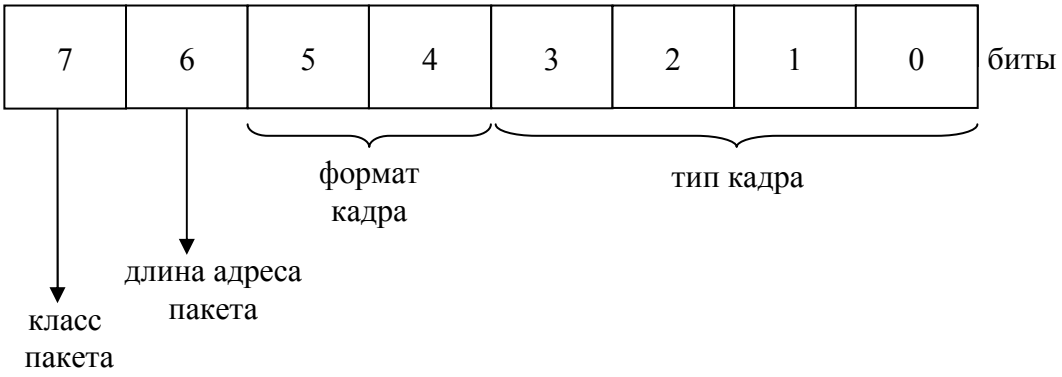


Рис. 6.11. Формат байта управления

1. *Бит класса пакета* определяет, синхронный или асинхронный это пакет.

2. *Бит длины адреса* определяет, какой адрес (6-байтовый или 2-байтовый) используется в данном пакете.

3. *Поле формата кадра* определяет, управляющий это кадр или информационный.

4. *Поле типа кадра* определяет, к какому типу относится данный кадр.

В заключение отметим, что несмотря на очевидные преимущества FDDI, данная сеть не получила пока широкого распространения, что связано главным образом с высокой стоимостью ее аппаратуры (порядка тысячи долларов). Основная область применения FDDI сейчас – это базовые, опорные (Backbone) сети, объединяющие несколько сетей. Применяется FDDI и для соединения мощных рабочих станций или серверов, требующих высокоскоростного обмена. Предполагается, что сеть Fast Ethernet может потеснить FDDI, однако преимущества оптоволоконного кабеля, маркерного метода управления и рекордный допустимый размер сети ставят в настоящее время FDDI вне конкуренции. А в тех случаях, когда стоимость аппаратуры имеет решающее значение, можно на некритичных участках применять версию FDDI на основе витой пары (TPDDI). К тому же стоимость аппаратуры FDDI может сильно уменьшится с увеличением объема ее выпуска.

Выводы

1. Технология FDDI первой использовала волоконно-оптический кабель в локальных сетях, а также работу на скорости 100 Мбит/с. В настоящее время существуют варианты с использованием UTP кабеля типа витая пара.

2. Существует преемственность между технологиями Token Ring и FDDI: для обеих характерны кольцевая топология и маркерный метод доступа.

3. Технология FDDI является наиболее отказоустойчивой технологией локальных сетей. При однократных отказах кабельной системы или станции сеть, за счет «сворачивания» двойного кольца в одинарное, остается вполне работоспособной.

4. Маркерный метод доступа FDDI предполагает разные варианты работы в зависимости от типа кадров (синхронные или асинхронные). Для передачи синхронного кадра станция всегда может захватить пришедший маркер на фиксированное время. Для передачи асинхронного кадра станция может захватить маркер только в том случае, когда маркер выполнил оборот по кольцу достаточно быстро, что говорит об отсутствии перегрузок кольца. Такой метод доступа, во-первых, отдает предпочтение синхронным кадрам, а во-вторых, регулирует загрузку кольца, притормаживая передачу несрочных асинхронных кадров.

5. Максимальное количество станций двойного подключения в кольце – 500, максимальная протяженность двойного кольца – 100 км. Максимальные расстояния между соседними узлами для многомодового кабеля равны 2 км, для витой пары UPT категории 5 – 100 м, а для одномодового оптоволокна в зависимости от его качества составляет десятки километров.

6.4. Сети 100VG-AnyLAN

6.4.1. Основные характеристики сетей 100VG-AnyLAN

Сеть 100VG-AnyLAN – одна из последних разработок высокоскоростных локальных сетей фирм Hewlett Packard и IBM, соответствующая стандарту IEEE 802.12, так что уровень ее стандартизации достаточно высокий. Главными ее достоинствами являются большая скорость обмена, сравнительно невысокая стоимость

аппаратуры, централизованный метод управления обменом без конфликтов и совместимость на уровне пакетов с популярными сетями Ethernet и Token Ring. В названии сети цифра 100 соответствует скорости 100 Мбит/с, буквы VG обозначают дешевую витую пару категории 3 (Voice Grade), а AnyLAN (любая сеть) обозначает то, что сеть совместима с двумя самыми распространенными сетями.

Основные технические характеристики сети 100VG-AnyLAN:

– скорость передачи – 100 Мбит/с;

– топология звезда с возможностью наращивания;

– метод доступа – централизованный, бесконфликтный (Demand Priority – *с запросом приоритета*);

– среда передачи – счетверенная неэкранированная витая пара (кабели UTP категории 3, 4 или 5), сдвоенная витая пара (кабель UTP категории 5), сдвоенная экранированная витая пара (STP), а также оптоволоконный кабель (сейчас в основном распространена счетверенная витая пара);

– максимальная длина кабеля между концентратором и абонентом и между концентраторами – 100 м (для кабеля UTP категории 3), 150 м (для кабеля UTP категории 5 и экранированного кабеля), 2 км (для оптоволоконного кабеля).

Таким образом, параметры сети 100VG-AnyLAN довольно близки к параметрам сети Fast Ethernet. Однако главное преимущество Fast Ethernet – это полная совместимость с наиболее распространенной сетью Ethernet (в случае 100VG-AnyLAN для этого обязательно требуется коммутатор или мост). В то же время централизованное управление 100VG-AnyLAN, исключающее конфликты и гарантирующее предельную величину времени доступа (чего не предусмотрено в сети Ethernet), также нельзя сбрасывать со счетов.

6.4.2. Структура сети 100VG-AnyLAN

Пример структуры сети 100VG-AnyLAN показан на *рис. 6.12*.

Сеть 100VG-AnyLAN состоит из центрального (основного) концентратора уровня 1, к которому могут подключаться как отдельные абоненты, так и концентраторы уровня 2, к которым, в свою очередь, подключаются абоненты и концентраторы уровня 3. При этом сеть может иметь не более трех таких уровней. Получается, что максимальный размер сети может составлять 600 метров для *неэкранированной витой пары*.

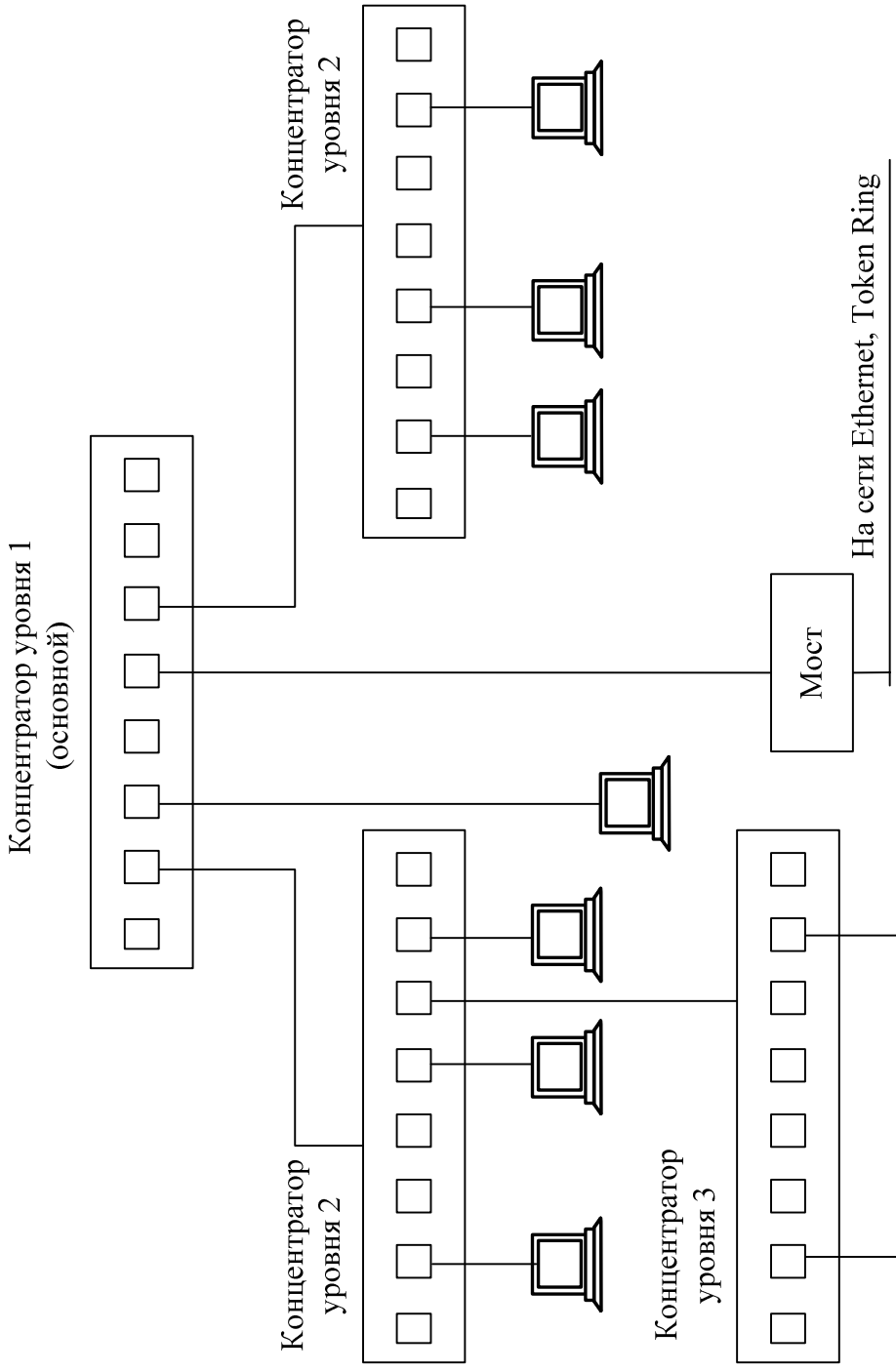


Рис. 6.12. Структура сети 100VG-AnyLAN

В отличие от неинтеллектуальных концентраторов других сетей (например, Ethernet), концентраторы сети l00VG-AnyLAN – это *интеллектуальные контроллеры*, которые управляют всем доступом к сети. Для этого они непрерывно контролируют запросы, поступающие на все порты. Концентраторы принимают все приходящие пакеты и отправляют их только тем абонентам, которым они адресованы. Однако никакой обработки информации они не производят, то есть в данном случае получается все-таки не настоящая (активная) звезда, но и не пассивная звезда.

Каждый из концентраторов может быть настроен на работу с форматами пакетов Ethernet или пакетов Token Ring, при этом концентраторы всей сети должны работать с пакетами только какого-нибудь одного формата. Для связи с сетями Ethernet и Token Ring необходимы мосты, но мосты довольно простые. Концентраторы имеют один порт верхнего уровня (для присоединения его к концентратору более высокого уровня) и несколько портов нижнего уровня (для присоединения абонентов). В качестве абонента может выступать компьютер (рабочая станция), сервер, мост, маршрутизатор, коммутатор, а также другой концентратор.

Каждый порт концентратора может быть установлен в один из двух возможных режимов работы: *нормальный режим*, предполагающий пересылку абоненту, присоединенному к порту, только пакетов, адресованных лично ему, и *мониторный режим*, предполагающий пересылку абоненту, присоединенному к порту, всех пакетов, приходящих на концентратор. Этот режим позволяет одному из абонентов контролировать работу всей сети в целом (выполнять функцию мониторинга).

6.4.3. Метод доступа в сетях 100VG-AnyLAN

В сетях 100VG-AnyLAN используется метод доступа Demand Priority (описан в пункте 3.2.1).

Каждый абонент, желающий передавать информацию, посылает концентратору свой запрос на передачу. Концентратор циклически прослушивает всех абонентов по очереди и дает право передачи абоненту, следующему по порядку за тем, который закончил передачу. Но этот простейший алгоритм усложнен в сети 100VG-AnyLAN, так как запросы могут иметь два уровня приоритета: *нормальный уровень приоритета*, используемый для обычных приложений, и *высокий уровень приоритета*, используемый для приложений, требующих быстрого обслуживания.

Запросы с высоким уровнем приоритета обслуживаются раньше, чем запросы с нормальным приоритетом. Если приходит запрос высокого приоритета, то нормальный порядок обслуживания прерывается, и после окончания приема текущего пакета обслуживается запрос высокого приоритета. Если таких высокоприоритетных запросов несколько, то возврат к нормальной процедуре обслуживания происходит только после полной обработки всех этих запросов. При этом концентратор следит за тем, чтобы не была превышена установленная величина гарантированного времени доступа. Если высокоприоритетных запросов слишком много, то запросы с нормальным приоритетом автоматически переводятся им в ранг высокоприоритетных. Таким образом, даже низкоприоритетные запросы не будут ждать своей очереди слишком долго.

Концентраторы более низких уровней также анализируют запросы абонентов, присоединенных к ним, и в случае необходимости пересылают их запросы к концентратору более высокого уровня. За один раз концентратор более низкого уровня может передать концентратору более высокого уровня не один пакет (как обычный абонент), а столько пакетов, сколько абонентов присоединено к нему.

Так, для примера на *рис. 6.13* в случае одновременного возникновения заявок на передачу у всех абонентов (компьютеров) порядок обслуживания будет такой: компьютер 1-2, затем 1-3, потом 2-1, 2-4, 2-8 и далее 1-6.

Однако так будет только при одинаковом (нормальном) приоритете всех запросов. Если же, например, от компьютеров 1-2, 2-4 и 2-8 поступят высокоприоритетные запросы, то порядок обслуживания будет таким: 1-2, 2-4, 2-8, 1-3, 2-1,1-6.

Помимо собственно передачи пакетов и пересылки запросов на передачу, в сети применяется также *специальная процедура подготовки к связи* (Link Training), во время которой концентратор и абоненты обмениваются между собой управляющими пакетами. При этом проверяется правильность присоединения линий связи и их исправность. Одновременно концентратор получает информацию об особенностях абонентов, подключенных к нему, об их назначении и их сетевых адресах. Запускается данная процедура самим абонентом при включении питания или после подключения к концентратору, а также автоматически при высоком уровне ошибок.

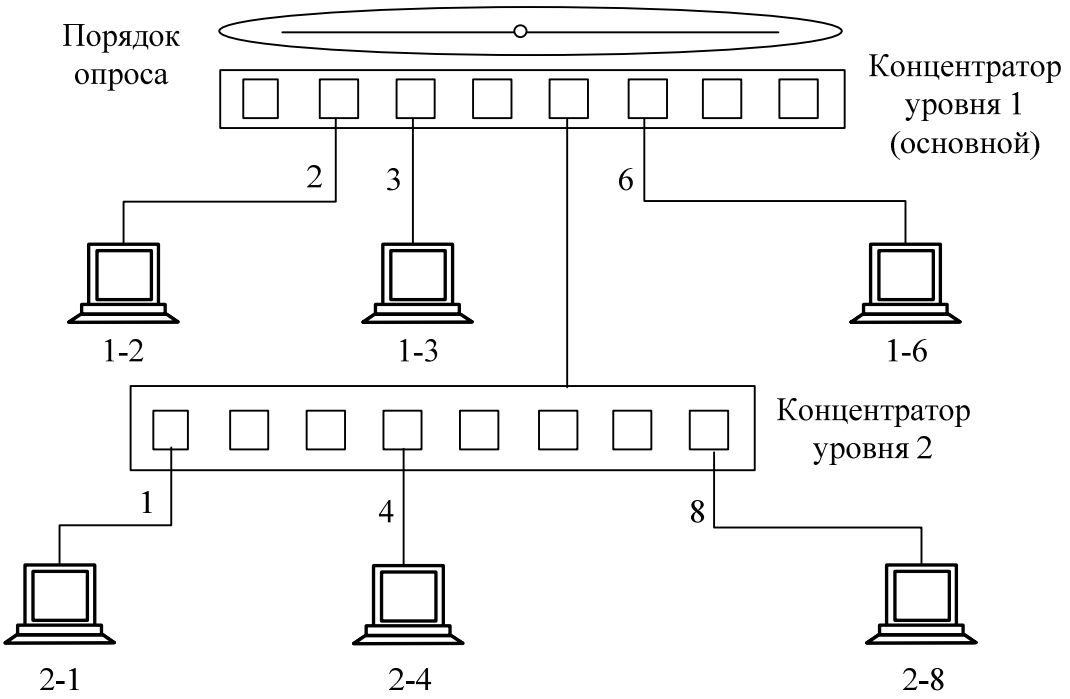


Рис. 6.13. Порядок обслуживания запросов абонентов на различных уровнях сети

6.4.4. Кодирование информации в сетях 100VG-AnyLAN

Проблема кодирования передаваемых данных решена в сети l00VG-AnyLAN достаточно интересно. Вся передаваемая информация проходит следующие этапы обработки:

1) разделение на квинтеты (группы по 5 бит);

2) перемешивание, скремблирование (scrambling) полученных квинтетов;

3) кодирование квинтетов специальным кодом 5B/6B (этот код обеспечивает в выходной последовательности не более трех единиц или нулей подряд, что используется для обнаружения ошибок);

4) добавление начального и конечного разделителей кадра.

Сформированные таким образом кадры передаются в 4 линии передачи (при использовании счетверенной витой пары). При сдвоенной витой паре и оптоволоконном кабеле применяется временное *мультиплексирование информации в каналах*.

В результате этих действий достигается **рандомизация сигналов**, то есть выравнивание количества передаваемых единиц и

нулей, снижение взаимовлияния кабелей друг на друга и самосинхронизация передаваемых сигналов без удвоения требуемой полосы пропускания, как в случае кода Манчестер-II.

В случае использования *счетверенной витой пары* передача по каждой из четырех витых пар производится со скоростью 30 Мбит/с (*рис. 6.14*).

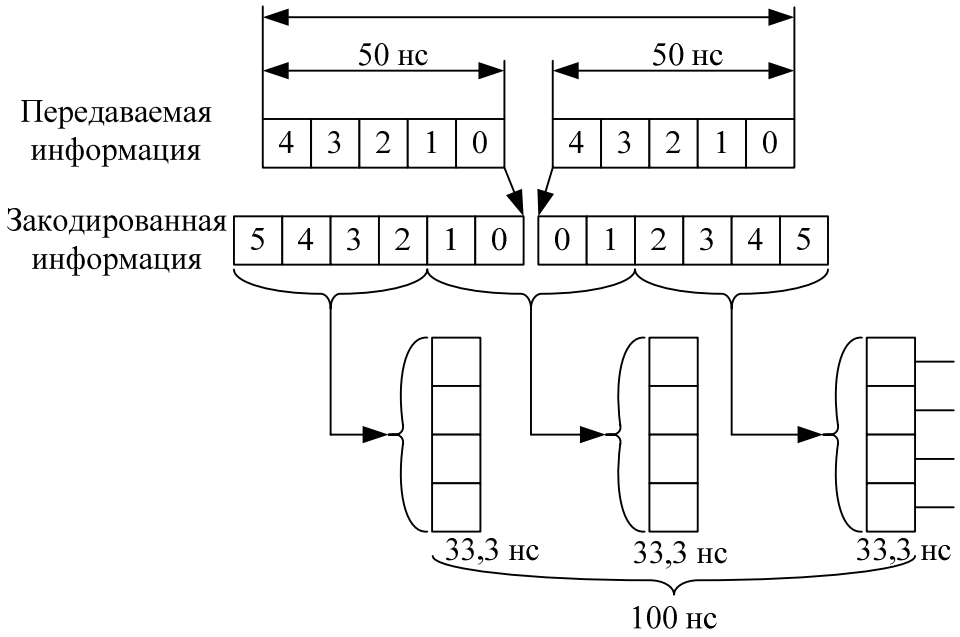


Рис. 6.14. Кодирование информации в сетях 100VG-AnyLAN

Суммарная скорость передачи составляет 120 Мбит/с. Однако полезная информация (вследствие использования кода 5B/6B) передается при этом всего лишь со скоростью 100 Мбит/с. Таким образом, частота сигнала в кабеле должна быть не менее 15 МГц. Этому требованию удовлетворяет кабель с витыми парами категории 3.

В сети 100VG-AnyLAN предусмотрены два режима обмена: *полудуплексный* и *полнодуплексный* (*дуплексный*).

При *полудуплексном обмене* все четыре витые пары используются для передачи одновременно в одном направлении (от абонента к концентратору или наоборот). Он используется для передачи пакетов.

При *полнодуплексном обмене* две витые пары передают в одном направлении, а две другие – в другом направлении. Он

используется для передачи управляющих сигналов. Для управления используются два тональных сигнала. Первый из них представляет собой последовательность из 16 логических единиц и 16 логических кулей, следующих со скоростью 30 Мбит/с (в результате частота сигнала получается равной 0,9375 МГц). Второй тональный сигнал имеет вдвое большую частоту (1,875 МГц) и образуется чередованием 8 логических единиц и 8 логических нулей. Все управление сетью осуществляется комбинацией этих двух тональных сигналов.

В *табл. 6.2* приведена расшифровка различных комбинаций этих сигналов, передаваемых абоненту и концентратору.

Таблица 6.2

Расшифровка комбинаций сигналов

Передаваемые сигналы	Расшифровка абонентом	Расшифровка концентратором
1-1	Нет информации для передачи	Нет информации для передачи
1-2	Концентратор принимает пакет	Запрос нормального приоритета
2-1	Зарезервировано	Запрос с высоким приоритетом
2-2	Запрос процедуры подготовки к связи	Запрос процедуры подготовки к связи

Когда ни у абонента, ни у концентратора нет информации для передачи, оба они посылают по обеим линиям первый тоновый сигнал (1-1). Если принимаемый концентратором пакет может быть адресован данному абоненту, ему посылается комбинация сигналов 1-2. При этом абонент должен прекратить передачу управляющих сигналов концентратору и освободить эти две линии связи для пересылки информационных пакетов. Такая же комбинация 1-2, полученная концентратором, означает *запрос на передачу пакета с нормальным приоритетом*.

Запрос на передачу пакета с высоким приоритетом передается комбинацией 2-1. Наконец, комбинация 2-2 сообщает как абоненту, так и концентратору о необходимости перейти к процедуре подготовки к связи.

В целом, сеть 100VG-AnyLAN представляет собой довольно доступное решение со скоростью передачи до 100 Мбит/с.

Однако она не обладает полной совместимостью ни с одной из стандартных сетей, поэтому ее дальнейшая судьба проблематична. К тому же в отличие от сети FDDI, она не имеет никаких рекордных параметров.

Выводы

1. Согласно стандарту 802.12, технология 100VG-AnyLAN использует тот же формат кадра, что и в сетях Ethernet, но при этом в ней существенно изменен метод доступа.

2. В технологии 100VG-AnyLAN арбитром, решающим вопрос о предоставлении станциям доступа к разделяемой среде, является концентратор, поддерживающий метод Demand Priority – приоритетные требования. Метод Demand Priority оперирует с двумя уровнями приоритетов, выставляемыми станциями, причем приоритет станции, долго не получающей обслуживания, повышается динамически.

3. Концентраторы VG могут объединяться в иерархию, причем порядок доступа к среде не зависит от того, к концентратору какого уровня подключена станция, а зависит только от приоритета кадра и времени подачи заявки на обслуживание.

4. Технология 100VG-AnyLAN поддерживает кабель UTP категории 3, причем для обеспечения скорости 100 Мбит/с передает данные одновременно по 4 парам. Имеется также физический стандарт для кабеля UTP категории 5, кабеля STP Type 1 и волоконно-оптического кабеля.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Приведите основные характеристики сетей Ethernet.
2. Какой метод доступа используется в сетях Ethernet?
3. Приведите стуктуру пакета сетей Ethernet.
4. Какова минимальная длина кадра в сетях Ethernet?
5. Приведите основные характеристики сетей Token Ring.
6. Опишите используемую топологию в сетях Token Ring.
7. Перечислите функции, которые выполняет концентратор в сетях Token Ring?
8. Какие существуют форматы кадров в сетях Token Ring?

9. Опишите процедуру приорететного доступа к кольцу в сетях Token Ring.
10. Приведите основные характеристики сетей FDDI.
11. Какой метод доступа используется в сетях FDDI?
12. Опишите используемую топологию в сетях FDDI.
13. Приведите стуктуру пакета сетей FDDI.
14. Опишите стуктуру сети FDDI.
15. Приведите основные характеристики сетей 100VG-AnyLAN.
16. Опишите метод доступа, используемый в сетях 100VG-AnyLAN.
17. Опишите процедуру кодирования информации в сетях 100VG-AnyLAN.
18. Опишите стуктуру сети 100VG-AnyLAN.
19. Какой тип кабеля может быть использован в сетях 100VG-AnyLAN?

7. ФИЗИЧЕСКАЯ СРЕДА ПЕРЕДАЧИ ДАННЫХ

Физическая среда является основой, на которой строятся физические средства соединения. Сопряжение с физическими средствами соединения посредством физической среды обеспечивает *физический уровень*. В качестве физической среды широко используются эфир, металлы, оптическое стекло и кварц. Среда передачи данных может включать как кабельные, так и беспроводные технологии. Хотя физические кабели являются наиболее распространенными носителями для сетевых коммуникаций, беспроводные технологии все более внедряются благодаря их способности связывать глобальные сети.

На этом уровне для физических кабелей определяются механические и электрические (оптические) свойства среды передачи, которые включают:

- тип кабелей и разъемов;
- разводку контактов в разъемах;
- схему кодирования сигналов для значений 0 и 1.

Канальный уровень определяет доступ к среде и управление передачей посредством процедуры передачи данных по каналу. 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.

7.1. Кабели, линии и каналы связи

Для организации связи в сетях используются следующие понятия:

- кабели связи;
- линии связи;
- каналы связи.

Кабель связи – это длинномерное изделие электротехнической промышленности. Из кабелей связи и других элементов (монтаж, крепеж, кожухи и т. д.) строят ***линии связи*** между узлами сети.

Прокладка линии – задача достаточно серьезная. Длина линий связи колеблется от десятков метров до десятков тысяч километров. В любую более-менее серьезную линию связи кроме кабелей входят: траншеи, колодцы, муфты, переходы через реки, моря и океаны, а также грозозащита (равно как и другие виды защиты) линий. Большую сложность представляют собой юридические вопросы, включающие согласование прокладки линий связи, особенно в городе.

При наличии кабелей связи создаются линии связи, а уже по линиям связи создаются каналы связи. Линии связи и каналы связи заводятся на ***узлы связи***. Линии, каналы и узлы образуют ***первичные сети связи***.

7.2. Кабельные системы

7.2.1. Типы кабелей и структурированные кабельные системы

В качестве среды передачи данных используются различные виды кабелей: *коаксиальный*, *кабель на основе экранированной* и *неэкранированной витой пары*, которые относятся к классу электрических, и *оптоволоконный кабель*.

Наиболее популярным видом среды передачи данных на небольшие расстояния (до 100 м) является *неэкранированная витая пара*, которая включена практически во все современные стандарты и технологии локальных сетей и обеспечивает пропускную способность до 100 Мбит/с (на кабелях категории 5) и выше. Также следует отметить, что *оптоволоконный кабель* применяется как для построения локальных связей, так и для образования магистралей глобальных сетей. Оптоволоконный кабель может обеспечить очень высокую пропускную способность канала (до нескольких десятков Гбит/с) и передачу на значительные расстояния (до нескольких десятков километров без промежуточного усиления сигнала).

В качестве среды передачи данных в вычислительных сетях используются также электромагнитные волны различных частот – *КВ* (короткие волны), *УКВ* (ультракороткие волны), *СВЧ* (сверхвысокие частоты). Однако пока в локальных сетях радиосвязь используется только в тех случаях, когда оказывается невозможной

прокладка кабеля. Это объясняется недостаточной надежностью и, прежде всего, безопасностью сетевых технологий, построенных на использовании электромагнитного излучения (так называемые *беспроводные сети* – wireless networks). Для построения глобальных каналов этот вид среды передачи данных используется шире – на нем построены спутниковые каналы связи и наземные радиорелейные каналы, работающие в зонах прямой видимости в СВЧ-диапазонах.

Очень важно правильно построить фундамент сети – **кабельную систему**. В последнее время в качестве такой надежной основы все чаще используется структурированная кабельная система.

Структурированная кабельная система (Structured Cabling System, SCS) – это набор коммутационных элементов (кабелей, разъемов, коннекторов, кроссовых панелей и шкафов), а также методика их совместного использования, которая позволяет создавать регулярные, легко расширяемые структуры связей в вычислительных сетях.

Преимущества структурированной кабельной системы

1. *Универсальность*. Структурированная кабельная система при продуманной организации может стать единой средой для передачи компьютерных данных в локальной вычислительной сети.

2. *Увеличение срока службы*. Срок старения хорошо структурированной кабельной системы может составлять 8–10 лет.

3. *Уменьшение стоимости добавления новых пользователей и изменения их мест размещения*. Стоимость кабельной системы в основном определяется не стоимостью кабеля, а стоимостью работ по его прокладке.

4. *Возможность легкого расширения сети*. Структурированная кабельная система является модульной, поэтому ее легко наращивать, позволяя легко и ценой малых затрат переходить на более совершенное оборудование, удовлетворяющее растущим требованиям к системам коммуникаций.

5. *Обеспечение более эффективного обслуживания*. Структурированная кабельная система облегчает обслуживание и поиск неисправностей.

6. *Надежность*. Структурированная кабельная система имеет повышенную надежность, поскольку обычно производство всех ее компонентов и техническое сопровождение осуществляется одной фирмой-производителем.

7.2.2. Стандарты кабелей

Кабель – это достаточно сложное изделие, состоящее из проводников, слоев экрана и изоляции.

Обычно кабели присоединяются к оборудованию с помощью разъемов. Кроме этого, для обеспечения быстрой перекоммутации кабелей и оборудования используются различные электромеханические устройства, называемые *кроссовыми секциями*, *кроссовыми коробками* или *шкафами*.

В компьютерных сетях применяются кабели, удовлетворяющие определенным стандартам, что позволяет строить кабельную систему сети из кабелей и соединительных устройств разных производителей. Сегодня наиболее употребительными в мировой практике являются следующие стандарты.

1. Американский стандарт EIA/TIA-568A, который был разработан совместными усилиями нескольких организаций: ANSI, EIA/TIA и лабораторией Underwriters Labs (UL). (Стандарт EIA/TIA-568 разработан на основе предыдущей версии стандарта EIA/TIA-568 и дополнений к этому стандарту TSB-36 и TSB-40A).
2. Международный стандарт ISO/IEC 11801.
3. Европейский стандарт EN50173.

Эти стандарты близки между собой и по многим позициям предъявляют к кабелям идентичные требования. Однако есть и различия между этими стандартами, например, в международный стандарт 11801 и европейский EN50173 вошли некоторые типы кабелей, которые отсутствуют в стандарте EIA/TAI-568A.

До появления стандарта EIA/TIA большую роль играл американский стандарт системы категорий кабелей Underwriters Labs, разработанный совместно с компанией Anixter. Позже этот стандарт вошел в стандарт EIA/TIA-568.

Кроме этих открытых стандартов, многие компании в свое время разработали свои фирменные стандарты, из которых до сих пор имеет практическое значение только один – стандарт компании IBM.

При стандартизации кабелей принят протокольно-независимый подход. Это означает, что в стандарте оговариваются электрические, оптические и механические характеристики, которым должен удовлетворять тот или иной тип кабеля или соединительного изделия – разъема, кроссовой коробки и т. п. Однако для какого протокола предназначен данный кабель, стандарт не оговаривает. Поэтому

нельзя приобрести кабель для протокола Ethernet или FDDI, нужно просто знать, какие типы стандартных кабелей поддерживают протоколы Ethernet и FDDI.

В ранних версиях стандартов определялись только характеристики кабелей, без соединителей. В последних версиях стандартов появились требования к соединительным элементам (документы TSB-36 и TSB-40A, вошедшие затем в стандарт 568A), а также к линиям (каналам), представляющим типовую сборку элементов кабельной системы, состоящую из шнура от рабочей станции до розетки, самой розетки, основного кабеля (длиной до 90 м для витой пары), точки перехода (например, еще одной розетки или жесткого кроссового соединения) и шнура активного оборудования, например, концентратора или коммутатора.

Мы остановимся только на основных требованиях к самим кабелям, не рассматривая характеристик соединительных элементов и собранных линий.

В стандартах кабелей оговаривается достаточно много характеристик, из которых наиболее важные перечислены ниже.

1. *Затухание* (Attenuation). Затухание измеряется в децибелах на метр для определенной частоты или диапазона частот сигнала.

2. *Перекрестные наводки на ближнем конце* (Near End Cross Talk, NECT). Измеряются в децибелах для определенной частоты сигнала.

3. *Импеданс* (Impedance, волновое сопротивление) – это полное (активное и реактивное) сопротивление в электрической цепи. Импеданс измеряется в омах (Ом) и является относительно постоянной величиной для кабельных систем (например, для коаксиальных кабелей, используемых в стандартах Ethernet, импеданс кабеля должен составлять 50 Ом). Для неэкранированной витой пары наиболее часто используемые значения импеданса – 100 и 120 Ом. В области высоких частот (100–200 МГц) импеданс зависит от частоты.

4. *Активное сопротивление* – это сопротивление постоянному току в электрической цепи. В отличие от импеданса активное сопротивление не зависит от частоты и возрастает с увеличением длины кабеля.

5. *Емкость* – это свойство металлических проводников накапливать энергию. Два электрических проводника в кабеле, разделенные диэлектриком, представляют собой конденсатор, способный

накапливать заряд. Емкость является нежелательной величиной, поэтому следует стремиться к тому, чтобы она была как можно меньше (иногда применяют термин «паразитная емкость»). Высокое значение емкости в кабеле приводит к искажению сигнала и ограничивает полосу пропускания линии.

6. *Уровень внешнего электромагнитного излучения*, или *электрический шум.* **Электрический шум** – это нежелательное переменное напряжение в проводнике. Электрический шум бывает двух типов: *фоновый* и *импульсный*.

Электрический шум можно также разделить на низко-, средне- и высокочастотный. Источниками фонового электрического шума в диапазоне до 150 кГц являются линии электропередачи, телефоны и лампы дневного света; в диапазоне от 150 кГц до 20 МГц – компьютеры, принтеры, ксероксы; в диапазоне от 20 МГц до 1 ГГц – телевизионные и радиопередатчики, микроволновые печи. Основными источниками импульсного электрического шума являются моторы, переключатели и сварочные агрегаты. Электрический шум измеряется в милливольтах.

7. *Диаметр*, или *площадь сечения проводника*. Для медных проводников достаточно употребительной является американская система AWG (American Wire Gauge), которая вводит некоторые условные типы проводников, например, 22 AWG, 24 AWG, 26 AWG. Чем больше номер типа проводника, тем меньше его диаметр. В вычислительных сетях наиболее употребительными являются типы проводников, приведенные выше в качестве примеров. В европейских и международных стандартах диаметр проводника указывается в миллиметрах.

Основное внимание в современных стандартах уделяется кабелям на основе витой пары и волоконно-оптическим кабелям.

7.2.3. Кабель типа витая пара

Витой парой (twisted pair) называется кабель, в котором изолированная пара проводников скручена с небольшим числом витков на единицу длины (*рис. 7.1*).

Скручивание проводов уменьшает электрические помехи извне при распространении сигналов по кабелю, а экранированные витые пары еще более увеличивают степень помехозащищенности сигналов.

Кабель типа витая пара используется во многих сетевых технологиях, включая Ethernet, ARCNet и IBM Token Ring.

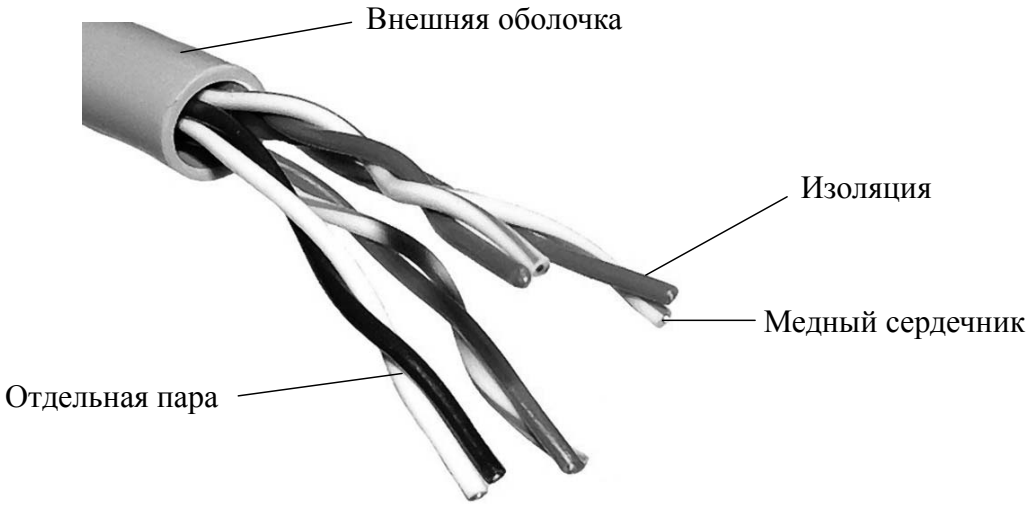


Рис. 7.1. Структура кабеля типа витая пара

Кабели на витой паре подразделяются на *неэкранированные* (Unshielded Twisted Pair, UTP) и *экранированные* медные кабели. Последние подразделяются на две разновидности: с экранированием каждой пары и общим экраном (Shielded Twisted Pair, STP) и с одним только общим экраном (Foiled Twisted Pair, FTP). Наличие или отсутствие экрана у кабеля вовсе не означает наличие или отсутствие защиты передаваемых данных, а говорит лишь о различных подходах к подавлению помех. Отсутствие экрана делает неэкранированные кабели более гибкими и устойчивыми к изломам. Кроме того, они не требуют дорогостоящего контура заземления для эксплуатации в нормальном режиме, как экранированные. Неэкранированные кабели идеально подходят для прокладки в помещениях внутри офисов, а экранированные лучше использовать для установки в местах с особыми условиями эксплуатации, например, рядом с очень сильными источниками электромагнитных излучений, которых в офисах обычно нет.

Кабели на основе неэкранированной витой пары. Медный неэкранированный кабель UTP в зависимости от электрических и механических характеристик разделяется на 5 категорий (Category 1 – Category 5). Кабели категорий 1 и 2 были определены в стандарте EIA/TIA-568, но в стандарт 568A уже не вошли, как устаревшие.

Кабели категории 1 применяются там, где требования к скорости передачи минимальны. Обычно это кабель для цифровой и аналоговой передачи голоса и низкоскоростной (до 20 Кбит/с) передачи данных. До 1983 года это был основной тип кабеля для телефонной разводки.

Кабели категории 2 были впервые применены фирмой IBM при построении собственной кабельной системы. Главное требование к кабелям этой категории – способность передавать сигналы со спектром до 1 МГц.

Кабели категории 3 были стандартизованы в 1991 году, когда был разработан *Стандарт телекоммуникационных кабельных систем для коммерческих зданий* (EIA-568), на основе которого затем был создан действующий стандарт EIA-568A. Стандарт EIA-568 определил электрические характеристики кабелей категории 3 для частот в диапазоне до 16 МГц, поддерживающих, таким образом, высокоскоростные сетевые приложения. Кабель категории 3 предназначен как для передачи данных, так и для передачи голоса. Шаг скрутки проводов равен примерно 3 виткам на 1 фут (30,5 см). Кабели категории 3 сейчас составляют основу многих кабельных систем зданий, в которых они используются для передачи и голоса, и данных.

Кабели категории 4 представляют собой несколько улучшенный вариант кабелей категории 3. Кабели категории 4 обязаны выдерживать тесты на частоте передачи сигнала 20 МГц и обеспечивать повышенную помехоустойчивость и низкие потери сигнала. Они хорошо подходят для применения в системах с увеличенными расстояниями (до 135 м) и в сетях Token Ring с пропускной способностью 16 Мбит/с. На практике используются редко.

Кабели категории 5 были специально разработаны для поддержки высокоскоростных протоколов. Поэтому их характеристики определяются в диапазоне до 100 МГц. Большинство новых высокоскоростных стандартов ориентируются на использование витой пары 5-й категории. На этом кабеле работают протоколы со скоростью передачи данных 100 Мбит/с – FDDI (с физическим стандартом TP-PMD), Fast Ethernet, 100VG-AnyLAN, а также более скоростные протоколы ATM на скорости 155 Мбит/с и Gigabit Ethernet на скорости 1000 Мбит/с (вариант Gigabit Ethernet на витой паре категории 5 стал стандартом в июне 1999 года).

Кабель категории 5 пришел на замену кабелю категории 3, и сегодня многие новые кабельные системы крупных зданий строятся именно на этом типе кабеля (в сочетании с волоконно-оптическим).

Кабели UTP 5-й категории выпускаются в 4-парном исполнении. Каждая из четырех пар кабеля имеет определенный цвет и шаг скрутки. Обычно две пары предназначены для передачи данных, и 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. Для кабеля категории 6 характеристики определяются до частоты 200 МГц, а для кабелей категории 7 – до 600 МГц. Кабели категории 7 обязательно экранируются, причем как каждая пара, так и весь кабель в целом.

Кабели на основе экранированной витой пары. Экранированная витая пара STP хорошо защищает передаваемые сигналы от внешних помех, а также меньше излучает электромагнитных колебаний, что защищает, в свою очередь, пользователей сетей от вредного для здоровья излучения. Наличие заземляемого экрана удорожает кабель 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 двух пар скрученных проводов, экранированных проводящей оплеткой, которая заземляется. Электрические параметры кабеля Type 1 примерно соответствуют параметрам кабеля UTP категории 5. Некоторые стандарты поддерживают кабель STP Type 1 – например, 100VG-AnyLAN, а также Fast Ethernet (хотя основным типом кабеля для Fast Ethernet является UTP категории 5). В случае, если технология может использовать UTP и STP, нужно убедиться, на какой тип кабеля рассчитаны приобретаемые трансиверы. Сегодня кабель

STP Type 1 включен в стандарты EIA/TIA-568A, ISO 11801 и EN50173, то есть приобрел международный статус.

Экранированные витые пары используются также в кабеле IBM Type 2, который представляет кабель Type 1 с добавленными двумя парами неэкранированного провода для передачи голоса.

Для присоединения экранированных кабелей к оборудованию используются разъемы конструкции IBM.

7.2.4. Коаксиальные кабели

Коаксиальные кабели (*рис. 7.2*) используются в радио- и телевизионной аппаратуре.

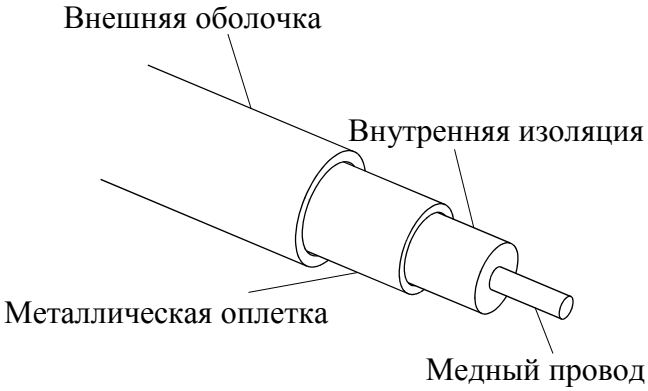


Рис. 7.2. Структура коаксиального кабеля

Коаксиальные кабели могут передавать данные со скоростью 10 Мбит/с на максимальное расстояние от 185 до 500 метров. Они разделяются на толстые и тонкие в зависимости от толщины.

Типы коаксиальных кабелей приведены в *табл. 7.1*.

Таблица 7.1

Типы коаксиальных кабелей

Тип	Название, значение сопротивления
RG-8 и RG-11	Thicknet, 50 Ом
RG-58/U	Thinnet, 50 Ом, сплошной центральный медный проводник
RG-58A/U	Thinnet, 50 Ом, центральный многожильный проводник
RG-59	Broadband/Cable television (широковещательное/кабельное телевидение), 75 Ом
RG-59/U	Broadband/Cable television (широковещательное/кабельное телевидение), 50 Ом
RG-62	ARCNet, 93 Ом

Кабель Thinnet, известный как кабель RG-58, является наиболее широко используемым физическим носителем данных. Сети при этом не требуют дополнительного оборудования и являются простыми и недорогими. Хотя тонкий коаксиальный кабель (Thin Ethernet) позволяет осуществлять передачу на меньшее расстояние, чем толстый, для соединений с тонким кабелем применяются стандартные байонетные разъемы BNC типа CP-50, и ввиду его небольшой стоимости он становится фактически стандартным для офисных ЛВС. Используется в технологии Ethernet 10Base2, описанной ниже.

Толстый коаксиальный кабель (Thick Ethernet) имеет большую степень помехозащищенности, большую механическую прочность, но требует специального приспособления для прокалывания кабеля, чтобы создать ответвления для подключения к ЛВС. Он более дорогой и менее гибкий, чем тонкий. Используется в технологии Ethernet 10Base5, описанной ниже. Сети ARCNet с передачей маркера обычно используют кабель RG-62A/U.

Рассмотрим основные параметры систем на основе коаксиальных кабелей.

Характеристики спецификации 10Base2:

- тонкий коаксиальный кабель;
- характеристики кабеля: диаметр 0,2 дюйма, RG-58A/U 50 Ом;
- приемлемые разъемы – BNC;
- максимальная длина сегмента – 185 м;
- минимальное расстояние между узлами – 0,5 м;
- максимальное число узлов в сегменте – 30.

Характеристики спецификации 10Base5:

- толстый коаксиальный кабель;
- волновое сопротивление – 50 Ом;
- максимальная длина сегмента – 500 метров;
- минимальное расстояние между узлами – 2,5 м;
- максимальное число узлов в сегменте – 100.

7.2.5. Оптоволоконный кабель

Волоконно-оптические линии связи – это вид связи, при котором информация передается по оптическим диэлектрическим волноводам, известным под названием *оптическое волокно*.

Оптическое волокно в настоящее время считается самой совершенной физической средой для передачи информации, а также

самой перспективной средой для передачи больших потоков информации на значительные расстояния. Основания так считать вытекают из ряда особенностей, присущих оптическим волноводам.

Физические особенности. Широкополосность оптических сигналов обусловлена чрезвычайно высокой частотой несущей (F_o = = 1014 Гц). Это означает, что по оптической линии связи можно передавать информацию со скоростью порядка 1000 Мбит/с. Говоря другими словами, по одному волокну можно передать одновременно 10 миллионов телефонных разговоров и миллион видеосигналов. Скорость передачи данных может быть увеличена за счет передачи информации сразу в двух направлениях, так как световые волны могут распространяться в одном волокне независимо друг от друга. На сегодняшний день предел по плотности передаваемой информации по оптическому волокну не достигнут.

Очень малое (по сравнению с другими средами) затухание светового сигнала в волокне. Лучшие образцы российского волокна имеют затухание 0,22 дБ/км на длине волны 1,55 мкм, что позволяет строить линии связи длиной до 100 км без *регенерации сигналов* (промежуточного усиления). Для сравнения, лучшее волокно Sumitomo на длине волны 1,55 мкм имеет затухание 0,154 дБ/км. В лабораториях разрабатываются еще более «прозрачные», так называемые *фторцирконатные волокна* с теоретическим пределом порядка 0,02 дБ/км на длине волны 2,5 мкм. Лабораторные исследования показали, что на основе таких волокон могут быть созданы линии связи с регенерационными участками через 4600 км при скорости передачи порядка 1 Гбит/с.

Технические особенности и преимущества оптических волокон. Волокно изготовлено из кварца, основу которого составляет двуокись кремния, широко распространенного, а потому недорогого материала, в отличие от меди.

Оптические волокна имеют диаметр около 100 мкм, то есть очень компактны и легки, что делает их перспективными для использования в авиации, приборостроении, в кабельной технике.

Применяя особо прочный пластик, на кабельных заводах изготавливают самонесущие подвесные кабели, не содержащие металла и тем самым безопасные в электрическом отношении. Такие кабели можно монтировать на мачтах существующих линий электропередач, как отдельно, так и встроенными в фазовый провод, экономя значительные средства на прокладку кабеля через реки и другие преграды.

Системы связи на основе оптических волокон устойчивы к электромагнитным помехам, а передаваемая по световодам информация защищена от несанкционированного доступа. Волоконно-оптические линии связи нельзя прослушать, не разрушив поверхность канала. Всякие воздействия на волокно могут быть зарегистрированы методом мониторинга (непрерывного контроля) целостности линии. Важное свойство оптического волокна – долговечность. Время жизни волокна, то есть сохранение им своих свойств в определенных пределах, превышает 25 лет, что позволяет проложить оптико-волоконный кабель один раз и по мере необходимости наращивать пропускную способность канала путем замены приемников и передатчиков на более быстродействующие.

Недостатки волоконной технологии. При создании линии связи требуются высоконадежные активные элементы, преобразующие электрические сигналы в свет и свет в электрические сигналы. Необходимы также оптические коннекторы (соединители) с малыми оптическими потерями и большим ресурсом на подключение-отключение. Точность изготовления таких элементов линии связи должна соответствовать длине волны излучения, то есть погрешности должны быть порядка доли микрона. Поэтому производство таких компонентов оптических линий связи очень дорогостоящее. Другой недостаток заключается в том, что для монтажа оптических волокон требуется прецизионное (высокоточное), а потому дорогое технологическое оборудование. Как следствие, при аварии (обрыве) оптического кабеля затраты на восстановление выше, чем при работе с медными кабелями.

Преимущества от применения волоконно-оптических линий связи (ВОЛС) настолько значительны, что, несмотря на перечисленные недостатки оптического волокна, эти линии связи все шире используются для передачи информации.

Структура оптоволокна. Волоконно-оптический кабель 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 и к тому же лучше других типов передающей среды обеспечивает защиту данных от внешних помех.

Волоконно-оптические кабели состоят из центрального проводника света (сердцевины) – стеклянного волокна, окруженного другим слоем стекла – оболочкой, обладающей меньшим показателем

преломления, чем сердцевина (*рис. 7.3*). Распространяясь по сердцевине, лучи света не выходят за ее пределы, отражаясь от покрывающего слоя оболочки.

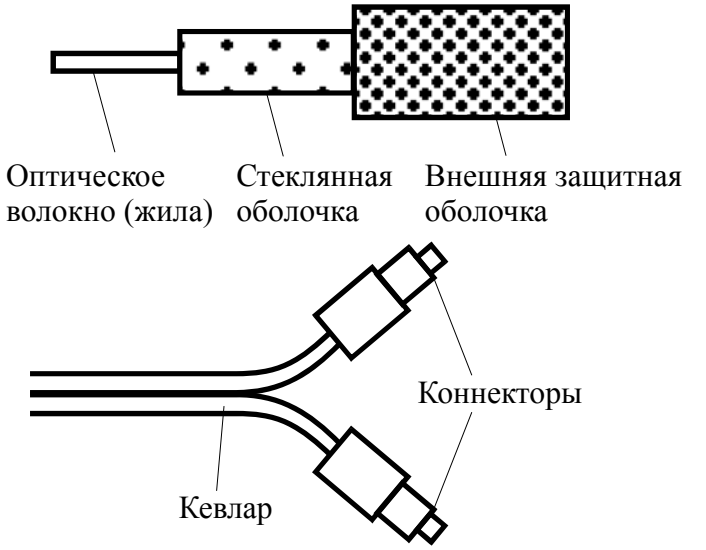


Рис. 7.3. Структура оптоволокна и оптоволоконного кабеля

В зависимости от распределения показателя преломления и от величины диаметра сердечника различают:

– многомодовое волокно со ступенчатым изменением показателя преломления (*рис. 7.4*, *а*);

– многомодовое волокно с плавным изменением показателя преломления (*рис. 7.4*, *б*);

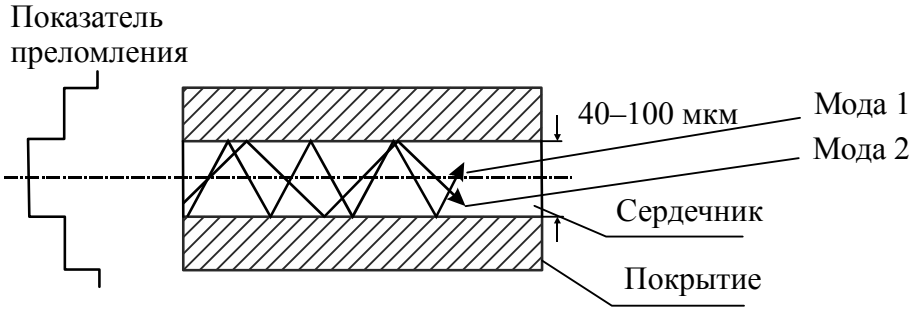
– одномодовое волокно (*рис. 7.4*, *в*).

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.

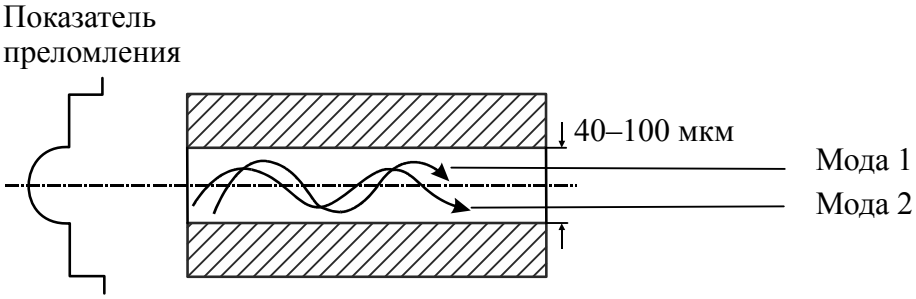
В *многомодовых кабелях* (Multi Mode Fiber, MMF) используются более широкие внутренние сердечники, которые легче изготовить технологически. В стандартах определены два наиболее употребительных многомодовых кабеля: 62,5/125 мкм и 50/125 мкм, где 62,5 мкм или 50 мкм – это диаметр центрального проводника, а 125 мкм – диаметр внешнего проводника. В многомодовых кабелях

во внутреннем проводнике одновременно существует несколько световых лучей, отражающихся от внешнего проводника под разными углами. Угол отражения луча называется модой луча.



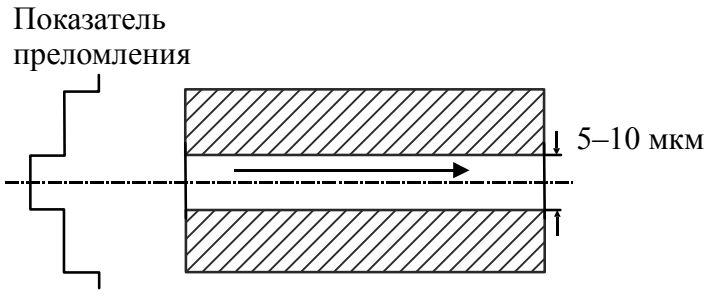
Многомодовое волокно со ступенчатым изменением показателя преломления

а



Многомодовое волокно с плавным изменением показателя преломления

б



Одномодовое оптоволокно

в

Рис. 7.4. Типы оптоволоконного кабеля

Параметры оптоволоконных кабелей. Оба типа волокна характеризуются двумя важнейшими параметрами: затуханием и дисперсией.

Затухание определяется потерями на поглощение и на рассеяние излучения в оптическом волокне (измеряется в дБ/км). Потери на поглощение зависят от чистоты материала, потери на рассеяние зависят от неоднородностей показателя преломления материала (*рис. 7.5*).

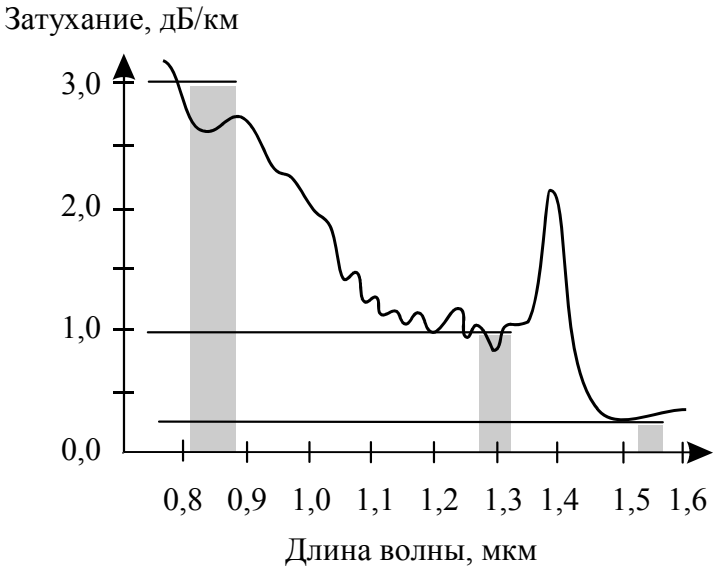


Рис. 7.5. Зависимость затухания от длины волны

Затухание зависит от длины волны излучения, вводимого в волокно. В настоящее время передачу сигналов по волокну осуществляют в трех диапазонах: 0,85 мкм, 1,3 мкм, 1,55 мкм, так как именно в этих диапазонах кварц имеет повышенную прозрачность.

Другой важнейший параметр оптического волокна – дисперсия. *Дисперсия* – это рассеяние во времени спектральных и модовых составляющих оптического сигнала.

7.3. Параметры кабельных систем Ethernet

7.3.1. Параметры систем на основе неэкранированной витой пары

Неэкранированная витая пара – это кабель из четырех скрученных пар проводов.

Характеристики кабеля*:*

– диаметр проводников 0,4–0,6 мм (22~26 AWG), 4 скрученные пары: 8 проводников, из которых для 10Base-T, 100Base-TX, 1000Base-TX используют одну, две или четыре пары (кабель должен иметь категорию 3, 5 или 6 и качество data grade или выше);

– максимальная длина сегмента 100 м;

– разъемы восьмиконтактные RJ-45 (*рис. 7.6*).

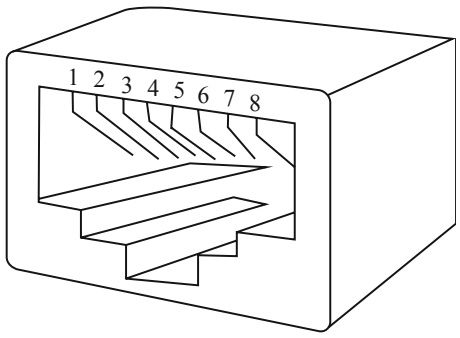


Рис. 7.6. Восьмиконтактные разъемы RJ-45

В *табл. 7.2* приведены сигналы (спецификация 100Base-T), соответствующие номерам контактов разъема RJ-45 (для спецификации 1000Base-TX используются все восемь контактов).

Таблица 7.2

Сигналы, соответствующие номерам контактов разъема RJ-45

Тип	Каскадирование	Нормальный режим
1	RD+ (прием)	TD+ (передача)
2	RD- (прием)	TD- (передача)
3	TD+ (передача)	RD+ (прием)
4	Не используется	Не используется
5	Не используется	Не используется
6	TD- (передача)	RD- (прием)
7	Не используется	Не используется
8	Не используется	Не используется

7.3.2. Стандартные разводки кабеля типа витая пара

В настоящее время наиболее популярны две схемы – T568A и T568B (*рис. 7.7*). Они идентичны в случае, если не используются вторая и третья пары.

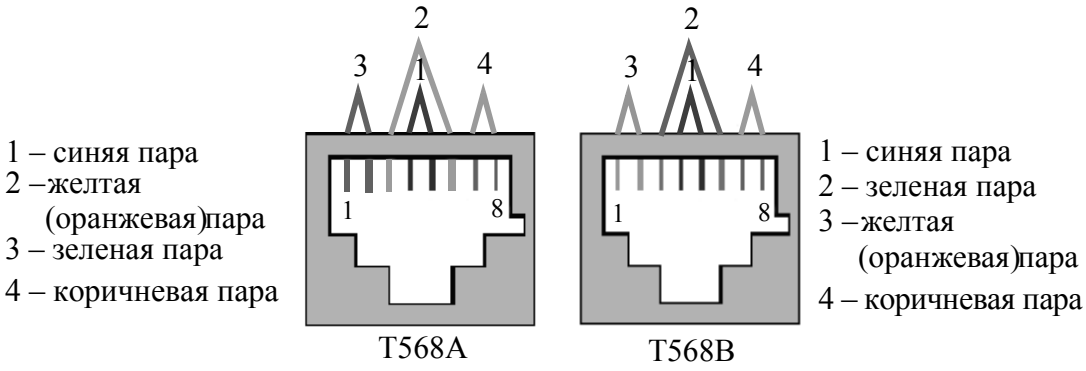


Рис. 7.7. Схемы разводки витой пары

Предпочтительна первая схема на *рис. 7.7*, поскольку она совместима с однопарной и двупарной конфигурацией системы USOC (*рис. 7.8*).

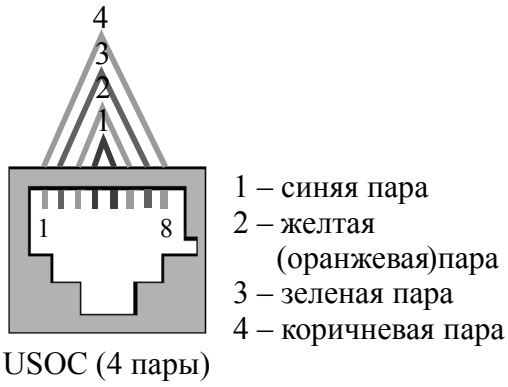
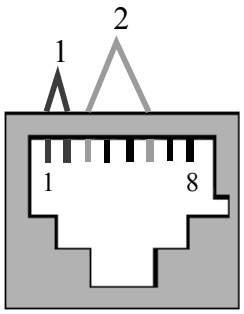


Рис. 7.8. Двупарная конфигурация системы USOC

Однако обе схемы могут использоваться для линий ISDN (Integrated Servises Digital Network), а также в высокоскоростных сетях. Дело в том, что схемы разработаны таким образом, чтобы свести к минимуму взаимные наводки в парах. А это необходимое условие для категорий 3, 4, 5, 5e и 6. Поэтому при реализации высокоскоростных сетей используют именно эти конфигурации.

7.3.3. Реализация сетевых топологий на основе стандартной разводки

Топология сети 10BaseT реализуется с помощью 8-пинового разъема по схожей схеме с T568A и T568B, однако на контакты выводятся другие пары (*рис. 7.9*).



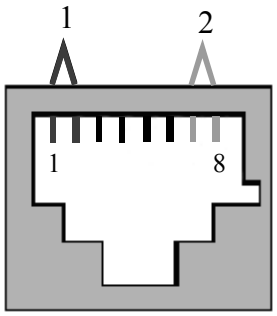
1 – синяя пара
2 – желтая (оранжевая) пара

10BASE-T (IEEE 802.3)

Рис. 7.9. Схема 8-пинового разъема для сетей 10BaseT

Если все же пользоваться стандартами T568, то в случае первой пары (по версии 10BaseT) необходимо использовать 3/2-ю пару разводки T568A/T568B, а в качестве второй 2/3-ю пару T568A/T568B.

Как и 10BaseT, ATM и TP-PMD реализуются только на 8-пиновом разъеме с использованием двух пар, и точно также схема схожа со стандартными разводками T568A и T568B (*рис. 7.10*).



1 – синяя пара
2 – желтая (оранжевая) пара

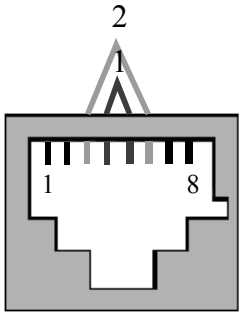
TP-PMD (IEEE 802.3) ATM

Рис. 7.10. Схема 8-пинового разъема для стандарта TP-PMD

В данной разводке в случае первой пары (по версии 10BaseT) необходимо использовать 3/2-ю пару разводки T568A/T568B, а в качестве второй 4-ю пару T568A или T568B.

Еще одна разводка, косвенно совместимая с T568A/B, а также и со схемой USOC – Token Ring (*рис. 7.11*).

Она строится на двух парах, занимащих центральные контакты. Причем Token Ring может сразу строиться на основе схемы T568A и USOC без каких-либо модификаций. В случае же использования T568B, необходимо в качестве второй пары применять 3-ю пару.



1 – синяя пара
2 – желтая
(оранжевая пара)

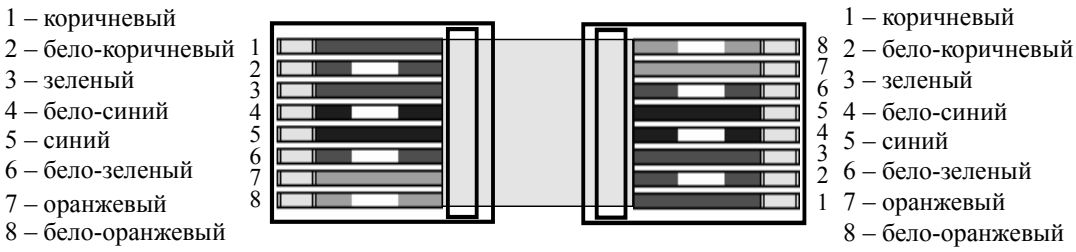
Token Ring (IEEE 802.5)

Рис. 7.11. Схема 8-пинового разъема
для сетей Token Ring

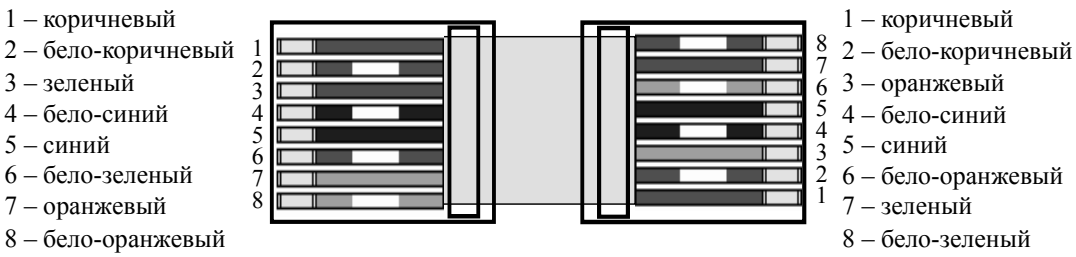
MMJ – частный стандарт для оборудования DEC, реализуется на 6-пиновом модифицированном разъеме. Разводка не совместима ни с USOC, ни с T568A/B. Первая пара выводится на 2-й и 3-й контакты, вторая на 4-й и 5-й, а третья пара занимает внешние 1-й и 6-й пины.

7.3.4. Кросс-разводка кабеля типа витая пара

Термин «*кросс-разводка*» используется применительно к разводке пар в *патч-кордах*. Всего существуют две базовые кросс-разводки – прямая и перекрестная (*рис. 7.12*).



а



б

Рис. 7.12. Схема прямой и перекрестной кросс-разводки:
а – прямая; *б* – перекрестная

Их названия говорят сами за себя. В первом случае каждый проводник выводится строго на один и тот же контакт разъемов с обоих концов кабеля. То есть 1-й контакт с одного конца соединен с 1-м на другом, 2-й – со 2-м, и так все пины. Патч-корды с подобной разводкой используются в кроссировочных узлах. При соединении с сетью оконечного оборудования, будь то персональный компьютер, факс и т. п., применяются патч-корды с перекрестной кросс-разводкой. Конкретная схема перекрестной кросс-разводки зависит от конкретной реализуемой сети, в частности, один из стандартов предполагает образование перекрестной разводки за счет перемены местами четырех пинов. Первый меняется с третьим, а второй с шестым.

7.4. Беспроводные технологии передачи данных

Методы *беспроводной технологии* (wireless) передачи данных являются удобным, а иногда незаменимым средством связи. Беспроводные технологии различаются по типам сигнала, частоте (большая частота означает большую скорость передачи) и расстоянию передачи. Большое значение имеют помехи и стоимость. Можно выделить три основных типа беспроводной технологии:

- радиосвязь;
- связь в микроволновом диапазоне;
- инфракрасная связь.

Передача данных в микроволновом диапазоне (microwaves) использует высокие частоты и применяется как на коротких, так и на больших расстояниях. Главное ограничение заключается в том, чтобы передатчик и приемник были в зоне прямой видимости. Применяется в местах, где использование физического носителя затруднено. Передача данных в микроволновом диапазоне при использовании спутников может быть очень дорогой.

Инфракрасные технологии (Infrared transmission) функционируют на очень высоких частотах, приближающихся к частотам видимого света. Они могут быть использованы для установления двусторонней или широковещательной передачи на близких расстояниях. При инфракрасной связи обычно используют светодиоды (Light Emitting Diode, LED) для передачи инфракрасных волн приемнику.

Инфракрасная передача ограничена малым расстоянием в прямой зоне видимости и может быть использована в офисных зданиях.

Технологии *радиосвязи* пересылают данные на радиочастотах и практически не имеют ограничений по дальности. Радиосвязь используется для соединения локальных сетей на больших географических расстояниях. Радиопередача в целом имеет высокую стоимость и чувствительна к электронному и атмосферному наложению, а также подвержена перехватам, поэтому требует шифрования для обеспечения уровня безопасности.

В настоящее время наибольшее распространение получила так называемая Wi-Fi связь, базирующаяся на стандарте IEEE 802.11.

Wi-Fi сеть (Wireless Local Area Network, WLAN) – это радиосеть, позволяющая передавать информацию между объектами по радиоволнам (без проводов). Разработкой стандартов в этой области занимается Wi-Fi Alliance.

WLAN-сети имеют ряд преимуществ перед обычными кабельными сетями:

– WLAN-сеть можно очень быстро развернуть, что очень удобно при проведении презентаций или в условиях работы вне офиса;

– пользователи мобильных устройств, при подключении к локальным беспроводным сетям, могут легко перемещаться в рамках действующих зон сети;

– скорости современных сетей довольно высоки (до 300 Мбит/с), что позволяет их использовать для очень широкого спектра задач;

– с помощью дополнительного оборудования беспроводная сеть может быть успешно соединена с кабельными сетями;

– WLAN-сеть может оказаться единственным выходом, если невозможна прокладка кабеля для обычной сети.

Несмотря на все достоинства, WLAN-сети обладают рядом недостатков, главный из которых – возможность легкого перехвата данных и взлома сети.

7.4.1. Требования к беспроводным локальным сетям

Беспроводные сети должны удовлетворять некоторым требованиям, типичным для всех локальных сетей, в том числе: высокая пропускная способность, возможность охвата небольших расстояний, связность подключенных станций и возможность широковещания. Кроме того, существует набор требований, характерных только для беспроводных локальных сетей. Перечислим важнейшие из них.

1. *Производительность*. Протокол управления доступом к среде должен максимально эффективно использовать беспроводную среду для максимизации пропускной способности.

2. *Число узлов*. От беспроводных локальных сетей может требоваться поддержка сотен узлов из множества ячеек.

3. *Соединение с магистральной локальной сетью*. В большинстве случаев требуется взаимосвязь со станциями магистральной локальной сети. Для беспроводных локальных сетей, имеющих внутреннюю инфраструктуру, это требование легко удовлетворяется посредством использования модулей управления, присоединяемых к локальным сетям обоих типов. Может также понадобиться специальное помещение для мобильных пользователей и организация эпизодических беспроводных сетей.

4. *Обслуживаемая область*. Типичная сфера охвата беспроводной локальной сети имеет диаметр 100–300 м.

5. *Потребление питания от батарей*. Мобильные сотрудники используют рабочие станции с питанием от батарей, потребление которого не должно быть большим при использовании беспроводных адаптеров. Это делает неприменимым протокол MAC, требующий, чтобы мобильные узлы постоянно следили за точками доступа или часто связывались с основной станцией.

6. *Устойчивость передачи и безопасность*. Беспроводные сети, если они разработаны неправильно, могут быть подвержены интерференции (наложение сигналов) и легко прослушиваться. Структура беспроводной локальной сети должна обеспечивать надежную передачу даже в обстановке шума, а также некоторый уровень зашиты от прослушивания.

7. *Совместная работа в сети*. С ростом популярности беспроводных сетей повысилась вероятность того, что две или более сетей будут работать в одной области или в нескольких областях, допускающих интерференцию разных локальных сетей. Такая интерференция может мешать нормальной работе алгоритма MAC и способствовать несанкционированному доступу к отдельной локальной сети.

8. *Работа без лицензии*. Пользователи желали бы приобретать продукты рынка беспроводных локальных сетей и работать с ними на нелицензируемой полосе частот.

9. *Переключение/роуминг*. Протокол MAC, используемый в беспроводных локальных сетях, должен позволять мобильным станциям перемещаться из одной ячейки в другую.

10. *Динамическая конфигурация*. MAC-адресация и сетевое управление локальной сети должны обеспечивать динамическое и автоматическое добавление, удаление и передислокацию конечных систем, не причиняя неудобств другим пользователям.

7.4.2. Физический уровень IEEE 802.11

Спецификация физического уровня стандарта IEEE 802.11 выпускалась в три этапа: первая часть увидела свет в 1997 году, две остальные – в 1999 году. Первая часть, именуемая просто IEEE 802.11, включала описание уровня MAC и три спецификации физического уровня – две в диапазоне 2,4 ГГц и одну в инфракрасном диапазоне, работающие при скоростях 1 и 2 Мбит/с. Спецификация IEEE 802a – это полоса 5 ГГц и скорость до 54 Мбит/с; IEEE 802.b – 2,4 ГГц и скорость 5,5 или 11 Мбит/с.

В исходном стандарте 802.11 были определены три физические среды передачи.

1. *Спектр, расширенный методом прямой последовательности*. Полоса ISM (группа нелицензируемых частот – аббревиатура состоит из названий областей, которые она затрагивает: Industria – промышленная, Scientific – научная, Medical – медицинская) – 2,4 ГГц, скорость передачи данных 1 или 2 Мбит/с.

2. *Спектр, расширенный методом скачкообразной перестройки частоты*. Полоса ISM 2,4 ГГц, скорость передачи данных 1 или 2 Мбит/с.

3. *Инфракрасный диапазон* (длина волны 850–950 нм). Скорость передачи данных 1 или 2 Мбит/с.

Расширение спектра методом прямой последовательности (DSSS). В системе DSSS может использоваться до семи каналов со скоростью передачи в каждом 1 или 2 Мбит/с. Количество доступных каналов зависит от ширины полосы, выделяемой конкретным государственным органом регулирования. В Европе, например, доступно до 13 каналов, а в Японии – только один. Ширина полосы каждого канала равна 5 МГц, схема кодирования: DBPSK – для скорости 1 Мбит/с и DQPSK – для скорости 2 Мбит/с.

Система DSSS использует раздробленный код, или псевдошумовую последовательность, для расширения скорости передачи данных, следовательно, полосы сигнала. В стандарте IEEE 802.11 определено использование последовательности Баркера.

Расширение спектра методом скачкообразной перестройки частоты (FHSS). Система FHSS использует множественные каналы, причем перестройка с одного канала на другой выполняется на основе псевдослучайной последовательности. В схеме IEEE 802.11 используются каналы шириной 1 МГц. Число каналов колеблется от 23 (Япония) до 70 (США).

Параметры схемы FHSS стандартом не задаются. В США, например, минимальная скорость перестройки частоты составляет 2,5 раза в секунду. Минимальное расстояние перехода (по частоте) в Северной Америке и большей части Европы составляет 6 МГц, в Японии – 5 МГц.

7.4.3. Стандарты для Wi-Fi сетей

Существует несколько разновидностей *WLAN-сетей*, которые различаются схемой организации сигнала, скоростями передачи данных, радиусом охвата сети, а также характеристиками радиопередатчиков и приемных устройств, параметрами передачи (шифрование, кодирование и т. д.), методами взаимодействия оборудования. В *табл. 7.3* и *7.4* представлены все основные и дополнительные стандарты спецификации IEEE 802.11.

Рассмотрим каждый из них более подробно.

Стандарт ***IEEE 802.11a*** был ратифицирован в 1999 году, но начал применяться только с 2001 года. Данный стандарт используется в основном в США и Японии. В России и в Европе он не получил широкого распространения.

В соответсвиии со стандартом предполагается использование высокочастотного диапазона (от 5,15 до 5,350 ГГц и от 5,725 до 5,825 ГГц). В США данный диапазон называют диапазоном *нелицензионной национальной информационной инфраструктуры* (Unlicensed National Information Infrastructure, UNII).

По многим параметрам протокол 802.11a мало чем отличается от протокола 802.11g. Передача данных осуществляется на скоростях 6, 9, 12 и 18 Мбит/с.

Последовательность обработки входных данных (битов) в стандарте IEEE 802.11a включает операции *избыточного кодирования* (см. подраздел 11.1) и *перемежения* (изменения исходной последовательности) данных.

Стандарт ***IEEE 802.11b*** является своего рода расширением базового протокола 802.11 и, кроме скоростей 1 и 2 Мбит/с, предусматривает скорости 5,5 и 11 Мбит/с.

Таблица 7.3

Основные стандарты беспроводных сетей

Наименование стандарта	Скорость передачи данных, Мбит/с	Обязательная поддержка скорости, Мбит/с	Число каналов	Расстояние и скорость передачи данных	Используемые ключевые технологии	Рабочая частота
IEEE 802.11a	до 54	Основные: 6; 12; 24 Дополнительные: 9; 18; 36; 48; 54	12 не перекрывающихся (4 в некоторых странах)	В закрытых помещениях: 12 м (54 Мбит/с); 91 м (6 Мбит/с) В открытых помещениях в пределах прямой видимости: 30 м (54 Мбит/с); 305 м (6 Мбит/с)	Мультиплексирование с разделением по ортогональным частотам (OFDM)	5 ГГц (5,15–5,350 ГГц и 5,725–5,825 ГГц)
IEEE 802.11b	до 11	Основные: 1; 2; 5,5; 11	3 не перекрывающиеся	В закрытых помещениях: 30 м (11 Мбит/с); 91 м (1 Мбит/с) В открытых помещениях в пределах прямой видимости: 120 м (11 Мбит/с); 460 м (1 Мбит/с)	Широкополосная модуляция с прямым расширением спектра (DSSS)	2,4 ГГц (2,4–2,4835 ГГц)
IEEE 802.11g	до 54	Основные: 1; 2; 5,5; 6; 11; 12; 24 Дополнительные: 33, 36, 48 и 54	3 не перекрывающиеся	В закрытых помещениях: 30 м (54 Мбит/с); 91 м (1 Мбит/с) В открытых помещениях в пределах прямой видимости: 120 м (54 Мбит/с); 460 м (1 Мбит/с)	Мультиплексирование с разделением по ортогональным частотам (OFDM)	2,4 ГГц (2,4–2,4835 ГГц)

Окончание табл. 7.3

Наименование стандарта	Скорость передачи данных, Мбит/с	Обязательная поддержка скорости, Мбит/с	Число каналов	Расстояние и скорость передачи данных	Используемые ключевые технологии	Рабочая частота
IEEE 802.11n	до 54	Основные: 6; 12; 24	52 (56) при ширине 20 Мгц; 104 (114) при ширине 40 Мгц	В закрытых помещениях: 12 м (54 Мбит/с); 91 м (6 Мбит/с)	Мультиплексирование с разделением по ортогональным частотам (OFDM) (с использованием технологии MIMO)	2,4 ГГц (2,4–2,4835 ГГц), 5 ГГц (5,15–5,350 ГГц и 5,725–5,825 ГГц)
		Дополнительные: 9; 18; 36; 48; 54		В открытых помещениях в пределах прямой видимости: 30 м (54 Мбит/с); 305 м (6 Мбит/с)		

Таблица 7.4

Дополнительные стандарты беспроводных сетей

Наименование стандарта	Назначение
IEEE 802.11h	Дополняет спецификации IEEE 802.11 алгоритмами эффективного выбора частот для офисных и уличных беспроводных сетей, а также средствами управления спектра
IEEE 802.11i	Предусматривает для стандартов IEEE 802.11 средства шифрования передаваемых данных, а также централизованной аутентификации пользователей и рабочих станций
IEEE 802.11j	Данный стандарт оговаривает существование в одном диапазоне сетей стандартов 802.11a и HiperLAN2. Спецификация предназначена для Японии и расширяет стандарт 802.11a добавочным каналом 4,9 ГГц
IEEE 802.11d	Стандарт определяет требования к физическим параметрам каналов (мощность излучения и диапазоны частот) и устройств беспроводных сетей с целью обеспечения их соответствия законодательным нормам различных стран
IEEE 802.11e	При сохранении полной совместимости с используемыми стандартами 802.11a и b, позволяет расширить их функциональность за счет поддержки потоковых мультимедиаданных и гарантированного качества услуг (QoS)
IEEE 802.11f	Данный стандарт определяет механизм взаимодействия точек связи между собой при перемещении клиента между сегментами сети

В стандарте применяется метод *широкополосной модуляции с прямым расширением спектра* – DSSS (Direct Sequence Spread Spectrum). Весь рабочий диапазон делится на 14 каналов, разнесенных на 25 МГц для исключения взаимных помех. Данные передаются по одному из этих каналов без переключения на другие. Возможно одновременное использование всего 3 каналов. Скорость передачи данных может автоматически меняться в зависимости от уровня помех и расстояния между передатчиком и приемником.

Стандарт IEEE 802.11b обеспечивает максимальную теоретическую скорость передачи 11 Мбит/с, что сравнимо с обычной кабельной сетью 10 Base-T Ethernet. Однако такая скорость возможна лишь при условии, что в данный момент только одно WLAN-устройство осуществляет передачу. При увеличении числа пользователей полоса пропускания делится на всех и скорость работы падает.

Стандарт ***802.11g*** окончательно был ратифицирован в июне 2003 года. Он является дальнейшей разработкой спецификации IEEE 802.11b и осуществляет передачу данных в том же частотном диапазоне.

При этом высокая скорость передачи достигается за счет одновременной передачи данных по всем каналам, тогда как скорость передачи в отдельном подканале может быть и невысокой.

При частотном разделении каналов необходимо, чтобы отдельный канал был достаточно узким для минимизации искажения сигнала, но в то же время достаточно широким для обеспечения требуемой скорости передачи. Кроме того, для экономного использования всей полосы канала, разделяемого на подканалы, желательно расположить частотные подканалы как можно ближе друг к другу, но при этом избежать *межканальной интерференции*, чтобы обеспечить их полную независимость. Частотные каналы, удовлетворяющие вышеперечисленным требованиям, называются *ортогональными*.

Рассмотренный способ деления широкополосного канала на ортогональные частотные подканалы называется **ортогональным частотным разделением с мультиплексированием** (OFDM). Одним из ключевых преимуществ метода OFDM является сочетание высокой скорости передачи с эффективным противостоянием многолучевому распространению.

В целом необходимо отметить, что в результате была достигнута скорость передачи данных 54 Мбит/с (11 Мбит/с у 802.11b),

что явилось основным преимуществом этого стандарта. Как и IEEE 802.11b, новая спецификация предусматривает использование диапазона 2,4 ГГц.

Особенностью данного стандарта является совместимость с 802.11b. Например, адаптеры 802.11b могут работать в сетях 802.11g (но при этом не быстрее 11 Мбит/с), а адаптеры 802.11g могут снижать скорость передачи данных до 11 Мбит/с для работы в старых сетях 802.11b.

Стандарт ***IEEE 802.11n*** основан на *технологии OFDM-MIMO* (Multiple Input Multiple Output). Очень многие реализованные в нем технические детали позаимствованы из стандарта 802.11a, однако в стандарте IEEE 802.11n предусматривается использование как частотного диапазона, принятого для стандарта IEEE 802.11a, так и частотного диапазона, принятого для стандартов IEEE 802.11b/g. То есть устройства, поддерживающие стандарт IEEE 802.11n, могут работать в частотном диапазоне либо 5, либо 2,4 ГГц, причем конкретная реализация зависит от страны.

Увеличение скорости передачи в стандарте IEEE 802.11n достигается, во-первых, благодаря удвоению ширины канала с 20 до 40 МГц, а во-вторых, за счет реализации технологии MIMO.

Технология MIMO (Multiple Input Multiple Output) предполагает применение нескольких передающих и принимающих антенн. По аналогии традиционные системы, то есть системы с одной передающей и одной принимающей антенной, называются SISO (Single Input Single Output).

Теоретически MIMO-система с n передающими и n принимающими антеннами способна обеспечить пиковую пропускную способность в n раз большую, чем системы SISO. Это достигается за счет того, что передатчик разбивает поток данных на независимые последовательности бит и пересылает их одновременно, используя массив антенн. Такая техника передачи называется **пространственным мультиплексированием**. Отметим, что все антенны передают данные независимо друг от друга в одном и том же частотном диапазоне.

В стандарте IEEE 802.11n предусмотрены как стандартные каналы связи шириной 20 МГц, так и каналы с удвоенной шириной. Однако применение 40-мегагерцевых каналов является опциональной возможностью стандарта, поскольку использование таких каналов может противоречить законодательству некоторых стран.

В протоколе IEEE 802.11n максимальная скорость *сверточного кодирования* равна 5/6, то есть каждые пять входных бит в сверточном кодере превращаются в шесть выходных.

Рабочая группа ***IEEE 802.11h*** дополнила существующие спецификаций 802.11 MAC (уровень доступа к среде передачи) и 802.11a PHY (физический уровень в сетях 802.11a) алгоритмами эффективного выбора частот для офисных и уличных беспроводных сетей, а также средствами управления использованием спектра, контроля за излучаемой мощностью и генерации соответствующих отчетов.

Решение этих задач базируется на использовании протоколов Dynamic Frequency Selection (DFS) и Transmit Power Control (TPC), предложенных Европейским институтом стандартов по телекоммуникациям (ETSI). Указанные протоколы предусматривают динамическое реагирование клиентов беспроводной сети на интерференцию радиосигналов путем перехода на другой канал, снижения мощности либо обоими способами.

До мая 2001 года стандартизация средств информационной безопасности для беспроводных сетей 802.11 относилась к ведению рабочей группы IEEE 802.11e, но затем эта проблематика была выделена в самостоятельное подразделение.

Разработанный стандарт ***IEEE 802.11i*** призван расширить возможности протокола 802.11 MAC, предусмотрев средства *шифрования передаваемых данных*, а также *централизованной аутентификации* пользователей и рабочих станций. В результате масштабы беспроводных локальных сетей можно будет наращивать до сотен и тысяч рабочих станций.

В основе 802.11i лежит *протокол аутентификации* Extensible Authentication Protocol (EAP), базирующийся на PPP. Сама процедура аутентификации предполагает участие в ней трех сторон – вызывающей (клиента), вызываемой (точки доступа) и сервера аутентификации (как правило, сервера RADIUS). В то же время новый стандарт, судя по всему, оставит на усмотрение производителей реализацию алгоритмов управления ключами.

Разработанные средства защиты данных должны найти применение не только в беспроводных, но и в других локальных сетях – Ethernet и Token Ring.

Целью создания данной спецификации явилось повышение уровня *безопасности беспроводных* сетей. В ней реализован на-

бор защитных функций при обмене информацией через беспроводные сети, в частности, технология AES (Advanced Encryption Standard) – алгоритм шифрования, поддерживающий ключи длиной 128, 192 и 256 бит.

Стандарт ***IEEE 802.11j*** оговаривает существование в одном диапазоне сетей стандартов 802.11a и HiperLAN2. Спецификация предназначена для Японии и расширяет стандарт 802.11a добавочным каналом 4,9 ГГц.

Стандарт ***IEEE 802.11d*** определяет требования к физическим параметрам каналов (мощность излучения и диапазоны частот) и устройств беспроводных сетей с целью обеспечения их соответствия законодательным нормам различных стран.

Спецификации стандарта ***IEEE 802.11e*** позволяют создавать *мультисервисные беспроводные локальные сети*, ориентированные на различные категории пользователей, как корпоративных, так и индивидуальных. При сохранении полной совместимости с уже принятыми стандартами 802.11a и b, он позволяет расширить их функциональность за счет поддержки *потоковых мультимедиаданных* и *гарантированного качества услуг* (QoS).

Создание данного стандарта связано с использованием средств мультимедиа. Он определяет механизм назначения приоритетов разным видам трафика, таким как аудио- и видеоприложения.

Спецификации ***IEEE 802.11f*** описывают протокол обмена служебной информацией между точками доступа (Inter Access Point Protocol, IAPP), что необходимо для построения распределенных беспроводных сетей передачи данных. Дата утверждения этих спецификаций в качестве стандарта пока не определена.

Данный стандарт, связанный с аутентификацией, определяет механизм взаимодействия точек связи между собой при перемещении клиента между сегментами сети. Другое название стандарта – Inter Access Point Protocol.

ВЫВОДЫ

1. В компьютерных сетях применяются кабели, удовлетворяющие определенным стандартам. Современные стандарты определяют характеристики не отдельного кабеля, а полного набора

элементов, необходимого для создания кабельного соединения. Сегодня наиболее употребительными стандартами являются: американский стандарт EIA/TIA-568A, международный стандарт ISO/IEC 11801, европейский стандарт EN50173, а также фирменный стандарт компании IBM.

2. Стандарты определены для четырех типов кабеля: на основе неэкранированной витой пары, на основе экранированной витой пары, коаксиального и волоконно-оптического.

3. Кабель на основе неэкранированной витой пары в зависимости от электрических и механических характеристик подразделяется на 7 категорий. В настоящее время активно используются кабели категории 5, которые были специально разработаны для поддержки высокоскоростных протоколов FDDI, Fast Ethernet, 100VG-AnyLAN, ATM и Gigabit Ethernet.

4. Особое место занимают кабели категорий 6 и 7. 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.

5. Кабель на основе экранированной витой пары хорошо защищает передаваемые сигналы от внешних помех, а пользователей сетей – от вредного для здоровья излучения. Наличие заземляемого экрана удорожает кабель и усложняет его прокладку. Экранированный кабель применяется только для передачи данных. Основным стандартом, определяющим параметры экранированной витой пары, является фирменный стандарт IBM.

6. Коаксиальные кабели представлены в большом разнообразии вариантов: «толстый» коаксиальный кабель, различные виды «тонкого» коаксиального кабеля, которые обладают худшими механическими и электрическими характеристиками по сравнению с «толстым» коаксиальным кабелем, зато за счет своей гибкости более удобны при монтаже, сюда же относится телевизионный кабель.

7. Волоконно-оптические кабели обладают отличными электромагнитными и механическими характеристиками, недостаток их состоит в сложности и высокой стоимости монтажных работ.

8. Беспроводная связь предусматривает использование трех основных технологий: радиосвязи; связи в микроволновом диапазоне; инфракрасной связи. Технологии радиосвязи пересылают данные на радиочастотах и практически не имеют ограничений по дальности. Именно они и получили набольшее распространение в настоящее время в виде так называемой Wi-Fi связи, базирующейся на стандарте IEEE 802.11.

9. Wi-Fi связь характеризуется большим числом преимуществ по сравнению с проводными системами (легко разворачивается; пользователи легко перемещаются в пределах зоны действия сети и т. д.), однако недостатком является возможность легкого перехвата данных и взлома сети, что в определенной степени может сдерживать ее распространение.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что может быть использовано в качестве физической среды передачи данных?
2. Какие вопросы при организации сети решаются на физическом уровне?
3. Что такое кабель?
4. Что такое линии связи?
5. Дайте определение каналов связи.
6. Какие проблемы существуют при организации каналов связи?
7. Дайте определение стуктурированной кабельной системы.
8. Перечислите преимущества использования стуктурированной кабельной системы.
9. Каково назначение структурированной кабельной системы?
10. Перечислите типы кабелей, используемые для передачи данных в сети.
11. Какими основными стандартами определены характеристики кабеля?
12. Перечислите основные характеристики электрических кабелей, определяемые стандартами.
13. На какие классы подразделяются кабельные системы?
14. Какие типы кабелей используются для передачи данных в сети?

15. Какие известны кабельные системы Ethernet?
16. Приведите основные характеристики кабеля типа витая пара в зависимости от категории.
17. Опишите стандартные разводки кабеля типа витая пара.
18. Какие существуют типы оптоволоконных кабелей?
19. Опишите физические особенности оптоволоконных кабелей.
20. Опишите технические особенности оптоволоконных кабелей.
21. Основные недостатки оптоволоконных кабелей.
22. Приведите основные параметры оптоволоконных кабелей.
23. Какие известны технологии беспроводной передачи данных?
24. В каких случаях используется инфракрасная связь?
25. В чем заключаются преимущества использования радиосвязи?
26. Перечислите стандарты беспроводных сетей (802.11).
27. Опишите стандарт IEEE 802.11a.
28. Опишите стандарт IEEE 802.11b.
29. Опишите стандарт IEEE 802.11g.
30. Опишите стандарт IEEE 802.11n.

8. СЕТЕВЫЕ ОПЕРАЦИОННЫЕ СИСТЕМЫ

Сетевые операционные системы (Network Operating System, NOS) – это комплекс программ, обеспечивающих обработку, хранение и передачу данных в сети.

Сетевая операционная система (СОС) составляет основу любой компьютерной сети. Каждый компьютер в сети автономен. Поэтому под ***сетевой операционной системой*** в широком смысле можно понимать совокупность операционных систем отдельных компьютеров, взаимодействующих с целью обмена сообщениями и разделения ресурсов по единым правилам – протоколам. В узком смысле **сетевая ОС** – это операционная система отдельного компьютера, обеспечивающая ему возможность работать в сети.

СОС выполняет функции прикладной платформы, предоставляет разнообразные виды сетевых служб и поддерживает работу прикладных процессов, выполняемых в абонентских системах. СОС используют клиент-серверную либо одноранговую архитектуру. Компоненты СОС располагаются на всех рабочих станциях, включенных в сеть.

СОС определяет взаимосвязанную группу протоколов верхних уровней, обеспечивающих выполнение основных функций сети. К ним, в первую очередь, относятся:

– адресация объектов сети;
– функционирование сетевых служб;
– обеспечение безопасности данных;
– управление сетью.

При выборе СОС необходимо рассматривать множество факторов. Среди них:

– набор сетевых служб, которые предоставляет сеть;
– возможность наращивания имен, определяющих хранимые данные и прикладные программы;
– механизм рассредоточения ресурсов по сети;
– способ модификации сети и сетевых служб;
– надежность функционирования и быстродействие сети;
– используемые или выбираемые физические средства соединения;

– типы компьютеров, объединяемых в сеть, их операционные системы;

– предлагаемые системы, обеспечивающие управление сетью;

– используемые средства защиты данных;

– совместимость с уже созданными прикладными процессами;

– число серверов, которое может работать в сети;

– перечень ретрансляционных систем, обеспечивающих сопряжение локальных сетей с различными территориальными сетями;

– способ документирования работы сети, организация подсказок и поддержек.

8.1. Структура сетевой операционной системы

Общая структура сетевой операционной системы представлена на *рис. 8.1*.

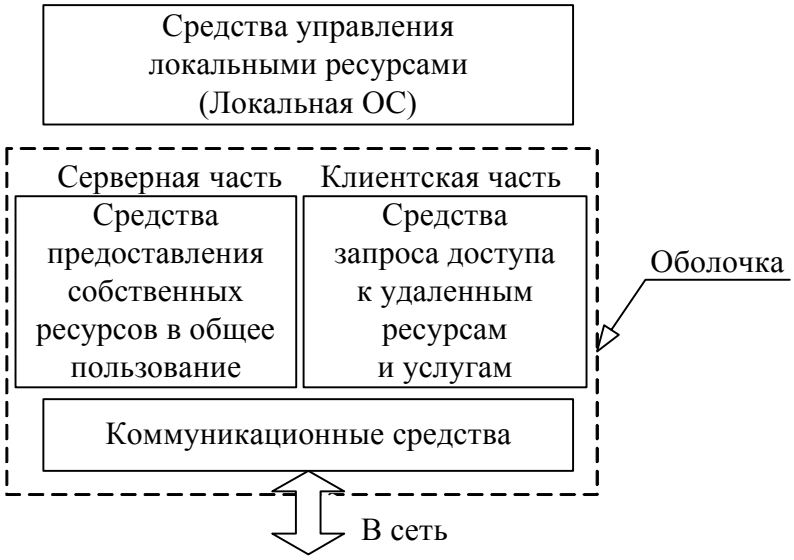


Рис. 8.1. Структура сетевой ОС

В соответствии со структурой, приведенной на *рис. 8.1*, в сетевой операционной системе отдельной машины можно выделить несколько частей.

1. *Средства управления локальными ресурсами компьютера:* функции распределения оперативной памяти между процессами, планирования и диспетчеризации процессов, управления процессорами, управления периферийными устройствами и другие функции управления ресурсами локальных ОС.

2. *Средства предоставления собственных ресурсов и услуг в общее пользование* – серверная часть ОС (сервер). Эти средства обеспечивают, например, блокировку файлов и записей, ведение справочников имен сетевых ресурсов; обработку запросов удаленного доступа к собственной файловой системе и базе данных; управление очередями запросов удаленных пользователей к своим периферийным устройствам.

3. *Средства запроса доступа к удаленным ресурсам и услугам* – клиентская часть ОС (редиректор). Эта часть выполняет распознавание и перенаправление в сеть запросов к удаленным ресурсам от приложений и пользователей. Клиентская часть также осуществляет прием ответов от серверов и преобразование их в локальный формат, так что для приложения выполнение локальных и удаленных запросов не различимо.

4. *Коммуникационные средства ОС*, с помощью которых происходит обмен сообщениями в сети. Эта часть обеспечивает адресацию и буферизацию сообщений, выбор маршрута передачи сообщения по сети, надежность передачи и прочее, т. е. является средством транспортировки сообщений.

8.2. Клиентское программное обеспечение

Для работы с сетью на клиентских рабочих станциях должно быть установлено клиентское программное обеспечение. Это программное обеспечение предоставляет доступ к ресурсам, расположенным на сетевом сервере. Тремя наиболее важными компонентами клиентского программного обеспечения являются *редиректоры* (redirector), *распределители* (designator) и *имена UNC* (UNC pathnames).

8.2.1. Редиректоры

Редиректор – сетевое программное обеспечение, которое принимает запросы ввода/вывода для *удаленных файлов*, *именованных каналов* или *почтовых слотов* и затем переназначает их сетевым сервисам другого компьютера.

Редиректор перехватывает все запросы, поступающие от приложений, и анализирует их. Фактически существуют два типа редиректоров, используемых в сети:

– *клиентский редиректор* (client redirector);
– *серверный редиректор* (server redirector).

Оба редиректора функционируют на представительском уровне модели OSI. Когда клиент делает запрос к сетевому приложению или службе, редиректор перехватывает этот запрос и проверяет, является ли ресурс локальным (находящимся на запрашивающем компьютере) или удаленным (в сети). Если редиректор определяет, что это локальный запрос, он направляет запрос центральному процессору для немедленной обработки. Если запрос предназначен для сети, редиректор направляет запрос по сети к соответствующему серверу. По существу, редиректоры скрывают от пользователя сложность доступа к сети. После того, как сетевой ресурс определен, пользователи могут получить к нему доступ без знания его точного расположения.

8.2.2. Распределители

Распределитель представляет собой часть программного обеспечения, управляющую присвоением букв накопителя (drive letter) как локальным, так и удаленным сетевым ресурсам или разделяемым дисководам, что помогает во взаимодействии с сетевыми ресурсами.

Когда между сетевым ресурсом и буквой локального накопителя создана ассоциация, известная также как отображение дисковода (mapping a drive), распределитель отслеживает присвоение такой буквы дисковода сетевому ресурсу. Затем, когда пользователь или приложение получат доступ к диску, распределитель заменит букву дисковода на сетевой адрес ресурса, прежде чем запрос будет послан редиректору.

8.2.3. Имена UNC

Редиректор и распределитель являются не единственными методами, используемыми для доступа к сетевым ресурсам.

Большинство современных сетевых операционных систем распознают **имена UNC** (Universal Naming Convention – универсальное соглашение по наименованию). UNC представляют собой стандартный способ именования сетевых ресурсов.

Эти имена имеют форму: *\\Имя_сервера\имя_ресурса*. Способные работать с UNC приложения и утилиты командной строки используют имена UNC вместо отображения сетевых дисков.

8.3. Серверное программное обеспечение

Для того чтобы компьютер мог выступать в роли сетевого сервера, необходимо установить серверную часть сетевой ОС, которая позволяет поддерживать ресурсы и распространять их среди сетевых клиентов. Важным вопросом для сетевых серверов является возможность ограничить доступ к сетевым ресурсам. Это называется *сетевой защитой* (network security). Она предоставляет средства управления над тем, к каким ресурсам могут получить доступ пользователи, степень этого доступа, а также сколько пользователей смогут получить такой доступ одновременно. Этот контроль обеспечивает конфиденциальность и защиту и поддерживает эффективную сетевую среду.

В дополнение к обеспечению контроля над сетевыми ресурсами сервер выполняет следующие функции:

– предоставляет проверку регистрационных имен (*logon identification*) для пользователей;

– управляет пользователями и группами;

– хранит инструменты сетевого администрирования для управления, контроля и аудита;

– обеспечивает отказоустойчивость для защиты целостности сети.

Некоторые из сетевых ОС, в том числе Windows, имеют программные компоненты, обеспечивающие компьютеру как клиентские, так и серверные возможности. Это позволяет компьютерам поддерживать и использовать сетевые ресурсы. В общем этот тип сетевых операционных систем не так мощен и надежен, как законченные сетевые операционные системы. Главное преимущество комбинированной клиентско-серверной сетевой операционной системы заключается в том, что важные ресурсы, расположенные на отдельной рабочей станции, могут быть разделены с остальной частью сети. Недостаток состоит в том, что если рабочая станция поддерживает много активно используемых ресурсов, она испытывает серьезное падение производительности. Если такое происходит, то необходимо перенести эти ресурсы на сервер для увеличения общей производительности.

В зависимости от функций, возлагаемых на конкретный компьютер, в его операционной системе может отсутствовать либо клиентская, либо серверная части.

На *рис. 8.2* компьютер 1 выполняет функции клиента, а компьютер 2 – функции сервера, соответственно на первой машине отсутствует серверная часть, а на второй – клиентская.

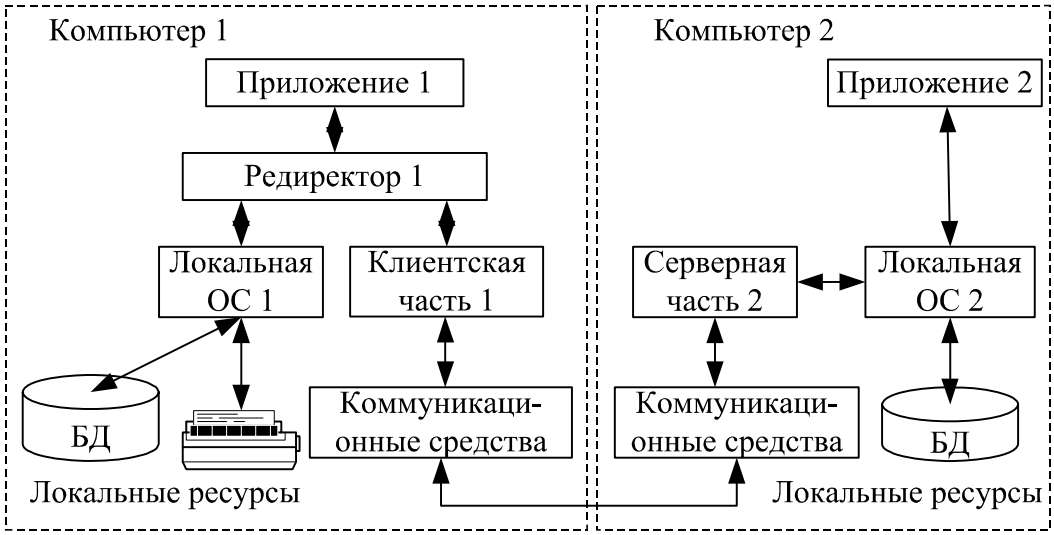


Рис. 8.2. Взаимодействие компонентов NOS

Если выдан запрос к ресурсу данного компьютера, то он переадресовывается локальной операционной системе. Если же это запрос к удаленному ресурсу, то он перенаправляется в клиентскую часть, где преобразуется из локальной формы в сетевой формат, а затем передается коммуникационным средствам. Серверная часть ОС компьютера 2 принимает запрос, преобразует его в локальную форму и передает для выполнения своей локальной ОС. После того, как результат получен, сервер обращается к транспортной подсистеме и направляет ответ клиенту, выдавшему запрос. Клиентская часть преобразует результат в соответствующий формат и адресует его тому приложению, которое выдало запрос.

При выборе сетевой операционной системы необходимо учитывать:

- совместимость оборудования;
- тип сетевого носителя;
- размер сети;
- сетевую топологию;
- требования к серверу;
- операционные системы на клиентах и серверах;

– сетевую файловую систему;
– соглашения об именах в сети;
– организацию сетевых устройств хранения.

8.4. Одноранговые и серверные сетевые операционные системы

В зависимости от того, как распределены функции между компьютерами сети, сетевые ОС могут выполнять функции как клиента, так и сервера.

Если компьютер предоставляет свои ресурсы другим пользователям сети, то он играет роль сервера. При этом компьютер, обращающийся к ресурсам другой машины, является клиентом. Компьютер, работающий в сети, может выполнять функции либо клиента, либо сервера, либо совмещать обе эти функции.

На *рис. 8.3* и *8.4* приведены примеры использования структур сетевых ОС в одноранговых сетях и сетях с выделенными серверами.

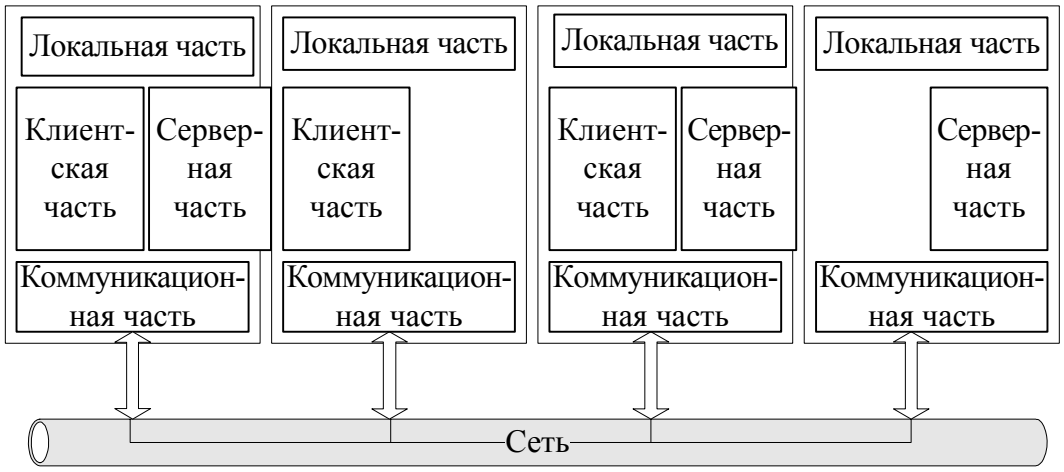


Рис. 8.3. Структура ОС для одноранговой сети

Если выполнение каких-либо серверных функций является основным назначением компьютера, то такой компьютер называется выделенным сервером. В зависимости от того, какой ресурс сервера является разделяемым, он называется файл-сервером, факс-сервером, принт-сервером, сервером приложений, сервером БД, Web-сервером и т. д. На выделенных серверах

устанавливается ОС для выполнения тех или иных серверных функций. Выделенный сервер не принято использовать в качестве компьютера для выполнения текущих задач, не связанных с его основным назначением, так как это может уменьшить производительность его работы как сервера.

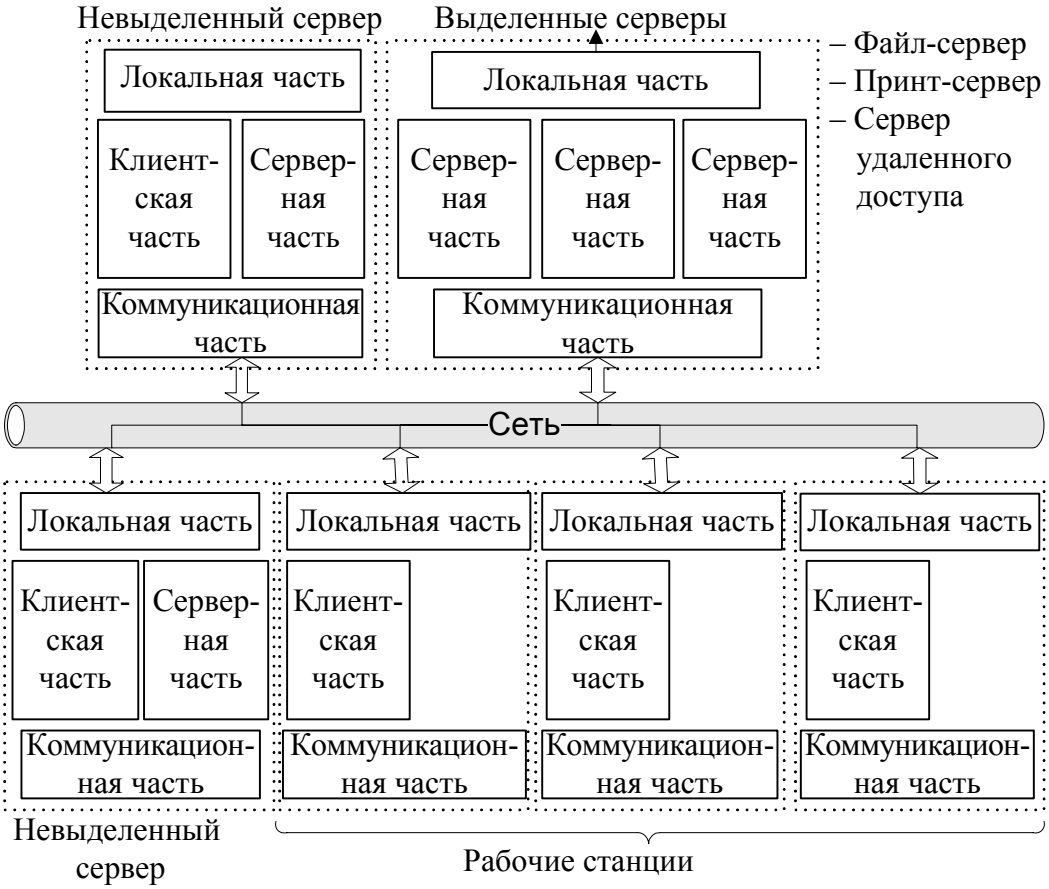


Рис. 8.4. Структура ОС для клиент-серверной сети

В *одноранговых сетях* все компьютеры равны в правах доступа к ресурсам друг друга. Каждый пользователь может по своему желанию объявить какой-либо ресурс своего компьютера разделяемым, после чего другие пользователи могут его эксплуатировать. В таких сетях на всех компьютерах устанавливается одна и та же ОС, которая предоставляет всем компьютерам в сети *потенциально* равные возможности. Одноранговые сети могут быть построены, например, на базе ОС LANtastic, Personal Ware, Windows (типа XP, Vista, Seven). Одноранговые сети проще в организации и эксплуатации. Но они применяются в основном для объединения не-

больших групп пользователей, не предъявляющих больших требований к объемам хранимой информации, ее защищенности от несанкционированного доступа и к скорости доступа.

При повышенных требованиях к этим характеристикам более подходящими являются сети с выделенными серверами, где сервер лучше решает задачу обслуживания пользователей своими ресурсами, так как его аппаратура и сетевая операционная система специально спроектированы для этой цели.

В *сетях с выделенными серверами* чаще всего используются сетевые ОС, в состав которых входит несколько вариантов ОС, отличающихся возможностями серверных частей. Например, сетевая операционная система Novell NetWare имеет серверный вариант, оптимизированный для работы в качестве файл-сервера, а также варианты оболочек для рабочих станций с различными локальными ОС, причем эти оболочки выполняют исключительно функции клиента. Другим примером ОС, ориентированной на построение сети с выделенным сервером, является операционная система Windows Server.

ВЫВОДЫ

Таким образом, сетевая операционная система – это операционная система, обеспечивающая компьютеру возможность работать в сети.

1. В общем она состоит из серверной и клиентской части, а также коммуникационных средств.

2. Для работы с сетью на клиентских рабочих станциях должно быть установлено клиентское программное обеспечение, позволяющее получить доступ к ресурсам, расположенным на сетевом сервере. Тремя наиболее важными компонентами клиентского программного обеспечения являются редиректоры, распределители и имена UNC.

3. Серверная часть сетевой операционной системы позволяет поддерживать ресурсы и распространять их среди сетевых клиентов. Однако важнейшим вопросом для сетевых серверов является возможность предоставлять средства управления над тем, к каким ресурсам могут получить доступ пользователи, уровень этого доступа. Этот контроль обеспечивает конфиденциальность и защиту предоставляемых ресурсов.

4. Отметим, что некоторые современные сетевые операционные системы, например Windows, имеют программные компоненты, обеспечивающие компьютеру как клиентские, так и серверные возможности, что позволяет компьютерам поддерживать и использовать сетевые ресурсы. Но в целом подобный тип сетевых операционных систем не так мощен и надежен, как законченные сетевые операционные системы.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что такое сетевая операционная система и каково ее назначение?
2. Какие функции сети выполняет сетевая операционная система?
3. Опишите структуру сетевой операционной системы.
4. Что такое редиректор и каковы его функции?
5. Что такое распределитель и каковы его функции?
6. Как подразделяются сетевые операционные системы по правам доступа к ресурсам?
7. В чем заключаются преимущества систем, обеспечивающие как клиентские, так и серверные возможности, и каковы их недостатки?
8. Опишите структуру одноранговой сети.
9. Опишите структуру сетей с использованием клиент-серверных ОС.
10. Как подразделяются серверы по их назначению?

9. АППАРАТНЫЕ СРЕДСТВА ДЛЯ ПЕРЕДАЧИ ДАННЫХ

9.1. Сетевые адаптеры

Сетевые адаптеры – это сетевое оборудование, обеспечивающее функционирование сети на физическом и канальном уровнях.

Сетевой адаптер относится к периферийному устройству компьютера, непосредственно взаимодействующему со средой передачи данных, которая прямо или через другое коммуникационное оборудование связывает его с другими компьютерами. Это устройство решает задачи надежного обмена двоичными данными, представленными соответствующими электромагнитными сигналами, по внешним линиям связи. Как и любой контроллер компьютера, сетевой адаптер работает под управлением *драйвера* операционной системы, и распределение функций между сетевым адаптером и драйвером может изменяться от реализации к реализации.

Компьютер, будь то сервер или рабочая станция, подключается к сети с помощью внутренней платы – сетевого адаптера (хотя бывают и внешние сетевые адаптеры, подключаемые к компьютеру через параллельный порт).

Сетевой адаптер вставляется в гнездо *материнской платы*. Карты сетевых адаптеров устанавливаются на каждой рабочей станции и на файловом сервере. Рабочая станция отправляет запрос к файловому серверу и получает ответ через сетевой адаптер, когда файловый сервер готов. Сетевые адаптеры преобразуют параллельные коды, используемые внутри компьютера и представленные маломощными сигналами, в последовательный поток мощных сигналов для передачи данных по внешней сети. Сетевые адаптеры должны быть совместимы с кабельной системой сети, внутренней информационной шиной ПК и сетевой операционной системой.

9.1.1. Назначение и настройка

Для работы ПК в сети надо правильно установить и настроить сетевой адаптер. Для адаптеров, отвечающих *стандарту PnP* (plug and play), настройка производится автоматически. В ином

случае необходимо настроить линию *запроса на прерывание* (Interrupt Request Line, IRQ) и *адрес ввода/вывода* (Input/Output address).

Адрес ввода/вывода – это трехзначное шестнадцатеричное число, которое идентифицирует коммуникационный канал между аппаратными устройствами и центральным процессором.

Чтобы сетевой адаптер функционировал правильно, должны быть настроены линия IRQ и адрес ввода/вывода. Запросы на прерывание IRQ и адреса ввода/вывода для основных устройств компьютера приведены в *таблице*.

Адреса ввода/вывода для основных устройств компьютера

Стандартное применение	Запрос на прерывание	Диапазон ввода/вывода
Системный таймер	IRQ0	
Клавиатура	IRQ1	
Вторичный контроллер IRQ или видеокарта	IRQ2	
Прерывание от асинхронного последовательного порта COM2 и COM4	IRQ3	От 2F0 до 2FF
Прерывание от асинхронного последовательного порта COM1 и COM3	IRQ4	От 3F0 до 3FF
Обычно свободен (может быть занят параллельным портом LPT2)	IRQ5	
Контроллер флоппи-диска	IRQ6	
Прерывание от параллельного принтерного порта LPT1	IRQ7	
Обычно свободен	IRQ9	От 370 до 37F
Обычно свободен (может быть занят первичным контроллером SCSI)	IRQ10	
Обычно свободен (может быть занят вторичным контроллером SCSI)	IRQ11	IRQ11
Мышь PS/2	IRQ12	IRQ12
Прерывание от сопроцессора	IRQ13	IRQ13
Прерывание от первичного контроллера жесткого диска	IRQ14	IRQ14
Обычно свободен (может быть занят вторичным контроллером жесткого диска IDE)	IRQ15	IRQ15

Обычно сетевая карта обнаруживает конфликт, если двум устройствам назначен один и тот же ресурс (запрос на прерывание или адрес ввода/вывода). Сетевые карты поддерживают различные типы сетевых соединений.

Физический интерфейс между самой сетевой картой и сетью называют **трансивером** (transceiver) – устройство, которое как получает, так и посылает данные.

Трансиверы на сетевых картах могут получать и посылать цифровые и аналоговые сигналы. Тип интерфейса, который использует сетевая карта, часто может быть физически определен на сетевой карте. Перемычки, или джамперы (маленькие перемычки, соединяющие два контакта), могут быть настроены для указания типа трансивера, который должна использовать сетевая карта в соответствии со схемой сети. Например, перемычка в одном положении может включить разъем RJ-45 для поддержки сети типа витая пара, в другом – поддержку внешнего трансивера.

9.1.2. Функции сетевых адаптеров

Сетевые адаптеры производят семь основных операций при приеме или передаче сообщения.

1. *Гальваническая развязка* с коаксиальным кабелем или витой парой. Для этой цели используются импульсные трансформаторы. Иногда для развязки используются оптроны.

2. *Прием (передача) данных*. Данные передаются из ОЗУ ПК в адаптер или из адаптера в память ПК через программируемый канал ввода/вывода, канал прямого доступа или разделяемую память.

3. *Буферизация*. Для согласования скоростей пересылки данных в адаптер или из него со скоростью обмена по сети используются буфера. Во время обработки в сетевом адаптере данные хранятся в буфере. Буфер позволяет адаптеру осуществлять доступ ко всему пакету информации. Использование буферов необходимо для согласования между собой скоростей обработки информации различными компонентами ЛВС.

4. *Формирование пакета*. Сетевой адаптер должен разделить данные на блоки в режиме передачи (или соединить их в режиме приема) данных и оформить в виде кадра определенного формата. Кадр включает несколько служебных полей, среди которых имеется адрес компьютера назначения и контрольная сумма кадра, по которой сетевой адаптер станции назначения делает вывод о корректности доставленной по сети информации.

5. *Доступ к каналу связи.* Набор правил, обеспечивающих доступ к среде передачи. Выявление конфликтных ситуаций и контроль состояния сети.

6. *Идентификация своего адреса в принимаемом пакете*. Физический адрес адаптера может определяться установкой переключателей, храниться в специальном регистре или прошиваться в ППЗУ.

7. *Преобразование параллельного кода в последовательный код* при передаче данных и из последовательного кода в параллельный при приеме. В режиме передачи данные передаются по каналу связи в последовательном коде.

8. *Кодирование и декодирование данных.* На этом этапе должны быть сформированы электрические сигналы, используемые для представления данных. Большинство сетевых адаптеров для этой цели используют *манчестерское кодирование*. Этот метод не требует передачи синхронизирующих сигналов для распознавания единиц и нулей по уровням сигналов, а вместо этого для представления 1 и 0 используется перемена полярности сигнала.

9. *Передача или прием импульсов.* В режиме передачи закодированные электрические импульсы данных передаются в кабель (при приеме импульсы направляются на декодирование).

Сетевые адаптеры вместе с сетевым программным обеспечением способны распознавать и обрабатывать ошибки, которые могут возникнуть из-за электрических помех, коллизий или плохой работы оборудования.

Последние типы сетевых адаптеров поддерживают технологию *Plug and Play*. Если сетевую карту установить в компьютер, то при первой загрузке система определит тип адаптера и запросит для него драйверы.

Некоторые сетевые адаптеры имеют возможность использовать оперативную память ПК в качестве буфера для хранения входящих и исходящих пакетов данных. *Базовый адрес* (Base Memory Address) представляет собой шестнадцатеричное число, которое указывает на адрес в оперативной памяти, где находится этот буфер. Важно выбрать базовый адрес без конфликтов с другими устройствами.

9.1.3. Типы сетевых адаптеров

Сетевые адаптеры различаются по типу и разрядности используемой в компьютере внутренней шины данных – ISA, PCI, PCI-E.

Сетевые адаптеры различаются также по типу принятой в сети технологии – Ethernet, Token Ring, FDDI и т. п. Как правило,

конкретная модель сетевого адаптера работает по определенной сетевой технологии (например, Ethernet). В связи с тем, что для каждой технологии сейчас имеется возможность использования различных сред передачи данных (тот же Ethernet поддерживает коаксиальный кабель, неэкранированную витую пару и оптоволоконный кабель), сетевой адаптер может поддерживать как одну, так и одновременно несколько сред. В случае, когда сетевой адаптер поддерживает только одну среду передачи данных, а необходимо использовать другую, применяются трансиверы и конверторы.

Различные типы сетевых адаптеров отличаются не только методами доступа к среде и протоколами, но еще и следующими параметрами:

- скорость передачи;
- объем буфера для пакета;
- тип шины;
- быстродействие шины;
- совместимость с различными микропроцессорами;
- использование прямого доступа к памяти (DMA);
- адресация портов ввода/вывода и запросов прерывания;
- конструкция разъема.

Классификация сетевых адаптеров. В качестве примера классификации адаптеров можно использовать подход фирмы 3Com, имеющей репутацию лидера в области адаптеров Ethernet. Фирма 3Com считает, что сетевые адаптеры Ethernet прошли в своем развитии три поколения.

Сетевые адаптеры *первого поколения* были выполнены на дискретных логических микросхемах, в результате чего обладали низкой надежностью. Они имели буферную память только на один кадр, что приводило к низкой производительности адаптера, так как все кадры передавались из компьютера в сеть или из сети в компьютер последовательно. Кроме этого, задание конфигурации адаптера первого поколения происходило вручную, с помощью перемычек. Для каждого типа адаптеров использовался свой драйвер, причем интерфейс между драйвером и сетевой операционной системой не был стандартизирован.

В сетевых адаптерах *второго поколения* для повышения производительности стали применять метод *многокадровой буферизации*. При этом следующий кадр загружается из памяти компьютера в буфер адаптера одновременно с передачей предыдущего кадра

в сеть. В режиме приема, после того как адаптер полностью принял один кадр, он может начать передавать этот кадр из буфера в память компьютера одновременно с приемом другого кадра из сети.

В сетевых адаптерах второго поколения широко используются микросхемы с высокой степенью интеграции, что повышает надежность адаптеров. Кроме того, драйверы этих адаптеров основаны на стандартных спецификациях. Адаптеры второго поколения обычно поставляются с драйверами, работающими как в стандарте NDIS (*спецификация интерфейса сетевого драйвера*), разработанном фирмами 3Com и Microsoft и одобренном IBM, так и в стандарте ODI (*интерфейс открытого драйвера*), разработанном фирмой Novell.

В сетевых адаптерах *третьего поколения* (к ним фирма 3Com относит свои адаптеры семейства EtherLink III) осуществляется *конвейерная схема обработки кадров*. Она заключается в том, что процессы приема кадра из оперативной памяти компьютера и передачи его в сеть совмещаются во времени. Таким образом, после приема нескольких первых байт кадра начинается их передача. Это существенно (на 25–55 %) повышает производительность цепочки *оперативная память – адаптер – физический канал – адаптер – оперативная память*. Такая схема очень чувствительна к порогу начала передачи, то есть к количеству байт кадра, которое загружается в буфер адаптера перед началом передачи в сеть. Сетевой адаптер третьего поколения осуществляет самонастройку этого параметра путем анализа рабочей среды, а также методом расчета без участия администратора сети. Самонастройка обеспечивает максимально возможную производительность для конкретного сочетания производительности внутренней шины компьютера, его системы прерываний и системы прямого доступа к памяти.

Адаптеры третьего поколения базируются на специализированных интегральных схемах (ASIC), что повышает производительность и надежность адаптера при одновременном снижении его стоимости. Компания 3Com назвала свою технологию конвейерной обработки кадров Parallel Tasking, другие компании также реализовали похожие схемы в своих адаптерах. Повышение производительности канала *адаптер – память* очень важно для повышения производительности сети в целом, так как производительность сложного маршрута обработки кадров, включающего, например, концентраторы, коммутаторы, маршрутизаторы, гло-

бальные каналы связи и т. п., всегда определяется производительностью его самого медленного элемента. Следовательно, если сетевой адаптер сервера или клиентского компьютера работает медленно, никакие быстрые коммутаторы не смогут повысить скорость работы сети.

Выпускаемые сегодня сетевые адаптеры можно отнести к *четвертому поколению*. В эти адаптеры обязательно входят элементы ASIC, выполняющие функции MAC-уровня, а также большое количество высокоуровневых функций. В набор таких функций может входить *поддержка агента удаленного мониторинга* RMON, схема приоритезации кадров, функции дистанционного управления компьютером и т. п. В серверных вариантах адаптеров почти обязательно наличие мощного процессора, разгружающего центральный процессор. Примером сетевого адаптера четвертого поколения может служить адаптер компании Intel – Intel PRO/1000 MT Desktop или Hardlink HA-32G фирмы MAS Elektronik AG.

Современные сетевые адаптеры, как правило, поддерживают следующие *функции*.

1. *PCI BUS-Mastering*. Данная функция означает возможность пересылки данных устройством без участия центрального процессора. На сетевой карте должны быть распаяны схемы, позволяющие осуществлять прямую передачу информации.

2. *BootRom*. Возможность загрузки системы по сети заложена в виде BootRom сетевой карты. Это микросхема энергонезависимой памяти, где хранится код загрузчика. Он выполняет поиск в сети сервера и запрашивает у него IP-адрес, а также путь, указывающий, где можно получить образ операционной системы. После того, как образ загружен и размещен в оперативной памяти, дальнейшее управление загрузкой передается ему точно так, как при работе с обычной загрузочной дискетой или диском. Таким образом, при соответствующей настройке ПК может работать вообще без жесткого диска. Загрузка через сеть настраивается в BIOS материнских плат, которые поддерживают данную функцию.

3. *Wake-on-Lan*. Данная технология представляет собой включение удаленной системы через сеть. Адаптер отслеживает сетевой траффик в ожидании специального Wake-пакета и при его получении пробуждает систему. При этом требуется, чтобы в настройках BIOS была разрешена активация компьютера по запросу с порта, на который установлена карта.

Выводы

1. От производительности сетевых адаптеров зависит производительность любой сложной сети, так как данные всегда проходят не только через коммутаторы и маршрутизаторы сети, но и через адаптеры компьютеров, а результирующая производительность последовательно соединенных устройств определяется производительностью самого медленного устройства.

2. Сетевые адаптеры характеризуются производительностью, шиной компьютера, к которой они могут присоединяться, типом приемопередатчика, а также наличием собственного процессора (его характеристиками и возможностями), разгружающего центральный процессор компьютера.

3. Сетевые адаптеры для серверов обычно имеют собственный процессор, а клиентские сетевые адаптеры – нет.

4. Современные адаптеры умеют адаптироваться к временным параметрам шины и оперативной памяти компьютера для повышения производительности обмена *сеть – компьютер*.

9.2. Повторители и концентраторы

Основная функция **повторителя** (repeater), как это следует из его названия, – повторение сигналов, поступающих на его порт. Повторитель улучшает электрические характеристики сигналов и их синхронность, и за счет этого появляется возможность увеличивать общую длину кабеля между самыми удаленными в сети узлами.

Многопортовый повторитель часто называют *концентратором* (concentrator) или *хабом* (hub), что отражает тот факт, что данное устройство реализует не только функцию повторения сигналов, но и концентрирует в одном центральном устройстве функции объединения компьютеров в сеть.

Практически во всех современных сетевых стандартах концентратор является необходимым элементом сети, соединяющим отдельные компьютеры в сеть.

Концентратор представляет собой сетевое устройство, действующее на физическом уровне сетевой модели OSI.

Отрезки кабеля, соединяющие два компьютера или какие-либо два других сетевых устройства, называются **физическими**

сегментами, поэтому концентраторы и повторители, которые используются для добавления новых физических сегментов, являются средством физической структуризации сети.

Концентратор – устройство, у которого суммарная пропускная способность входных каналов выше пропускной способности выходного канала (*рис. 9.1*).

Рис. 9.1. Внешний вид концентратора фирмы D-Link

Так как потоки входных данных в концентраторе больше выходного потока, то главной его задачей является концентрация данных. При этом возможны ситуации, когда число блоков данных, поступающих на входы концентратора, превышает его возможности. Тогда концентратор ликвидирует часть этих блоков.

Ядром концентратора является *процессор*. Для объединения входной информации чаще всего используется *множественный доступ с разделением времени*. Функции, выполняемые концентратором, близки к задачам, возложенным на мультиплексор. Наращиваемые (модульные) концентраторы позволяют выбирать их компоненты, не анализируя совместимость с уже используемыми. Современные концентраторы имеют порты для подключения к разнообразным локальным сетям.

Концентратор является активным оборудованием, служит центром (шиной) звездообразной конфигурации сети и обеспечивает подключение сетевых устройств. В концентраторе для каждого узла (ПК, принтеры, серверы доступа, телефоны и пр.) должен быть предусмотрен отдельный порт.

Наращиваемые концентраторы представляют собой отдельные модули, которые объединяются при помощи быстродействующей системы связи. Такие концентраторы предоставляют удобный способ поэтапного расширения возможностей и мощности ЛВС.

Концентратор осуществляет электрическую развязку отрезков кабеля до каждого узла, поэтому короткое замыкание на одном из отрезков не выведет из строя всю ЛВС.

Концентраторы образуют из отдельных физических отрезков кабеля общую среду передачи данных – **логический сегмент**.

Логический сегмент также называют *доменом коллизий*, поскольку при попытке одновременной передачи данных любых двух компьютеров этого сегмента, хотя бы и принадлежащих разным физическим сегментам, возникает блокировка передающей среды. Следует особо подчеркнуть, что, какую бы сложную структуру ни образовывали концентраторы, например, путем иерархического соединения, все компьютеры, подключенные к ним, образуют единый логический сегмент, в котором любая пара взаимодействующих компьютеров полностью блокирует возможность обмена данными для других компьютеров.

Концентраторы поддерживают технологию Plug and Play и не требуют какой-либо установки параметров. Необходимо просто спланировать свою сеть и вставить разъемы в порты концентратора и компьютеров.

9.2.1. Планирование сети с концентратором

При выборе места для установки концентратора следует принять во внимание следующие аспекты:

- местоположение;
- расстояние;
- питание.

Выбор места установки концентратора является наиболее важным этапом планирования небольшой сети. Хаб разумно расположить вблизи геометрического центра сети (на одинаковом расстоянии от всех компьютеров). Такое расположение позволит минимизировать расход кабеля. Длина кабеля от концентратора до любого из подключаемых к сети компьютеров или периферийных устройств не должна превышать 100 м.

Концентратор можно поставить на стол или закрепить его на стене с помощью входящих в комплект хаба скоб. Установка хаба на стене позволяет упростить подключение кабелей, если они уже проложены в офисе.

При планировании сети необходимо предусматривать возможность наращивания (каскадирования) хабов.

9.2.2. Преимущества концентратора

Концентраторы имеют много преимуществ. Во-первых, в сети используется топология звезда, при которой соединения с компьютерами образуют лучи, а хаб является центром звезды. Такая топология упрощает установку и управление сети. Любые перемещения компьютеров или добавление в сеть новых узлов при такой топологии совсем несложно выполнить. Кроме того, эта топология значительно надежнее, поскольку при любом повреждении кабельной системы сеть сохраняет работоспособность (перестает работать лишь поврежденный луч). Светодиодные индикаторы хаба позволяют контролировать состояние сети и легко обнаруживать неполадки.

Различные производители концентраторов реализуют в своих устройствах различные наборы вспомогательных функций, но наиболее часто встречаются следующие:

– объединение сегментов с различными физическими средами (например, коаксиал, витая пара и оптоволокно) в единый логический сегмент;

– автосегментация портов – автоматическое отключение порта при его некорректном поведении (повреждение кабеля, интенсивная генерация пакетов ошибочной длины и т. п.);

– поддержка между концентраторами резервных связей, которые используются при отказе основных;

– защита передаваемых по сети данных от несанкционированного доступа (например, путем искажения поля данных в кадрах, повторяемых на портах, не содержащих компьютер с адресом назначения);

– поддержка средств управления сетями – протокола SNMP, баз управляющей информации MIB.

9.2.3. Многосегментные концентраторы

При рассмотрении некоторых моделей концентраторов возникает вопрос: зачем в этой модели имеется такое большое количество портов, например, 192 или 240? Имеет ли смысл разделять среду в 10 или 100 Мбит/с между таким большим количеством станций? В таких концентраторах имеется несколько несвязанных внутренних шин, которые предназначены для создания нескольких разделяемых сред. Например, концентратор имеет три внутренние шины Ethernet. Если в таком концентраторе

72 порта, то каждый из этих портов может быть связан с любой из трех внутренних шин. Между собой компьютеры, подключенные к разным сегментам, общаться через концентратор не могут, так как шины внутри концентратора никак не связаны.

Многосегментные концентраторы нужны для создания разделяемых сегментов, состав которых может легко изменяться. Большинство многосегментных концентраторов, например, System 5000 компании Nortel Networks или PortSwitch Hub компании 3Com, позволяют выполнять операцию соединения порта с одной из внутренних шин чисто программным способом, например, с помощью локального конфигурирования через консольный порт. В результате администратор сети может присоединять компьютеры пользователей к любым портам концентратора, а затем с помощью программы конфигурирования концентратора управлять составом каждого сегмента. Если вдруг сегмент 1 станет перегруженным, то его компьютеры можно распределить между оставшимися сегментами концентратора.

Многосегментные концентраторы – это программируемая основа больших сетей.

Возможность многосегментного концентратора программно изменять связи портов с внутренними шинами называется **конфигурационной коммутацией** (configuration switching).

Для соединения сегментов между собой нужны устройства другого типа – ***мосты*** или ***коммутаторы*** (см. подраздел 9.3). Такое межсетевое устройство должно подключаться к нескольким портам многосегментного концентратора, подсоединенным к разным внутренним шинам, и выполнять передачу кадров или пакетов между сегментами точно так же, как если бы они были образованы отдельными устройствами-концентраторами.

Для крупных сетей многосегментный концентратор играет роль *интеллектуального кроссового шкафа*, который выполняет новое соединение не за счет механического перемещения вилки кабеля в новый порт, а за счет программного изменения внутренней конфигурации устройства.

9.2.4. Конструктивное исполнение концентраторов

На конструктивное устройство концентраторов большое влияние оказывает их область применения. Концентраторы рабочих групп чаще всего выпускаются как устройства с фиксирован-

ным количеством портов, корпоративные концентраторы – как модульные устройства на основе шасси, а концентраторы отделов могут иметь стековую конструкцию. Такое деление не является жестким, и в качестве корпоративного концентратора может использоваться, например, модульный концентратор.

Концентратор с фиксированным количеством портов – это наиболее простое конструктивное исполнение, когда устройство представляет собой отдельный корпус со всеми необходимыми элементами (портами, органами индикации и управления, блоком питания), и эти элементы заменять нельзя.

Обычно все порты такого концентратора поддерживают одну среду передачи, общее количество портов изменяется от 4–8 до 24. Один порт может быть специально выделен для подключения концентратора к магистрали сети или же для объединения концентраторов (в качестве такого порта часто используется порт с интерфейсом AUI, в этом случае применение соответствующего трансивера позволяет подключить концентратор к практически любой физической среде передачи данных).

Модульный концентратор выполняется в виде отдельных модулей с фиксированным количеством портов, устанавливаемых на общее шасси.

Шасси имеет внутреннюю шину для объединения отдельных модулей в единый повторитель. Часто такие концентраторы являются многосегментными, тогда в пределах одного модульного концентратора работает несколько несвязанных между собой повторителей. Для модульного концентратора могут существовать различные типы модулей, отличающиеся количеством портов и типом поддерживаемой физической среды. Часто агент протокола SNMP выполняется в виде отдельного модуля, при установке которого концентратор превращается в интеллектуальное устройство. Модульные концентраторы позволяют более точно подобрать необходимую для конкретного применения конфигурацию концентратора, а также гибко и с минимальными затратами реагировать на изменения конфигурации сети.

Ввиду ответственной работы, которую выполняют корпоративные модульные концентраторы, они снабжаются модулем управления, системой терморегулирования, избыточными источниками питания и возможностью замены модулей «на ходу».

Недостатком концентратора на основе шасси является высокая начальная стоимость такого устройства для случая, когда предприятию на первом этапе создания сети нужно установить всего 1–2 модуля. Высокая стоимость шасси вызвана тем, что оно поставляется вместе со всеми общими устройствами, такими как избыточные источники питания и т. п. Поэтому для сетей средних размеров большую популярность завоевали стековые концентраторы.

Стековый концентратор, как и концентратор с фиксированным числом портов, выполнен в виде отдельного корпуса без возможности замены отдельных его модулей.

Однако стековыми эти концентраторы называются не потому, что они устанавливаются один на другой. Такая чисто конструктивная деталь вряд ли удостоилась бы особого внимания, так как установка нескольких устройств одинаковых габаритных размеров в общую стойку практикуется очень давно. Стековые концентраторы имеют специальные порты и кабели для объединения нескольких таких корпусов в единый повторитель, который имеет общий блок повторения, обеспечивает общую ресинхронизацию сигналов для всех своих портов и поэтому с точки зрения правила 4 хабов считается одним повторителем.

Если стековые концентраторы имеют несколько внутренних шин, то при соединении в стек эти шины объединяются и становятся общими для всех устройств стека. Число объединяемых в стек корпусов может быть достаточно большим (обычно до 8, но бывает и больше). Стековые концентраторы могут поддерживать различные физические среды передачи, что делает их почти такими же гибкими, как и модульные концентраторы, но при этом стоимость этих устройств в расчете на один порт получается обычно ниже, так как сначала предприятие может купить одно устройство без избыточного шасси, а потом нарастить стек еще несколькими аналогичными устройствами.

Стековые концентраторы, выпускаемые одним производителем, выполняются в едином конструктивном стандарте, что позволяет легко устанавливать их друг на друга, образуя единое настольное устройство, или помещать их в общую стойку. Экономия при организации стека происходит еще и за счет единого для всех

устройств стека модуля SNMP-управления (который вставляется в один из корпусов стека как дополнительный модуль), а также общего избыточного источника питания.

Модульно-стековые концентраторы представляют собой модульные концентраторы, объединенные специальными связями в стек. Как правило, корпуса таких концентраторов рассчитаны на небольшое количество модулей (1–3). Эти концентраторы сочетают достоинства концентраторов обоих типов.

Выводы

1. Концентраторы, кроме основной функции протокола (побитного повторения кадра на всех портах или на последующем порту), всегда выполняют ряд полезных дополнительных функций, определяемых производителем концентратора.
2. Автосегментация – одна из важнейших дополнительных функций, с помощью которой концентратор отключает порт при обнаружении разнообразных проблем с кабелем и конечным узлом, подключенным к данному порту.
3. В число дополнительных функций входят функции защиты сети от несанкционированного доступа, запрещающие подключение к концентратору компьютеров с неизвестными MAC-адресами, а также заполняющие нулями поля данных кадров, поступающих не к станции назначения.
4. Стековые концентраторы сочетают преимущества модульных концентраторов и концентраторов с фиксированным количеством портов. Многосегментные концентраторы позволяют делить сеть на сегменты программным способом, без физической перекоммутации устройств.
5. Сложные концентраторы, выполняющие дополнительные функции, обычно могут управляться централизованно по сети по протоколу SNMP.

9.3. Мосты и коммутаторы

9.3.1. Мосты

Мост (bridge) – ретрансляционная система, соединяющая каналы передачи данных (*рис. 9.2*).

Рис. 9.2. Внешний вид беспроводного сетевого моста

В соответствии с базовой эталонной моделью взаимодействия открытых систем мост описывается протоколами физического и канального уровней, над которыми располагаются канальные процессы. Мост опирается на пару связываемых им физических средств соединения, которые в этой модели представляют физические каналы. Мост преобразует физический (1A, 1B) и канальный (2A, 2B) уровни различных типов (*рис. 9.3*). Что касается канального процесса, то он объединяет разнотипные каналы передачи данных в один общий.

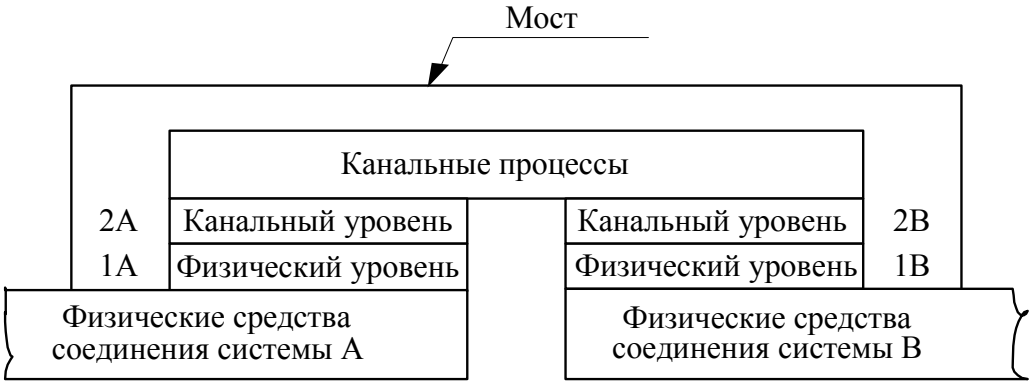


Рис. 9.3. Структура моста

Мост, а также его быстродействующий аналог *коммутатор* (switching hub) делят общую среду передачи данных на логические сегменты.

Логический сегмент образуется путем объединения нескольких физических сегментов (отрезков кабеля) с помощью одного или нескольких концентраторов. Каждый логический сегмент подключается к отдельному порту моста/коммутатора. При поступлении кадра на какой-либо из портов мост/коммутатор повторяет

этот кадр, но не на всех портах, как это делает концентратор, а только на том порту, к которому подключен сегмент, содержащий компьютер-адресат.

Мосты могут соединять сегменты, использующие разные типы носителей, например, 10BaseT, 100BaseT, 1000BaseT (витая пара), 10Base2 (тонкий коаксиальный кабель) и 1000BaseFX (оптоволокно). Они могут соединять сети с разными методами доступа к каналу, например, сети Ethernet (метод доступа CSMA/CD) и Token Ring (метод доступа TPMA).

Мосты используются только для связи локальных сетей с глобальными, то есть как средства удаленного доступа, поскольку в этом случае необходимость в параллельной передаче между несколькими парами портов просто не возникает (*рис. 9.4*).

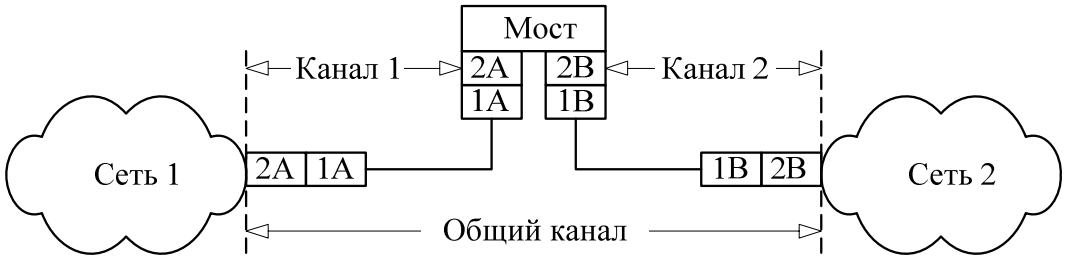


Рис. 9.4. Соединение двух сетей при помощи двух каналов

По мере развития данного типа оборудования, они стали многопортовыми и получили название *коммутаторов* (switch). Некоторое время оба понятия существовали одновременно, а позднее вместо термина «*мост*» стали применять «*коммутатор*». Далее в этой теме будет использоваться термин «коммутатор» для обозначения этих обеих разновидностей устройств, поскольку все сказанное ниже в равной степени относится и к мостам, и к коммутаторам. Следует отметить, что в последнее время локальные мосты полностью вытеснены коммутаторами.

Нередки случаи, когда необходимо соединить локальные сети, в которых различаются лишь протоколы физического и канального уровней. Протоколы остальных уровней в этих сетях приняты одинаковыми. Такие сети могут быть соединены мостом. Часто мосты наделяются дополнительными функциями. Такие мосты обладают определенным интеллектом (интеллектом в сетях называют действия, выполняемые устройствами) и фильтруют сквозь

себя блоки данных, адресованные абонентским системам, расположенным в той же сети. Для этого в памяти каждого моста имеются адреса систем, включенных в каждую из сетей. Блоки, проходящие через интеллектуальный мост, дважды проверяются, на входе и выходе. Это позволяет предотвращать появление ошибок внутри моста.

Мосты не имеют механизмов управления потоками блоков данных. Поэтому может оказаться, что входной поток блоков окажется большим, чем выходной. В этом случае мост не справится с обработкой входного потока, и его буферы могут переполняться. Чтобы этого не произошло, избыточные блоки выбрасываются. Специфические функции выполняет мост в радиосети. Здесь он обеспечивает взаимодействие двух радиоканалов, работающих на разных частотах. Его именуют ***ретранслятором***.

Таким образом, мосты оперируют данными на высоком уровне и имеют совершенно определенное назначение. Во-первых, они предназначены для соединения сетевых сегментов, имеющих различные физические среды, например, для соединения сегмента с оптоволоконным кабелем и сегмента с коаксиальным кабелем. Мосты также могут быть использованы для связи сегментов, имеющих различные протоколы низкого уровня (физического и канального).

9.3.2. Коммутатор

Коммутатор (switch) – устройство, осуществляющее выбор одного из возможных вариантов направления передачи данных (*рис. 9.5*).

Рис. 9.5. Внешний вид коммутатора фирмы Cisco

Общая структура коммутатора аналогична стуктуре моста (внешний вид одного из них показан на *рис. 9.3*), т. е. современные

коммутаторы оперируют не только на физическом, но и на канальном уровне модели OSI.

В коммуникационной сети коммутатор является ретрансляционной системой (система, предназначенная для передачи данных или преобразования протоколов), обладающей свойством прозрачности (т. е. коммутация осуществляется здесь без какой-либо обработки данных). Коммутатор не имеет буферов и не может накапливать данные. Поэтому при использовании коммутатора скорости передачи сигналов в соединяемых каналах передачи данных должны быть одинаковыми. Канальные процессы, реализуемые коммутатором, выполняются специальными интегральными схемами. В отличие от других видов ретрансляционных систем, здесь, как правило, не используется программное обеспечение.

Коммутатор может соединять серверы в кластер и служить основой для объединения нескольких рабочих групп. Он направляет пакеты данных между узлами ЛВС. Каждый коммутируемый сегмент получает доступ к каналу передачи данных без конкуренции и видит только тот трафик, который направляется в его сегмент. Коммутатор должен предоставлять каждому порту возможность соединения с максимальной скоростью без конкуренции со стороны других портов (в отличие от совместно используемого концентратора). Обычно в коммутаторах имеется один или два высокоскоростных порта, а также достаточные инструментальные средства для решения задач управления.

Коммутатором можно заменить маршрутизатор, дополнить им наращиваемый маршрутизатор или использовать коммутатор в качестве основы для соединения нескольких концентраторов. Коммутатор может служить отличным устройством для направления трафика между концентраторами ЛВС рабочей группы и загруженными файл-серверами.

Коммутатор локальной сети (local area network switch) – устройство, обеспечивающее взаимодействие сегментов одной либо группы локальных сетей.

Коммутатор локальной сети, как и обычный коммутатор, обеспечивает взаимодействие подключенных к нему локальных сетей (*рис. 9.6*).

В дополнение к основной функции он осуществляет преобразование интерфейсов, если соединяются различные типы

сегментов локальной сети. Чаще всего это сети Ethernet, кольцевые сети IBM, сети с оптоволоконным распределенным интерфейсом данных.

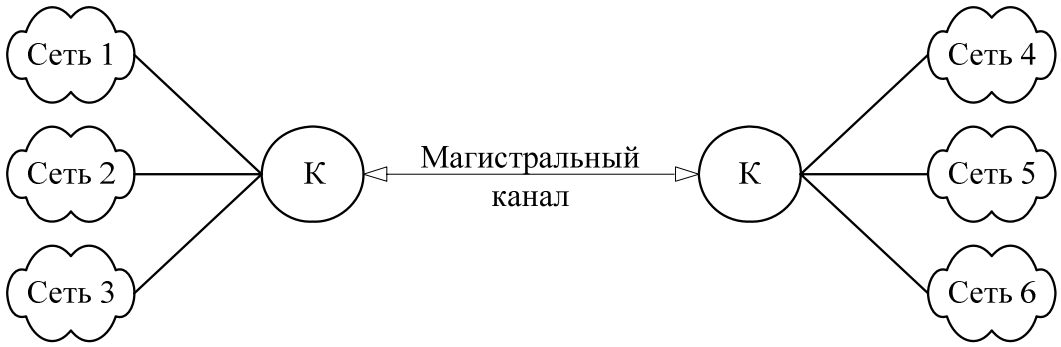


Рис. 9.6. Схема подключения локальных сетей к коммутаторам

В перечень функций, выполняемых коммутатором локальной сети, входят:

- обеспечение сквозной коммутации;
- наличие средств маршрутизации;
- поддержка простого протокола управления сетью;
- имитация моста либо маршрутизатора;
- организация виртуальных сетей;
- скоростная ретрансляция блоков данных.

В заключение необходимо отметить, что, несмотря на сходство мостов и коммутаторов, ключевая разница между ними состоит в том, что *мост в каждый момент времени может осуществлять передачу кадров только между одной парой портов, а коммутатор одновременно поддерживает потоки данных между всеми своими портами*. Другими словами, мост передает кадры последовательно, а коммутатор параллельно.

9.3.3. Техническая реализация и дополнительные функции коммутаторов

В настоящее время существует большое разнообразие моделей коммутаторов. Они отличаются как внутренней организацией, так и набором выполняемых дополнительных функций, таких как трансляция протоколов, поддержка алгоритма покрывающего дерева, образование виртуальных логических сетей и рядом других.

Современные коммутаторы используют в качестве базовой одну из трех схем, на которой строится такой узел обмена:

– коммутационная матрица;
– разделяемая многовходовая память;
– общая шина.

Часто эти три способа взаимодействия комбинируются в одном коммутаторе.

В конструктивном отношении коммутаторы делятся на следующие типы:

– автономные коммутаторы с фиксированным количеством портов;
– модульные коммутаторы на основе шасси;
– коммутаторы с фиксированным количеством портов, собираемые в стек.

Автономный коммутатор обычно предназначен для организации небольших рабочих групп.

Модульные коммутаторы на основе шасси чаще всего предназначены для применения на магистрали сети. Поэтому они выполняются на основе какой-либо комбинированной схемы, в которой взаимодействие модулей организуется по быстродействующей шине или же на основе быстрой разделяемой памяти большого объема. Модули такого коммутатора выполняются на основе технологии «hot swap», то есть допускают замену на ходу, без выключения коммутатора, так как центральное коммуникационное устройство сети не должно иметь перерывов в работе. Шасси обычно снабжается резервированными источниками питания и резервированными вентиляторами в тех же целях.

С технической точки зрения определенный интерес представляют ***стековые коммутаторы***. Эти устройства представляют собой коммутаторы, которые могут работать автономно, так как выполнены в отдельном корпусе, но имеют специальные интерфейсы, которые позволяют их объединять в общую систему, работающую как единый коммутатор. Говорят, что в этом случае отдельные коммутаторы образуют стек.

Обычно такой специальный интерфейс представляет собой высокоскоростную шину, которая позволяет объединить отдельные корпуса подобно модулям в коммутаторе на основе шасси. Так как расстояния между корпусами больше, чем между модулями на

шасси, скорость обмена по шине обычно ниже, чем у модульных коммутаторов: 200–400 Мбит/с. Не очень высокие скорости обмена между коммутаторами стека обусловлены также тем, что стековые коммутаторы обычно занимают промежуточное положение между коммутаторами с фиксированным количеством портов и коммутаторами на основе шасси. Стековые коммутаторы применяются для создания сетей рабочих групп и отделов, поэтому сверхвысокие скорости шин обмена им не очень нужны и не соответствуют их ценовому диапазону.

Выводы

1. Логическая структуризация сети необходима при построении сетей средних и крупных размеров. Использование общей разделяемой среды приемлемо только для сети, состоящей из небольшого количества (не более одного-двух десятков) компьютеров. Деление сети на логические сегменты повышает производительность, надежность, гибкость построения и управляемость сети.

2. Для логической структуризации сети применяются мосты и их современные преемники – коммутаторы. Они позволяют разделить сеть на логические сегменты с помощью минимума средств – только на основе протоколов канального уровня. Кроме того, эти устройства не требуют конфигурирования.

3. Основное различие между коммутатором и мостом состоит в том, что мост в каждый момент времени может осуществлять передачу кадров только между одной парой портов, а коммутатор одновременно поддерживает потоки данных между всеми своими портами.

5. Коммутаторы в настоящее время считаются наиболее быстродействующими коммуникационными устройствами, они позволяют соединять высокоскоростные сегменты без блокирования (уменьшения пропускной способности) межсегментного трафика.

6. Коммутаторы связывают процессоры портов по трем основным схемам – коммутационная матрица, общая шина и разделяемая память. В коммутаторах с фиксированным количеством портов обычно используется коммутационная матрица, а в модульных коммутаторах – сочетание коммутационной матрицы

в отдельных модулях с общей шиной и разделяемой памятью для связи модулей.

9.4. Маршрутизаторы и шлюзы

9.4.1. Структура маршрутизатора

Маршрутизатор (router) – ретрансляционная система, соединяющая две коммуникационные сети либо их части.

Каждый маршрутизатор реализует протоколы физического (1А, 1В), канального (2А, 2В) и сетевого (3А, 3В) уровней, как показано на *рис. 9.7*.

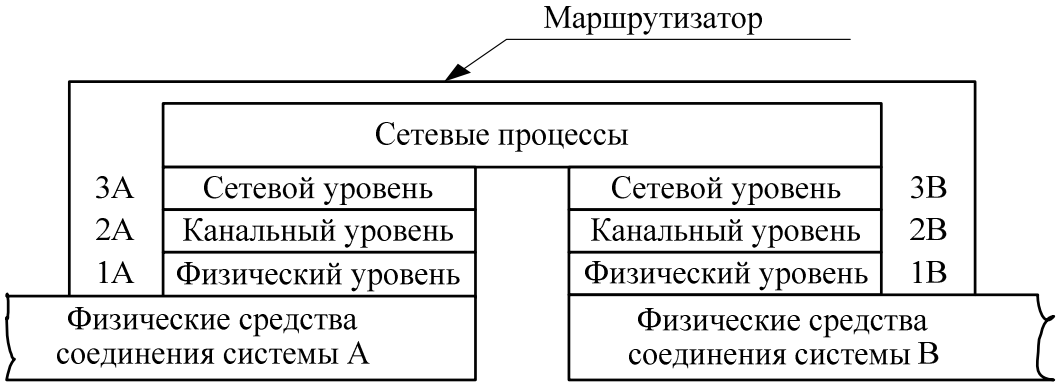


Рис. 9.7. Структура маршрутизатора

Специальные сетевые процессы соединяют части коммутатора в единое целое. Физический, канальный и сетевой протоколы в разных сетях различны. Поэтому соединение пар коммуникационных сетей осуществляется через маршрутизаторы, которые осуществляют необходимое преобразование указанных протоколов. Сетевые процессы выполняют взаимодействие соединяемых сетей.

Маршрутизатор работает с несколькими каналами, направляя в какой-нибудь из них очередной блок данных. Маршрутизаторы обмениваются информацией об изменениях структуры сетей, трафике. Благодаря этому, выбирается оптимальный маршрут следования блока данных в разных сетях от абонентской системы-отправителя к системе-получателю. Маршрутизаторы обеспечивают также соединение административно независимых коммуникационных сетей.

Архитектура маршрутизатора также используется при создании узла коммутации пакетов.

9.4.2. Различие между маршрутизаторами и мостами

Маршрутизаторы превосходят мосты своей способностью фильтровать и направлять пакеты данных в сети.

Так как маршрутизаторы работают на сетевом уровне, они могут соединять сети, использующие разную сетевую архитектуру, методы доступа к каналам связи и протоколы.

Маршрутизаторы не обладают такой способностью к анализу сообщений как мосты, но зато могут принимать решение о выборе оптимального пути для данных между двумя сетевыми сегментами.

Мосты принимают решение по поводу адресации каждого из поступивших пакетов данных, переправлять его через мост или нет в зависимости от адреса назначения. Маршрутизаторы же выбирают из таблицы маршрутов наилучший для данного пакета.

В «поле зрения» маршрутизаторов находятся только пакеты, адресованные к ним предыдущими маршрутизаторами, в то время как мосты должны обрабатывать все пакеты сообщений в сегменте сети, к которому они подключены.

Тип топологии или протокола уровня доступа к сети не имеет значения для маршрутизаторов, так как они работают на уровень выше, чем мосты (сетевой уровень модели OSI). Маршрутизаторы часто используются для связи между сегментами с одинаковыми протоколами высокого уровня. Наиболее распространенным транспортным протоколом, который используют маршрутизаторы, является IPX фирмы Novell или TCP фирмы Microsoft.

Необходимо запомнить, что для работы маршрутизаторов требуется один и тот же протокол во всех сегментах, с которыми он связан. При связывании сетей с различными протоколами лучше использовать мосты. Для управления загруженностью трафика сегмента сети также можно использовать мосты.

9.4.3. Шлюзы

Шлюз (gateway) – ретрансляционная система, обеспечивающая взаимодействие информационных сетей.

Структура шлюза представлена на *рис. 9.8*.

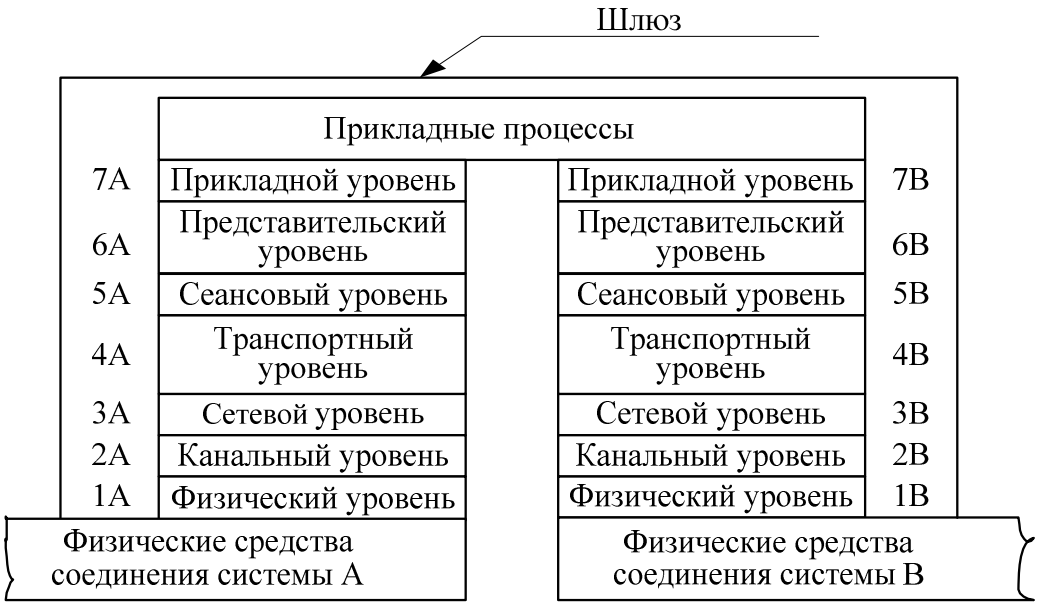


Рис. 9.8. Структура шлюза

Шлюз является наиболее сложной ретрансляционной системой, обеспечивающей взаимодействие сетей с различными наборами протоколов всех семи уровней. В свою очередь, наборы протоколов могут опираться на различные типы физических средств соединения.

В тех случаях, когда соединяются информационные сети, в них часть уровней может иметь одни и те же протоколы. Тогда сети соединяются не при помощи шлюза, а на основе более простых ретрансляционных систем, именуемых маршрутизаторами и мостами.

Шлюзы оперируют на верхних уровнях модели OSI (сеансовом, представительском и прикладном) и представляют наиболее развитый метод подсоединения сетевых сегментов и компьютерных сетей. Необходимость в сетевых шлюзах возникает при объединении двух систем, имеющих различную архитектуру. Например, шлюз приходится использовать для соединения сети (протокол TCP/IP) и большой ЭВМ со стандартом SNA. Эти две архитектуры не имеют ничего общего, и потому требуется полностью переводить весь поток данных, проходящих между двумя системами.

В качестве шлюза обычно используется выделенный компьютер, на котором запущено программное обеспечение шлюза

и производятся преобразования, позволяющие взаимодействовать нескольким системам в сети. Другой функцией шлюзов является преобразование протоколов. При получении сообщения IPX/SPX для клиента TCP/IP шлюз преобразует его в соответствии с протоколом TCP/IP.

Выводы

1. Соединение коммуникационных сетей осуществляется через маршрутизаторы, которые выполняют необходимое преобразование определенных протоколов.
2. Маршрутизаторы в процессе работы обмениваются информацией об изменениях структуры сетей, трафике и их состоянии, благодаря чему может быть осуществлен выбор оптимального маршрута следования блока данных.
3. Тип топологии или протокола уровня доступа к сети не имеет значения для маршрутизаторов, так как они работают на сетевом уровене модели OSI.
4. Шлюз является ретрансляционной системой, обеспечивающей взаимодействие информационных сетей. Обычно шлюзом являются серверы с настроенной службой маршрутизации, поэтому шлюзы функционируют на всех семи уровнях модели OSI.
5. Шлюзы сложны в установке и настройке. Шлюзы работают медленнее, чем маршрутизаторы.

9.5. Оборудование для сетей Wi-Fi

Сети Wi-Fi отождествляются с аббревиатурей *WLAN* (Wireless Local Area Network). Для организации *сетей Wi-Fi* (Wireless Fidelity, беспроводное соответствие) необходимы Wi-Fi сетевые карты, точки доступа и антенны. Необходимость в использовании точек доступа отпадает, когда мы говорим об очень малых сетях, размещенных в одном помещении. Использование точек доступа позволяет более гибко настроить сеть, объединить клиентов проводных и беспроводных сетей, а также установить связь с удаленными объектами (внешнее исполнение).

Wi-Fi сетевые карты по сути мало чем отличаются от обычных сетевых карт, за исключением некоторых особенностей настройки. Wi-Fi сетевые карты представлены в трех основных вариантах исполнения – внутренние PCI-карты, CARDBUS и USB-адаптеры. Также существуют адаптеры в COMPACT FLASH форм-факторе.

Адаптеры различаются по платформе, в которой они используются: PCI – настольный компьютер, CARDBUS – ноутбук, Compact Flash – карманный компьютер, USB – универсален. Принцип построения и настройки сетей един и не зависит от форм-фактора Wi-Fi адаптера. Необходимо отметить, что тип адаптера влияет лишь на излучаемую мощность передатчика и чувствительность приемника, а также возможность использования внешней антенны.

9.5.1. Wi-Fi точки доступа

Wi-Fi точки доступа – устройства, позволяющие объединять клиентов сети (как проводной, так и беспроводной) в единую сеть. Другими словами – для Wi-Fi клиентов, точка доступа – это своеобразный хаб (концентратор). Для клиентов проводной сети – возможность выхода в сеть к беспроводным клиентам.

Wi-Fi точки доступа представлены в двух основных вариантах исполнения – для использования внутри помещений и для внешнего использования. Существуют варианты исполнения точек доступа, совмещенных с панельными антеннами для внешнего использования.

При рассмотрении точек доступа исполнение играет очень важную роль. Т. е. внутриофисные точки доступа нельзя использовать на улице, а внешние – крайне нецелесообразно использовать внутри помещений. Также исполнение Wi-Fi точек доступа определяет их функциональные возможности.

Внутриофисные точки доступа служат для объединения Wi-Fi клиентов внутри помещений. Они оснащены функциями фильтров, создания виртуальных сетей и т. д. Но зачастую используются точки доступа с более широкими возможностями – WAN-порт, firewall, Ftp-сервер и т. д.

Внешние Wi-Fi точки доступа служат для объединения Wi-Fi клиентов вне помещений, например, в публичных местах. Внешние точки доступа имеют защищенное исполнение, более

жесткие эксплуатационные характеристики и т. д. При применении нескольких внешних точек доступа можно соединить достаточно удаленные объекты и создать публичный *хот-спот*. Внешние Wi-Fi точки доступа отличаются и большей излучаемой мощностью. Ко всем внешним точкам доступа можно подключить дополнительные антенны, что позволяет расширить зону покрытия Wi-Fi сети.

Следует обратить внимание на то, что многие точки доступа могут выступать в роли беспроводного клиента, что значительно расширяет область их применения.

9.5.2. Wi-Fi антенны

Внешние Wi-Fi антенны служат для передачи и приема сигнала, усиление которого в режиме передачи позволяет увеличить зону покрытия Wi-Fi сетей.

В основном распространены *пассивные антенны – направленные* (*рис. 9.9*) и *круговые*, или *всенаправленные* (*рис. 9.10*). Основное различие – характер распространения волн антенной. Круговая антенна излучает сигнал по кругу 360° (горизонталь), а направленная лишь на определенный сектор.

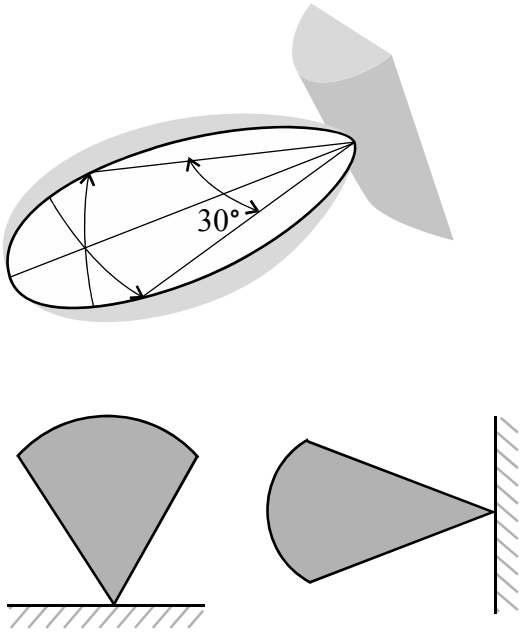


Рис. 9.9. Направленные Wi-Fi антенны

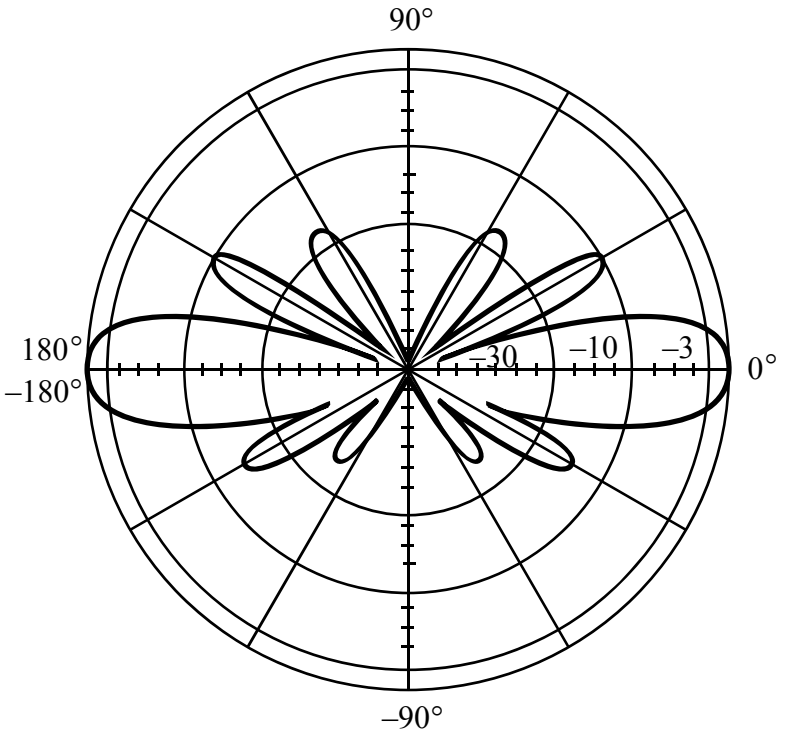


Рис. 9.10. Круговые Wi-Fi антенны

Wi-Fi антенны характеризуются четырьмя основными параметрами.

1. *Поляризация* отражает специфику распространения радиоволн. Поляризация бывает горизонтальная (линейная) и вертикальная, что необходимо учитывать при подборе антенн на стадии проектирования сети.

2. *HPBW по горизонтали* – угол распространения волн по горизонтали. Для всех круговых антенн равен 360°. Для направленных Wi-Fi антенн значительно меньше.

3. *HPBW по вертикали* – угол распространения волн по вертикали. При малом угле возможно возникновение мертвых зон.

4. *Усиление* характеризует усиление сигнала. Чем больше данный параметр, тем на большем расстоянии можно установить связь с сетью.

Удлинительные провода для антенн используются, если антенна удалена от точки доступа или сетевой карты. Особое внимание следует уделить разъемам, т. к. у разных производителей они могут различаться. Провода используются специальные – СВЧ, длина проводов должна быть как можно меньше.

9.5.3. Принципы организации беспроводных сетей

Выделяют два вида организации беспроводных сетей – это *Ad-Hoc* (Independent Basic Service Set (IBSS) или Peer-to-Peer) и *Infrastructure Mode*.

Режим Ad-Hoc является простейшей структурой локальной сети, при которой узлы сети (ноутбуки или компьютеры) связываются напрямую друг с другом.

Такая структура удобна для быстрого развертывания сетей. Для ее организации требуется минимум оборудования – каждый узел должен быть оборудован адаптером WLAN.

В ***режиме Infrastructure Mode*** узлы сети связаны друг с другом не напрямую, а через точку доступа, т. н. Access Point. Различают два режима взаимодействия с точками доступа – *BSS* (Basic Service Set) и *ESS* (Extended Service Set).

В режиме BSS все узлы связаны между собой через одну точку доступа, которая может играть роль моста для соединения с внешней кабельной сетью.

Режим ESS представляет собой объединение нескольких точек доступа, т. е. объединяет несколько сетей BSS. В этом случае точки доступа могут взаимодействовать и друг с другом. Расширенный режим удобно использовать тогда, когда необходимо объединить в одну сеть несколько пользователей или подключить нескольких проводных сетей.

Важным вопросом при организации WLAN-сетей является дальность покрытия. На этот параметр влияет сразу несколько факторов.

1. Используемая частота (чем она больше, тем меньшая дальность действия радиоволн).

2. Наличие преград между узлами сети (различные материалы по-разному поглощают и отражают сигналы).

3. Режим функционирования – Infrastructure Mode или Ad-Hoc.

4. Мощность оборудования.

Если рассматривать идеальные условия, то зона покрытия с одной точкой доступа будет иметь следующий средний радиус покрытия:

– сеть стандарта IEEE 802.11a – 50 м;

– сети 802.11b и 802.11g – порядка 100 м.

За счет увеличения количества точек доступа (в режиме Infrastructure ESS) можно расширять зоны покрытия сети на всю необходимую область охвата.

9.5.4. Безопасность Wi-Fi сетей

С точки зрения практического использования беспроводных сетей очень актуальны вопросы безопасности и защиты передаваемых данных, так как для перехвата данных в общем случае достаточно просто оказаться в зоне действия сети.

Первоначально созданные в этой сфере технологии обладали невысокой степенью защиты, данная проблема остается актуальной и на сегодняшний день.

Для защиты передаваемых данных предусмотрены следующие методы.

1. *Использование MAC-адресов* (Media Access Control ID): у каждого адаптера есть свой абсолютно уникальный код, установленный производителем. Эти адреса необходимо занести в списки адресов доступа у используемых для организации сети точек доступа. Все остальные WLAN-адаптеры с неправильными адресами будут исключены из сети автоматически.

2. *Использование ключей SSID* (Service Set Identifier): каждый легальный пользователь сети должен получить от администратора сети свой уникальный идентификатор сети.

3. *Шифрование данных*. Первые два способа не обеспечивают защиту от прослушивания и перехвата пакетов данных, поэтому защитить сеть в случае перехвата данных можно только с помощью шифрования.

Изначально стандарт 802.11 предусматривал аппаратный *протокол шифрования данных, WEP* (Wired Equivalent Privacy – защищенность, эквивалентная беспроводным сетям), основанный на *алгоритме шифрования RC4*. Однако в скором времени было обнаружено, что защищенную с его помощью сеть довольно легко взломать. Ранние версии предусматривали шифрование с использованием 40-битного *ключа*, более поздние 64, 128 или 256-битного. Но даже такая длина ключа в WEP не может обеспечить высокий уровень защиты сети, т. к. основная слабость данной технологии заключается в статичности ключа шифрования.

Хотя при использовании данного ключа увеличивается время взлома и количество пакетов данных, которые нужно перехватить, чтобы вычислить ключ, сама возможность взлома остается. Это абсолютно неприемлемо для определенного круга серьезных компаний и организаций.

На смену WEP была создана новая технология *WPA* (Wi-Fi Protected Access), разрабатывающаяся IEEE совместно с Wi-Fi Alliance. Главной особенностью новой системы безопасности является *шифрование данных с динамическими изменяемыми ключами* и *проверка аутентификации пользователей*.

В отличие от WEP здесь используется *протокол целостности временных ключей, TKIP* (Temporal Key Integrity Protocol), который подразумевает обновление ключей перед началом каждой сессии шифрования и проверкой пакетов на принадлежность к данной сессии.

Для аутентификации пользователей используются *сертификаты RADIUS* (Remote Authentication Dial-In User Service – сервер RADIUS должен подтвердить право доступа). Такой метод подразумевает, главным образом, корпоративное использование. Второй упрощенный вариант аутентификации требует предварительной установки разделяемых паролей на сетевые устройства (режим аутентификации PSK (Pre-Shared Keys)). Этот метод лучше всего применять в домашних условиях или там, где не происходит обмен важной информацией.

Изначально WPA была разработана как временная технология, которая со временем должна была быть заменена новым стандартом 802.11i. Данный стандарт, с учетом всех уже существующих наработок, призван обеспечить надежное шифрование передаваемых данных, а также аутентификацию пользователей сети.

В большинстве уже выпущенных Wi-Fi устройств (точки доступа, сетевые карты) можно установить протокол WPA посредством обновления программного обеспечения.

Выводы

1. Для организации беспроводных сетей Wi-Fi необходимы соответствующие сетевые карты, точки доступа и антенны.

2. Wi-Fi точки доступа представляют собой устройства, позволяющие объединять клиентов сети (как проводной, так и бес-

проводной) в единую сеть. Wi-Fi точки доступа разделяются по исполнению на два основных варианта – для использования внутри помещений и для внешнего использования.

3. Wi-Fi антенны служат для усиления сигнала, что позволяет увеличить зону покрытия Wi-Fi сетей.

4. Выделяют два основных вида организации беспроводных сетей: Ad-Hoc и Infrastructure Mode. В режиме Ad-Hoc узлы сети связываются напрямую друг с другом, а в режиме Infrastructure Mode узлы сети связаны друг с другом через точку доступа.

5. Наиболее актуальной проблемой функционирования Wi-Fi сетей является обеспечение требуемого уровня безопасности. Для защиты передаваемых данных предусмотрено несколько различных методов: использование MAC-адресов, использование ключей SSID, шифрование данных.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Назначение сетевого адаптера.
2. Какие параметры необходимо устанавливать у сетевого адаптера?
3. Перечислите функции сетевых адаптеров.
4. Что такое физический адрес адаптера?
5. Как определить физический адрес адаптера?
6. Какие есть типы сетевых адаптеров?
7. На каком уровне сетевой модели OSI используется сетевой адаптер?
8. Каково назначение повторителя?
9. В каких случаях ставят сетевой повторитель?
10. Что такое сетевой концентратор и каково его назначение?
11. На каком уровне сетевой модели OSI используется Hub?
12. Назначение моста.
13. На каком уровне сетевой модели OSI используется мост?
14. Какие сегменты сети может соединять мост?
15. Назначение коммутатора.
16. На каком уровне сетевой модели OSI используется коммутатор?

17. Каково различие между мостом и коммутатором?

18. Назначение маршрутизатора.

19. На каком уровне сетевой модели OSI используется маршрутизатор?

20. Каково различие между маршрутизаторами и мостами?

21. Что такое шлюз и каково его назначение?

22. На каком уровне сетевой модели OSI используется шлюз?

23. Оборудование для организации беспроводных сетей Wi-Fi и его назначение.

24. Классификация Wi-Fi антенн.

25. Перечислите виды организации беспроводных сетей.

26. Перечислите методы защиты передаваемых данных в сетях Wi-Fi.

10. ПЕРСПЕКТИВНЫЕ СЕТЕВЫЕ ТЕХНОЛОГИИ

10.1. Беспроводные сотовые сети

10.1.1. Организация сотовой сети

Сотовой радиосвязью называется технология, разработанная для увеличения пропускной способности мобильных радиотелефонных услуг.

До введения сотовой радиосвязи для предоставления этих услуг требовались передатчики и приемники высокой мощности. Типичная система связи могла обслуживать около 25 каналов и имела *эффективный радиус действия* около 80 км. Для увеличения *пропускной способности* такой системы нужно было использовать оборудование более низкой мощности и, следовательно, меньшего радиуса действия при участии в ней нескольких передатчиков и приемников.

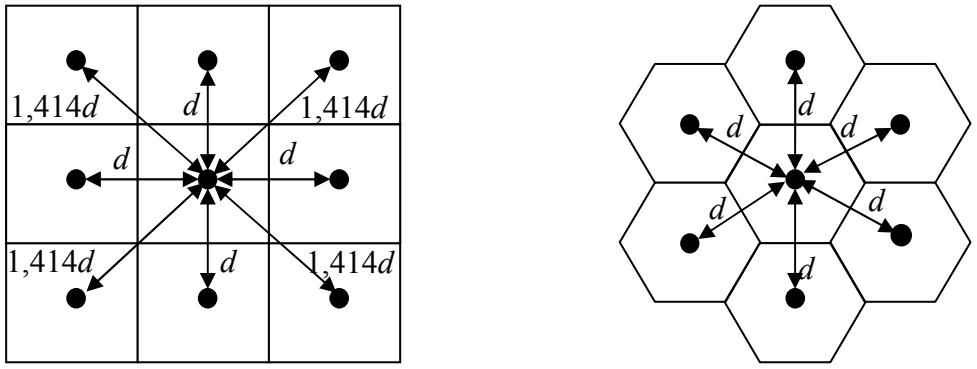
В начале данного раздела кратко рассматривается организация сотовой системы, после чего анализируются некоторые особенности ее внедрения.

Принцип организации сотовой связи состоит в использовании множества маломощных (100 Вт и ниже) передатчиков.

Поскольку диапазон действия таких передатчиков довольно мал, зону обслуживания системы можно разбивать на *ячейки*, каждая из которых будет обслуживаться собственной антенной. Каждая ячейка, которой выделяется своя полоса частот, обслуживается базовой станцией, состоящей из передатчика, приемника и модуля управления. Смежные ячейки используют разные частоты, чтобы избежать появления интерференции или перекрестных помех. В то же время ячейки, находящиеся на довольно большом расстоянии друг от друга, могут использовать одинаковые полосы частот.

При проектировании такой системы первое, что нужно сделать, – это решить, какую форму должны иметь ячейки, на которые будет разбита зона обслуживания. Самым простым решением была бы сетка, состоящая из квадратных ячеек (*рис. 10.1*, *а*). Однако такая геометрическая форма оказалась не идеальной. Если

сторона квадратной ячейки равна d, тогда ячейка будет иметь четыре соседа на расстоянии d и четыре – на расстоянии $\sqrt{2d}$. В то же время, если пользователь мобильных услуг находится в пределах одной ячейки и движется по направлению к ее границе, было бы лучше, чтобы все смежные антенны находились на равных расстояниях друг от друга. В этом случае проще определить момент, в который следует переключать пользователя на другую антенну, а также выбрать новую антенну. Равное расстояние между смежными антеннами достигается только в шестиугольной схеме (*рис. 10.1*, *б*). Радиус шестиугольника определяется как радиус окружности, описанной вокруг него (эта величина равна расстоянию от центра фигуры до каждой из ее вершин, а также длине стороны шестиугольника). Для ячейки с радиусом R расстояние между центром ячейки и центром любой смежной ячейки равняется $d = \sqrt{3R}$.



а *б*

Рис. 10.1. Геометрические структуры сотовых систем:
а – квадратная схема; *б* – гексогональная схема

На практике точная шестиугольная структура не используется. Отклонения от идеальных шестиугольников обусловлены топографическими ограничениями, местными условиями распространения сигнала и соображениями целесообразности расположения антенн.

10.1.2. Многократное использование частот и увеличение пропускной способности сети

В каждой ячейке сотовой сети есть базовый *трансивер*. Мощность передаваемых сигналов тщательно регулируется (насколько

это возможно для быстроменяющихся условий сред мобильной связи). Как правило, каждой ячейке выделяется 10–50 частот в зависимости от планируемой нагрузки. Кроме того, нужен механизм использования одной и той же частоты в ячейках, расположенных недалеко друг от друга, чтобы одну частоту можно было использовать для нескольких одновременных сеансов связи.

Важным вопросом, разумеется, является определение удаленности двух ячеек, использующих одну частоту, поскольку сигналы этих ячеек не должны интерферировать друг с другом. Были предложены различные модели многократного использования частот, некоторые примеры приведены на *рис. 10.2*, *10.3* и *10.4*.

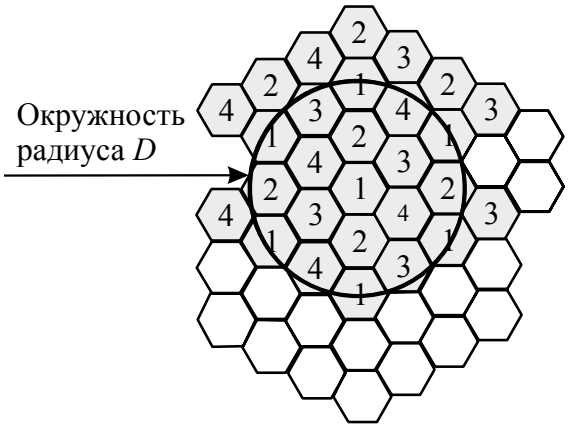


Рис. 10.2. Схема повторного использования частот для $N = 4$

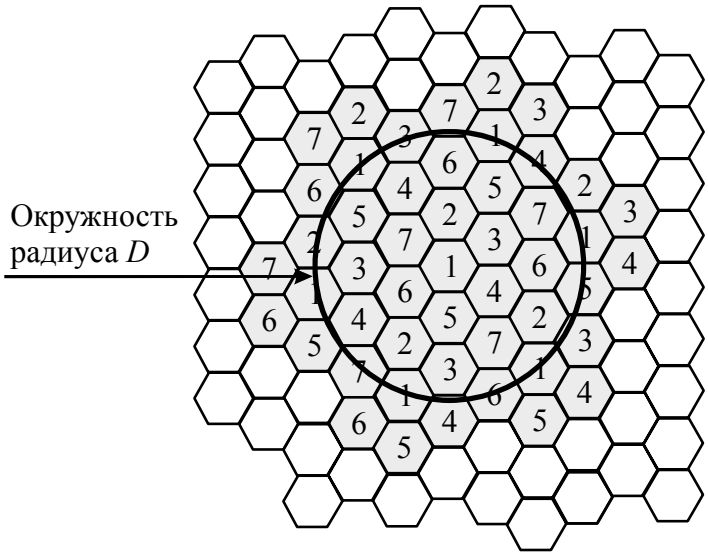


Рис. 10.3. Схема повторного использования частот для $N = 7$

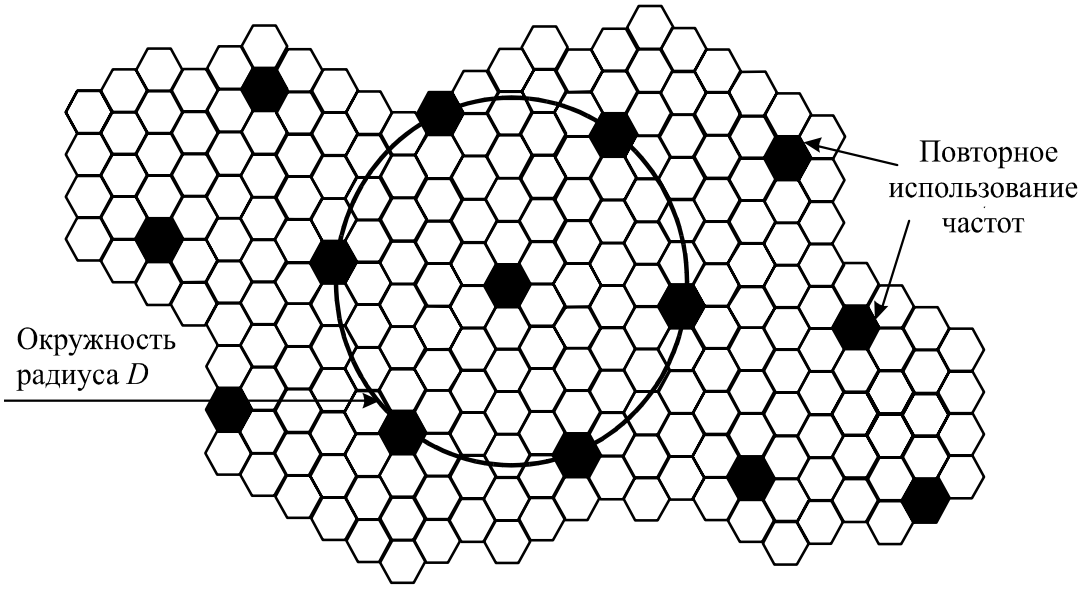


Рис. 10.4. Схема многократного использования частот для $N = 19$

Если схема состоит из N ячеек, для которых выделяется одинаковое количество частот, то каждая ячейка будет иметь K/N частот, где K – общее число частот, выделяемых системе.

Мобильная телефонная система AMPS, в которой $K = 395$, а $N = 7$, представляет собой наименьшую систему, в которой можно обеспечить достаточную изоляцию двух сеансов использования одной и той же частоты. Это означает, что в среднем на одну ячейку должно приходиться не более 57 частот.

Для характеристики повторного использования частоты существуют следующие параметры: D – минимальное расстояние между центрами ячеек (см. *рис. 10.2*), которые используют одну и ту же полосу частот (называемую группой внутренних каналов); R – радиус ячейки; d – расстояние между центрами смежных ячеек ($d = \sqrt{3}R$); N – число ячеек в минимальном фрагменте, периодическим повторением которого образуется вся схема (каждая ячейка фрагмента использует уникальную полосу частот). Этот параметр еще называют кратностью использования.

В шестиугольной схеме возможны только следующие значения $N = I2 + J2 + (I \cdot J)$, $I, J = 0, 1, 2, 3, \ldots$.

Таким образом, возможными значениями N являются числа 1, 3, 4, 7, 9, 12, 13, 16, 19, 21 и т. д. Верно следующее соотношение:

$$D / R = \sqrt{N}. \qquad (10.1)$$

Это можно записать и по-другому:

$$D / d = \sqrt{N}. \qquad (10.2)$$

Со временем, когда система будет обслуживать все больше клиентов, трафик может распределиться таким образом, что какой-нибудь ячейке для обслуживания звонков не хватит выделенных ей частот. Для выхода из такой ситуации используется несколько подходов.

Добавление новых каналов. Обычно, когда система установлена в определенном регионе, используются не все каналы, и с расширением системы можно просто добавлять новые.

Заимствование частот. В самом простом случае перегруженные ячейки могут использовать частоты смежных ячеек.

Расщепление ячеек. На практике распределение трафика и топография местности неоднородны, что также дает возможность увеличения пропускной способности. Ячейки в областях с повышенным спросом на услуги мобильной связи можно расщеплять. Как правило, размеры исходных ячеек колеблются от 6,5 до 13 км. Меньшие ячейки также можно разбивать, однако следует помнить, что на практике радиус 1,5 км считается минимальным (см. ниже микроячейки). При использовании меньших ячеек нужно уменьшать уровень мощности, чтобы сигнал оставался в пределах ячейки. Кроме того, при движении мобильные устройства переходят из одной ячейки в другую, что требует передачи вызова от одного базового трансивера другому. Этот процесс называется переключением (handoff). Так, по мере уменьшения размера ячейки переключения будут происходить все чаще. При уменьшении радиуса ячейки в F раз размеры покрываемой области уменьшаются в F^2 раз, а требуемое число базовых станций увеличивается в те же F^2 раз.

Разбивка ячеек на секторы. При разбивке на секторы ячейка делится на несколько клиновидных секторов, в каждом из которых остается свой набор каналов. Обычно на ячейку приходится 3–6 секторов. Каждому сектору предоставляется отдельный набор каналов ячейки, а для фокусировки сигнала на отдельных секторах используются направляемые антенны базовой станции.

Микроячейки. По мере уменьшения ячейки антенны перемещаются с крыш высотных зданий и вершин холмов на крыши зданий поменьше или на стены высотных домов и в конце концов

оказываются на фонарных столбах, с высоты которых они обслуживают микроячейки. Любое уменьшение размера ячейки сопровождается уменьшением уровня мощности сигналов, излучаемых базовой станцией. Микроячейки полезно располагать на городских улицах в густонаселенных районах, а также внутри больших зданий общественного пользования.

10.1.3. Функционирование сотовой системы

На *рис. 10.5* показаны основные элементы сотовой системы.

Примерно в центре каждой ячейки находится **базовая станция**. Базовая станция состоит из антенны, контроллера и нескольких трансиверов, которые служат для связи в каналах, выделенных в этой ячейке.

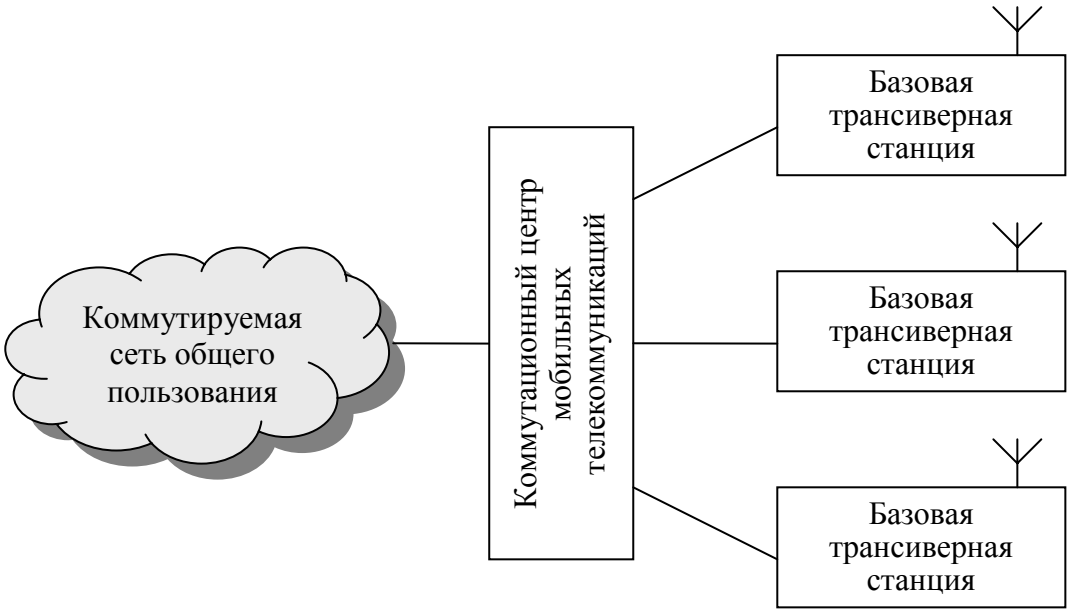


Рис. 10.5. Общий вид сотовой системы

Контроллер используется для обработки соединений мобильного устройства с остальной сетью. В любой момент в пределах ячейки могут быть активными и перемещаться несколько пользователей мобильной связи, сообщающихся с базовой станцией. Каждая базовая станция подсоединена к *коммутатору мобильных телекоммуникаций* (Mobile Telecommunications Switching Office, MTSO), причем один коммутатор MTSO может обслуживать несколько базовых станций. Обычно связь между коммутатором MTSO и базовой станцией является проводной, хотя возможна также беспроводная связь.

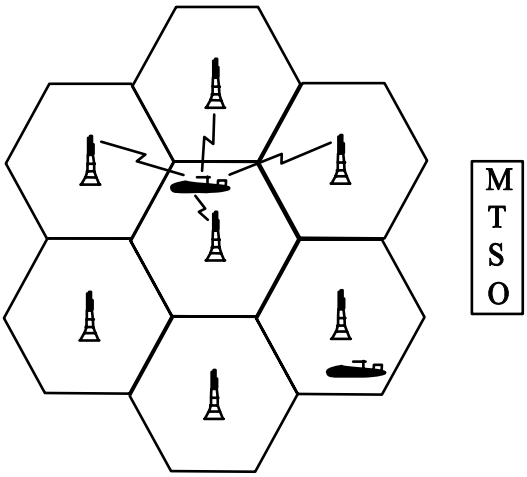
Коммутатор MTSO устанавливает соединение между мобильными устройствами. Кроме того, MTSO соединен также с общественной телефонной или телекоммуникационной сетью и может соединять стационарных абонентов с сетью общего пользования и мобильных абонентов с сотовой сетью. Коммутатор MTSO выделяет для каждого соединения голосовой канал, выполняет переключения и контролирует звонки для передачи информации о счетах.

Работа сотовой системы полностью автоматизирована и не требует от пользователя никаких действий, кроме заказа разговоров и ответа на звонки.

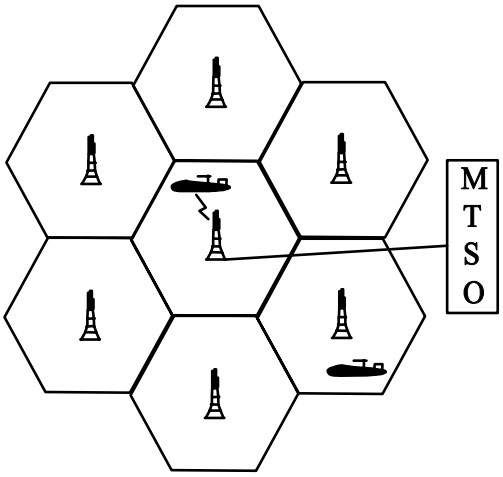
Между мобильным устройством и базовой станцией можно устанавливать каналы связи двух типов: ***каналы управления*** и ***информационные каналы***.

Каналы управления используются для обмена информацией, касающейся заказа и поддержания звонка, а также установления связи между мобильным устройством и ближайшей к нему базовой станцией. Информационные каналы служат для передачи голоса или данных между пользователями. На *рис. 10.6* показаны шаги, которые следует предпринять для обычного соединения двух мобильных пользователей, находящихся в зоне действия одного коммутатора MTSO.

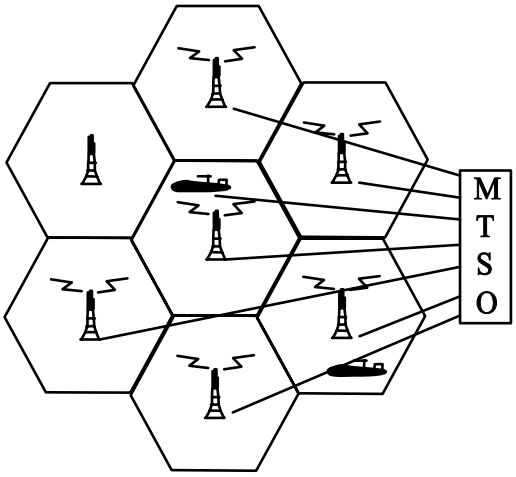
1. *Инициализация мобильного устройства*. Включенное мобильное устройство проводит *сканирование* и выбирает самый сильный настроечный канал управления, используемый данной системой (*рис. 10.6*, *а*). Ячейки с различными полосами частот периодически транслируют сигналы в различных настроечных каналах. Приемник мобильного устройства выбирает самый сильный настроечный канал и начинает его прослушивать. В результате этой процедуры мобильное устройство автоматически выбирает антенну базовой станции той ячейки, в пределах которой оно будет действовать. Затем выполняется *квитирование* между мобильным устройством и коммутатором MTSO, контролирующим данную ячейку, что тоже осуществляется через базовую станцию этой ячейки. Квитирование используется для опознания пользователя и для регистрации его местоположения. Все время, пока включено мобильное устройство, эта процедура сканирования периодически повторяется, что позволяет следить за движением устройства. Если устройство входит в новую ячейку, выбирается новая базовая станция. Кроме того, мобильное устройство следит за сигналами избирательного вызова, о чем будет сказано ниже.



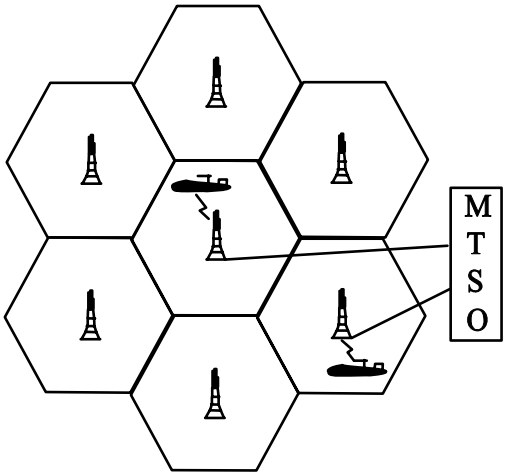
а – поиск сильнейшего сигнала



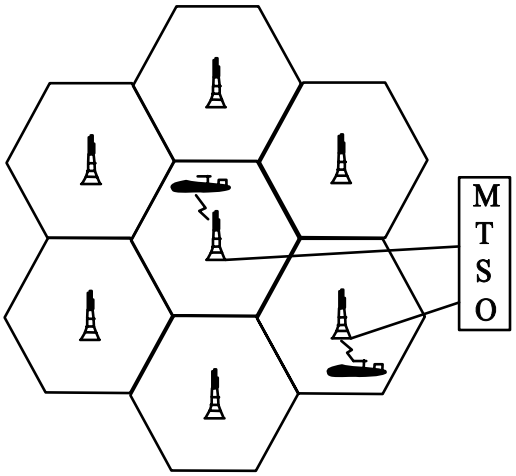
б – запрос на соединение



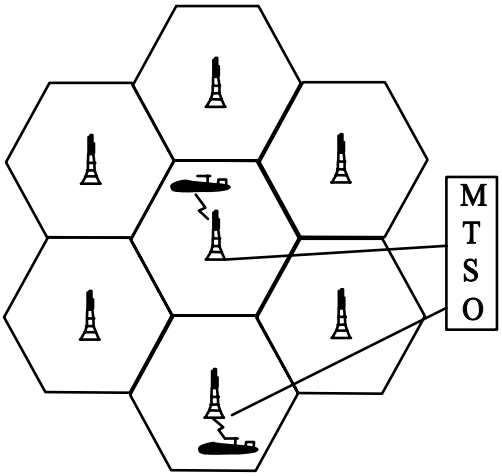
в – передача сигнала



г – вызов принят



д – исходящий вызов



е – переключение

Рис. 10.6. Пример мобильного сотового соединения

2. *Звонок с мобильного устройства*. Звонок с мобильного устройства начинается с отправки номера вызываемого устройства по предварительно выбранному каналу *(рис. 10.6, б)*. Приемник мобильного устройства сначала проверяет, свободен ли настроечный канал, анализируя информацию в прямом (от базовой станции) канале.

Когда обнаруживается, что канал свободен, мобильное устройство может начинать передачу в соответствующем обратном (к базовой станции) канале. Базовая станция в свою очередь отправляет запрос на коммутатор MTSO.

3. *Избирательный вызов*. Далее коммутатор MTSO пытается установить связь с вызываемым устройством. Коммутатор отправляет адресное сообщение определенной базовой станции, в зависимости от номера вызывающего мобильного устройства (*рис. 10.6*, *в*). Каждая базовая станция передает сигналы избирательного вызова в собственном выделенном настроечном канале.

4. *Принятие вызова*. Вызываемое мобильное устройство распознает свой номер в настроечном канале, за которым следит в настоящий момент, и отвечает данной базовой станции. Базовая станция отправляет ответ на коммутатор MTSO, который устанавливает канал связи между вызывающей и вызываемой базовыми станциями. В то же самое время коммутатор MTSO выбирает подходящий канал информационного обмена внутри ячейки каждой базовой станции и уведомляет каждую базовую станцию, которые в свою очередь уведомляют свои мобильные устройства (*рис. 10.6*, *г*). Оба мобильных устройства настраиваются на выделенные им каналы.

5. *Текущий вызов*. Пока поддерживается соединение, два мобильных устройства обмениваются голосовыми сигналами или данными, проходящими через соответствующие базовые станции и коммутатор MTSO (*рис. 10.6*, *д*).

6. *Переключение*. Если мобильное устройство во время соединения выходит за пределы одной ячейки и входит в зону действия другой, то старый информационный канал следует заменить каналом, выделенным новой базовой станции в новой ячейке (*рис. 10.6*, *е*). Система осуществляет это изменение, не прерывая звонка и не беспокоя пользователя.

Система также выполняет некоторые другие функции, не представленные на *рис. 10.6*.

1. *Блокирование вызова*. Если при звонке с мобильного устройства все информационные каналы, выделенные ближайшей базовой станции, заняты, то мобильное устройство предпринимает предварительно заданное количество последовательных попыток установления связи. После определенного количества неудачных попыток пользователю возвращается сигнал «занято».

2. *Завершение вызова*. Когда один или оба пользователя вешают трубку, об этом узнает коммутатор MTSO и освобождает информационные каналы обеих базовых станций.

3. *Потеря вызова*. Если в определенный период соединения из-за интерференции или слабого сигнала базовая станция не может поддерживать минимально требуемую интенсивность сигнала, то информационный канал связи с пользователем прерывается, о чем уведомляется коммутатор MTSO.

4. *Звонки стационарным и удаленным мобильным абонентам/от стационарных и удаленных мобильных абонентов*. Коммутатор MTSO подключен к коммутатору общественной телефонной сети. Это означает, что коммутатор MTSO может устанавливать соединение между мобильным пользователем из своей зоны и стационарным абонентом через телефонную сеть. Более того, MTSO может соединяться через телефонную сеть либо через выделенные каналы связи с удаленными MTSO и устанавливать соединение между мобильным пользователем из своей зоны и удаленным мобильным пользователем.

10.1.4. Сотовые системы первого и второго поколения

Сотовые системы первого поколения, подобные AMPS, быстро приобрели широкую популярность и постоянно наращивают пропускную способность. Существуют следующие ключевые различия между системами первого и следующего поколений.

1. *Цифровые информационные каналы*. Системы первого поколения практически полностью аналоговые, в то время как системы второго поколения являются цифровыми. В частности, системы первого поколения спроектированы для поддержки голосовых каналов с использованием частотной модуляции; цифровые данные можно передавать только с использованием модема, который преобразует цифровые данные в аналоговую форму.

2. *Шифрование*. Системы первого поколения отправляют пользовательские данные в чистом виде, не обеспечивая никакой защиты.

3. *Обнаружение и исправление ошибок*. В результате можно обеспечить довольно чистый прием речи.

4. *Доступ к каналам*. В системах первого поколения каждая ячейка поддерживает несколько каналов. В любой момент времени канал может быть выделен только одному пользователю. В системах второго поколения ячейкам также выделяется по несколько каналов, к тому же каждый канал может совместно использоваться несколькими пользователями посредством схем множественного доступа с временным разделением (TDMA) или множественного доступа с кодовым разделением (CDMA).

Начиная с 90-х годов, было внедрено немало различных систем второго поколения. В *таблице* перечислены некоторые ключевые характеристики трех наиболее важных систем этого поколения.

Сотовые телефонные системы второго поколения

Характеристика	GSM	IS–136	IS–95
Метод доступа	TDMA	TDMA	CDMA
Полоса частот для передачи сигналов базовой станции	935–960 МГц	869–894 МГц	869–894 МГц
Полоса частот для передачи сигналов мобильного устройства	890–915 МГц	824–849 МГц	824–849 МГц

Доступ многих пользователей к сотовой системе первого поколения осуществляется с помощью технологии FDMA.

Технология разделения каналов TDMA уже упоминалась в разделе 3. Применение схемы TDMA в сотовой системе можно описать следующим образом. Также, как и при использовании FDMA, каждой ячейке выделяется некоторое количество каналов, половина из которых используется для обратной связи, а половина – для прямой. Передача данных осуществляется в виде последовательности кадров с повторяющейся структурой: каждый кадр делится на некоторое число слотов. Положение каждого слота в последовательности кадров определяет отдельный логический канал.

Множественный доступ с кодовым разделением каналов (Code Division Multiple Access, CDMA) представляет собой основанную на расширении спектра схему, которая является второй, после TDMA, альтернативой разделения каналов для сотовых сетей второго поколения.

Схему CDMA для сотовых систем можно описать следующим образом. Как и при использовании FDMA, каждой ячейке выделяется некоторая полоса частот, которая делится на две части – половина для обратного канала (от мобильного устройства к базовой станции) и половина для прямого канала (от базовой станции к мобильному устройству). Использование схемы CDMA для сотовых сетей имеет несколько преимуществ.

1. *Частотное разнесение*. Из-за того, что передаваемые сигналы рассеяны по широкой полосе частот, искажение передачи на определенной частоте, например, вследствие шума или селективного замирания, меньше влияет на сигнал.

2. *Снижение негативных эффектов многолучевого распространения*.

3. *Конфиденциальность*. Каждый пользователь имеет свой код, такой схеме изначально присуща конфиденциальность.

4. *Постепенное снижение эффективности функционирования системы*. В схемах TDMA или FDMA к системе может одновременно обращаться только фиксированное число пользователей. В CDMA же по мере того, как все больше пользователей получают одновременный доступ к системе, уровень шума и, следовательно, *частота появления ошибок* увеличиваются.

Следует упомянуть и о некоторых недостатках сотовой схемы CDMA.

1. *Проблема расположения*. Сигналы, поступающие от более близких к передатчику объектов, не так затухают, как сигналы, пришедшие издалека. Поэтому в системах CDMA очень важное значение имеют схемы регулирования мощности.

2. *Мягкое переключение*. Как будет показано далее, для плавности переключения с одной ячейки в следующую требуется, чтобы мобильное устройство вошло в новую ячейку до того, как оно оставит старую. Это называется мягким переключением, которое является более сложным, чем жесткое переключение, используемое в схемах FDMA и TDMA.

10.1.5. Архитектура глобальной системы мобильной связи

До того как была разработана глобальная система мобильной связи (GSM), в странах Европы использовалось множество разных несовместимых сотовых телефонных технологий первого поколения.

Стандарт GSM был разработан для внедрения в Европе общей технологии второго поколения, чтобы одни и те же абонентские устройства можно было использовать по всему континенту. Эта технология оказалась весьма успешным и, возможно, самым популярным мировым стандартом для систем нового поколения. Впервые стандарт GSM появился в 1990 году в Европе. Теперь подобные системы внедрены в Северной и Южной Америке, Азии, Северной Африке, а также в Средней Азии и в Австралии.

На *рис. 10.7* показаны ключевые функциональные элементы системы GSM.

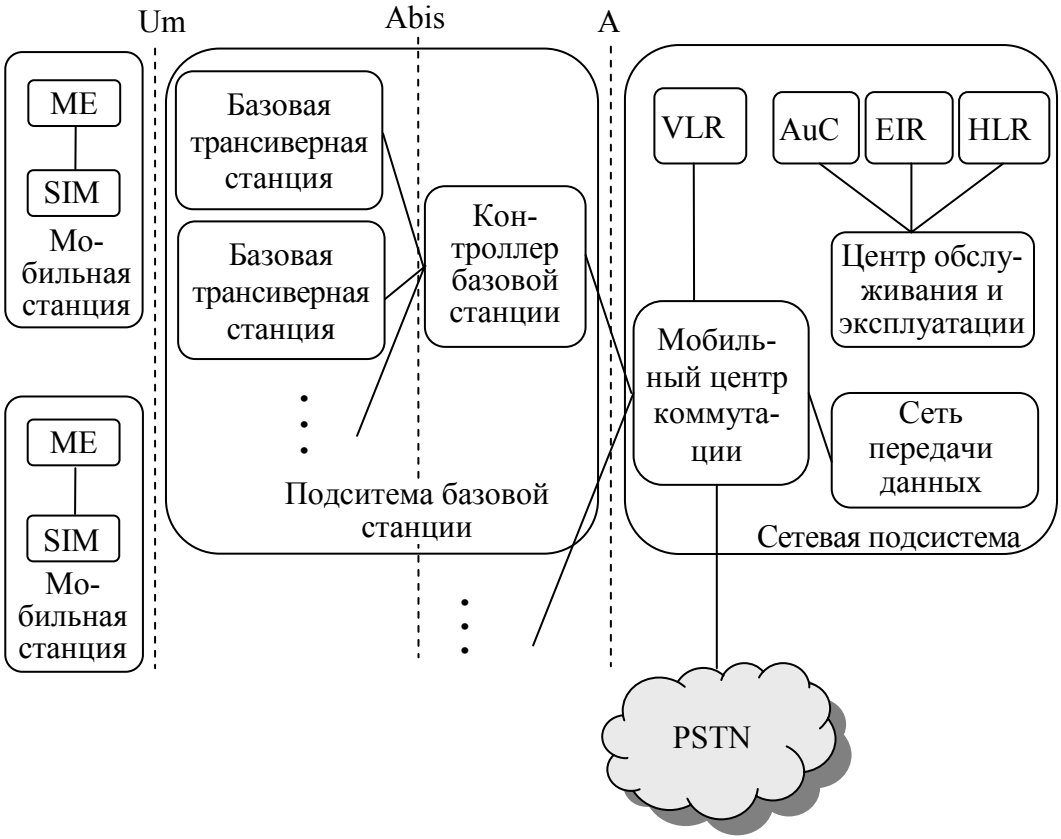


Рис. 10.7. Общая архитектура GSM

На *рис. 10.7* линии *Um*, *Abis* и *A* обозначают интерфейсы между функциональными элементами, которые стандартизированы в документации GSM (AuC – центр аутентификации; EIR – регистр идентификации оборудования; HLR – регистр исходного положения; ME – мобильное оборудование; PSTN – общественная коммутируемая телефонная сеть; SIM – модуль идентификации абонента;

VLR – регистр местонахождения посетителей). Таким образом, можно приобретать оборудование у разных поставщиков и ожидать, что оно будет успешно взаимодействовать. В стандарте GSM определены также дополнительные интерфейсы.

Мобильная станция. Через интерфейс Um, называемый также *радиоинтерфейсом*, мобильная станция сообщается с трансивером базовой станции в той ячейке, в которой находится мобильное устройство. Термином мобильное оборудование (Mobile Equipment, ME) обозначается физический терминал, такой, как телефон или устройство персональной службы связи (Personal Communication Service, PCS), включающее в себя радиотрансивер, процессоры для обработки цифровых сигналов и модуль идентификации абонента (Subscriber Identity Module, SIM).

SIM представляет собой портативное устройство, имеющее вид интеллектуальной карточки или встраиваемого модуля, в котором хранится идентификационный номер абонента, координаты сетей, которыми разрешено пользоваться абоненту, ключи шифрования и другая информация об абоненте.

Абонентские устройства GSM до вставки модуля SIM абсолютно неотличимы друг от друга. Поэтому путешествующий абонент, захвативший с собой свой модуль SIM, может в разных странах использовать разные устройства, вставляя в них свой модуль. В действительности, за исключением определенных срочных соединений, абонентские устройства не будут работать без вставленного модуля SIM.

Подсистема базовой станции (Base Station Subsystem, BSS) состоит из контроллера базовых станций и одной или нескольких базовых трансиверных станций. Каждая *базовая трансиверная станция* (Base Transceiver Station, BTS) определяет ячейку, в которую входит радиоантенна, радиотрансивер и канал связи с контроллером базовых станций.

Ячейка GSM может иметь радиус от 100 м до 35 км, в зависимости от среды. *Контроллер базовой станции* (Base Station Controller, BSC) может совмещаться с BTS или управлять работой нескольких устройств BTS, а следовательно, несколькими ячейками. Контроллер BSC резервирует радиочастоты, управляет переключениями мобильных устройств с одной ячейки на другую в пределах одной подсистемы BSS и контролирует избирательное обращение.

Сетевая подсистема (Network Subsystem, NS) обеспечивает связь между сотовой сетью и общественными коммутируемыми телекоммуникационными сетями. Подсистема NS управляет переключениями между ячейками, находящимися в различных подсистемах базовых станций, опознает пользователей и подтверждает достоверность их счетов, а также выполняет функции роуминга мобильных пользователей. Центральным элементом подсистемы NS является *мобильный центр коммутации* (Mobile Switching Center, MSC). Он управляет четырьмя базами данных.

1. *База данных регистра исходного положения* (home location register, HLR). В регистре HLR хранится информация, как временная, так и постоянная, о каждом из абонентов, который «принадлежит» системе (т. е. об абонентах, телефонные номера которых связаны с центром коммутации).

2. *База данных регистра местонахождения посетителей* (Visitor Location Register, VLR). Одну из важных частей информации составляет местонахождение абонента. Местонахождение определяется из регистра VLR, в который введен абонент. В регистре местонахождения посетителей хранится информация об абонентах, которые в данный момент физически находятся в районе, обслуживаемом данным центром коммутации. В регистре отмечается, является ли абонент активным, а также фиксируются другие параметры, связанные с абонентом. При поступлении звонка абоненту система использует связанный с абонентом телефонный номер для опознания исходного для данного абонента центра коммутации. Этот центр коммутации, в свою очередь, в своем регистре HLR может найти центр коммутации, в зоне действия которого в данный момент физически находится абонент. При поступлении звонка от абонента регистр VLR используется для инициирования звонка. Даже если абонент находится в зоне, принадлежащей его исходному центру коммутации, он может также быть представлен в регистрах VLR других центров коммутации.

3. *База данных центра аутентификации* (Authentication Center, AuC). Эта база данных используется в процессе аутентификации; например, в ней хранятся ключи аутентификации и шифрования для всех абонентов, представленных как в регистрах исходного положения, так и в регистрах местонахождения посетителей. Центр управляет доступом к данным пользователей, а также процессом аутентификации при присоединении абонента к сети. Данные, передаваемые системами GSM, шифруются,

поэтому они конфиденциальны. Для шифровки данных, передаваемых от абонента трансиверу базовой станции, используется поточный шифр A5. В то же время переговоры по сети с наземными линиями связи проходят без шифрования. Другой поточный шифр A3 используется для аутентификации.

4. *База данных регистра идентификации оборудования* (Equipment Identity Register, EIR). В этой базе данных хранятся записи о типе оборудования, которое имеется на мобильной станции. Эта база данных также важна для безопасности (например, для блокирования звонков с украденных мобильных устройств и предотвращения использования сети станциями, которым не было дано такого разрешения).

10.1.6. Сотовые системы третьего поколения 3G

Беспроводные системы связи третьего поколения разрабатываются с целью получения высокоскоростных беспроводных средств передачи не только речи, но и данных, мультимедиа и видео. По инициативе ITU IMT-2000 определены следующие возможности систем третьего поколения. Приведем некоторые их характеристики.

1. Качество речи сравнимо с качеством речи в общественной коммутируемой телефонной сети: доступна скорость передачи данных в 144 Кбит/с.

2. Для низкоскоростных систем доступная скорость передачи данных составляет 384 Кбит/с.

3. Для учреждений поддерживается скорость передачи данных 2,048 Мбит/с.

4. Передачи данных могут быть симметричными и асимметричными.

5. Поддерживается связь как с коммутацией пакетов, так и с коммутацией каналов.

6. Имеется адаптивный интерфейс с Internet, который позволяет эффективно отразить асимметрию прибывающего и отправляемого трафика.

7. Как правило, доступный спектр частот используется более эффективно.

8. Поддерживается разнообразное мобильное оборудование.

9. Система достаточно гибка для введения новых услуг и технологий.

Эти характеристики и концепции глобальной беспроводной связи были названы *персональными службами связи* (PCS) и *персональными сетями связи* (PCN), а их воплощение в жизнь является задачей беспроводных систем третьего поколения.

Вообще планируется, что в дальнейшем технология будет цифровой с возможностью множественного доступа с временным или кодовым разделением каналов, чтобы эффективно использовать спектр частот и обеспечивать высокую пропускную способность.

Телефоны PCS согласно проекту должны иметь меньшую мощность и быть относительно маленькими и легкими. Во всех странах сейчас ведутся работы, по завершении которых одни и те же терминалы можно будет использовать повсеместно.

Сети третьего поколения 3G работают на частотах дециметрового диапазона, как правило, в диапазоне около 2 ГГц, передавая данные со скоростью до 14 Мбит/с. Они позволяют организовывать видеотелефонную связь.

Стандарт 3G включает в себя 5 отдельных стандартов семейства IMT-2000 (UMTS/W-CDMA, CDMA2000, TD-CDMA, DECT и UWC-136). Из перечисленных составных частей 3G только первые три представляют собой полноценные стандарты сотовой связи третьего поколения, а DECT и UWC-136 играют вспомогательную роль. DECT (Digital Enhanced Cordless Telecommunications) – это стандарт беспроводной телефонии домашнего или офисного назначения, который в рамках мобильных технологий третьего поколения может использоваться только для организации точек горячего подключения к данным сетям. Стандарт UWC-136 (Universal Wireless Communications) – это технология EDGE (Enhanced Data rates for GSM Evolution), которая относится к предыдущему поколению.

Стандарт UMTS (Universal Mobile Telecommunication System – универсальная система мобильной связи) теоретически обеспечивает обмен информацией на скоростях до 2048 кбит/с, однако на практике скорость может быть несколько ниже. В сетях W-CDMA (Wideband Code Division Multiple Access) используют разделение сигнала по кодово-частоному принципу, т. е. идентификация пакетов информации, передаваемых абонентами, производится не только по уникальному идентификатору, но и по частоте. Для передачи данных протоколы UMTS используют

частоты: 1885–2025 МГц – для передачи данных в режиме от мобильного терминала к базовой станции и 2110–2200 МГц – для передачи данных в режиме от станции к терминалу.

Стандарт TD-CDMA (Time Division Code Division Multiple Access) близок к рассмотренному выше стандарту W-CDMA, однако его основой является гибридный кодово-временной принцип разделения сигнала. В целом считается, что именно стандарт TD-CDMA является наилучшим для передачи данных Интернет.

Технологию CDMA2000 следует рассматривать как эволюцию технологии CDMA, тогда как UMTS радикально отличается от GSM. Стандарт CDMA2000 разделяют на три фазы – 1X (известна также как IS-95C), 1X EV-DO (только данные) и 1X EV-DV (данные и голос). Именно стандарт 1X EV-DV может считаться полноценным 3G-стандартом. Отметим, что изначально не было разделения на 1X EV-DO и 1X EV-DV, а в стандарте CDMA выделяли только две фазы 1XRTT и 3XRTT. Скорость обмена информацией в сетях CDMA2000 1X может достигать 153,6 Кбит/с, в стандарте CDMA2000 1X EV-DO – 2,4 Мбит/с (ревизия 0) и 3,1 Мбит/с (ревизия A). В отличие от стандарта UMTS, стандарт CDMA2000 не оговаривает, какие частоты должны использоваться для передачи сигнала, поэтому построение сетей CDMA2000 возможно во всех частотных диапазонах, используемых операторами сотовой связи – 450, 700, 800, 900, 1700, 1800, 1900, 2100 МГц.

В сетях 3G обеспечивается предоставление двух базовых услуг: передача данных и передача голоса. Согласно регламентам ITU (International Telecommunications Union – Международный Союз Электросвязи) сети 3G должны поддерживать следующие скорости передачи данных:

– для абонентов с высокой мобильностью (до 120 км/ч) – не менее 144 Кбит/с;

– для абонентов с низкой мобильностью (до 3 км/ч) – 384 Кбит/с;

– для неподвижных объектов – 2,048 Мбит/с.

В настоящее время сети 3G характеризуются преобладанием трафика data-cards (USB-модемы, ExpressCard/PCMCIA-карты для ноутбуков) над трафиком телефонов и смартфонов 3G.

В сетях с кодовым разделением каналов, в том числе и 3G, есть важное преимущество – улучшенная защита от обрывов связи в движении за счет «мягкого» переключения между станциями. По

мере удаления от одной базовой станции клиента «подхватывает» другая. Она начинает передавать все больше и больше информации, в то время как первая станция передает все меньше и меньше, пока клиент вообще не покинет ее зону обслуживания. При хорошем покрытии сети вероятность обрыва полностью исключается системой подобных «подхватов». Это отличается от поведения систем с частотным и временным разделением каналов (GSM), в которых переключение между станциями «жесткое», и может приводить к задержкам в передаче и даже обрывам соединения.

Выводы

1. Принцип организации сотовой связи состоит в использовании множества маломощных передатчиков. Поскольку диапазон действия таких передатчиков довольно мал, зону обслуживания системы можно разбивать на ячейки, каждая из которых будет обслуживаться собственной антенной (на практике используется гексагональная схема). Каждая ячейка, которой выделяется своя полоса частот, обслуживается базовой станцией, состоящей из передатчика, приемника и модуля управления.
2. В каждой ячейке сотовой сети имеется базовый трансивер. Мощность передаваемых сигналов тщательно регулируется. Как правило, каждой ячейке выделяется 10–50 частот в зависимости от планируемой нагрузки.
3. Предусмотрено несколько вариантов расширения числа обслуживаемых клиентов одной ячейкой: добавление новых каналов, заимствование частот, расщепление ячеек, разбивка ячеек на секторы, микроячейки.
4. Сотовые системы первого поколения являлись аналоговыми, а системы второго поколения – цифровыми, что позволило использовать шифрование, а также средства исправления ошибок для обеспечения качества передачи. В системах первого поколения каждая ячейка поддерживает несколько каналов. В любой момент времени канал может быть выделен только одному пользователю. В системах второго поколения ячейкам также выделяется по несколько каналов, однако каждый канал может совместно использоваться несколькими пользователями посредством схем множественного доступа с временным разделением. Дальнейшее

развитие сотовых систем второго поколения привело к использованию множественного доступа с кодовым разделением (CDMA).

5. Стандарт GSM был разработан для внедрения в Европе общей технологии второго поколения, чтобы одни и те же абонентские устройства можно было использовать по всему континенту.

6. Беспроводные системы связи третьего поколения разрабатываются с целью получения высокоскоростных беспроводных средств передачи не только речи, но и данных, мультимедиа и видео.

10.2. Сети Bluetooth

Bluetooth – это внедренное в микрочип невыключающееся радиоустройство ближнего действия.

Технология была представлена шведским производителем мобильных средств связи Ericsson в 1994 году как средство, позволяющее портативным компьютерам совершать звонки по мобильным телефонам. С тех пор несколько тысяч компаний работают над тем, чтобы технология Bluetooth стала стандартом множества маломощных, действующих на близком расстоянии беспроводных устройств.

Название *Bluetooth* («голубой зуб») произошло от прозвища датского короля Гарольда Блаатанда (Harald Blaatand), жившего в X веке. Стандарты Bluetooth публикуются промышленным консорциумом Bluetooth SIG (Special Interest Group – специальная группа).

Цель разработки стандартов Bluetooth – унифицировать возможности ближней радиосвязи. В диапазоне 2,4 ГГц (общедоступные нелицензируемые частоты для маломощных устройств) два аппарата Bluetooth, находящиеся на расстоянии до 10 м, могут совместно использовать пропускную способность до 720 Кбит/с. Bluetooth предназначена для поддержки многих приложений (полный список достаточно объемен и продолжает пополняться: передача данных, аудио, графики, видео и т. д.). Например, чип Bluetooth может внедряться в такие аудиоустройства, как наушники, беспроводные и обычные телефоны, домашние стереопроигрыватели и цифровые MP3-плейеры. С помощью Bluetooth потребители могут делать следующее:

– звонить с беспроводного головного телефона, удаленно связанного с телефоном ячейки сотовой связи;

– соединять компьютеры с периферией (принтеры, клавиатуры, мыши), не используя кабель;

– подключать без проводов MP3-плейеры к другим машинам с целью загрузки музыкальных файлов;

– организовывать домашние сети.

10.2.1. Области применения Bluetooth

Технология Bluetooth предназначена для работы в среде со многими пользователями. В маленькую сеть, называемую *пикосетью* (piconet), могут объединяться до восьми устройств. Десять таких пикосетей могут сосуществовать в одном радиодиапазоне Bluetooth. Для обеспечения безопасности каждый канал связи кодируется и защищается от подслушивания и интерференции.

Bluetooth предусматривает поддержку трех основных областей применения с использованием беспроводной связи ближнего действия.

1. *Точки доступа для ввода данных* (в том числе посредством голоса). Bluetooth способствует передаче в реальном времени данных и речи, обеспечивая удобную беспроводную связь портативных и стационарных аппаратов связи.

2. *Замена кабеля*. При наличии Bluetooth отпадает необходимость в многочисленных кабельных проводках, которые сопровождают практически все устройства связи. Соединение Bluetooth устанавливается мгновенно, причем связываемые устройства не обязательно должны находиться в пределах прямой видимости. Радиус охвата порядка 10 м, а если использовать усилитель, эту величину можно довести до 100 м.

3. *Организация эпизодических сетей*. Устройство, оснащенное чипом Bluetooth, может мгновенно устанавливать связь с другим устройством, находящимся в пределах области охвата.

Приведем несколько примеров того, как можно использовать технологию Bluetooth.

1. *Телефон «три в одном»*. Если вы в офисе – телефон работает как *интерком* (не нужно платить за услуги телефонии), дома это беспроводной телефон (оплачивается как стационарное устройство), а если вы перемещаетесь, его можно использовать как обычный мобильный телефон (это уже сотовая связь).

2. *Мост Internet*. Портативный ПК можно связать с Internet откуда угодно либо посредством мобильного телефона

(беспроводное соединение), либо с помощью кабеля (PSTN, ISDN, ЛВС, xDSL).

3. *Интерактивная конференция.* На встречах и конференциях информацию можно мгновенно распространять между всеми участниками. Кроме того, проектором можно управлять и не имея проводного соединения.

4. *Удаленный головной телефон.* Соединить головной телефон с мобильным ПК или любым проводным соединением.

5. *Громкоговоритель портативного ПК.* Соединить беспроводной головной микрофон портативным ПК и использовать его как микрофон.

6. *Почта из портфеля.* Получить доступ к электронной почте, не вынимая портативный ПК из портфеля. Как только ПК получит почту, вам об этом сообщит мобильный телефон. Используя тот же мобильный телефон, можно просмотреть входящую почту и прочитать сообщения.

7. Задержанные сообщения. Электронную почту можно занести в ПК. Как только появится возможность воспользоваться мобильным телефоном, сообщения будут посланы немедленно.

8. *Автоматическая синхронизация.* Автоматически синхронизируется настольный компьютер, портативный ПК, ноутбук и мобильный телефон.

9. *Мгновенная цифровая открытка.* Подключить (без проводов) камеру к мобильному телефону или к любому выходу проводной связи, ввести комментарий с мобильного телефона, ноутбука или портативного ПК – и готовую открытку можно отправлять немедленно.

10. *Беспроводной настольный компьютер.* Компьютеру не нужны провода, чтобы соединиться с принтером, сканером, клавиатурой, мышью или локальной сетью.

10.2.2. Стандарты Bluetooth и структура протоколов

Стандарты Bluetooth содержат *технологическую (внутреннюю) спецификацию Bluetooth* и *спецификацию профиля*. *Внутренние спецификации* описывают детали разнообразных уровней протокольной архитектуры Bluetooth (от радиоинтерфейса до управления каналом связи).

В *спецификациях профиля* описано использование технологии Bluetooth для поддержки различных приложений. В каждой

спецификации рассматривается применение технологии, определенной во внутренней спецификации, для реализации конкретной модели использования. В спецификации профиля указывается, какие аспекты внутренних спецификаций Bluetooth являются обязательными, необязательными и неприменимыми. Bluetooth определяется как *многоуровневая протокольная архитектура* (*рис. 10.8*).

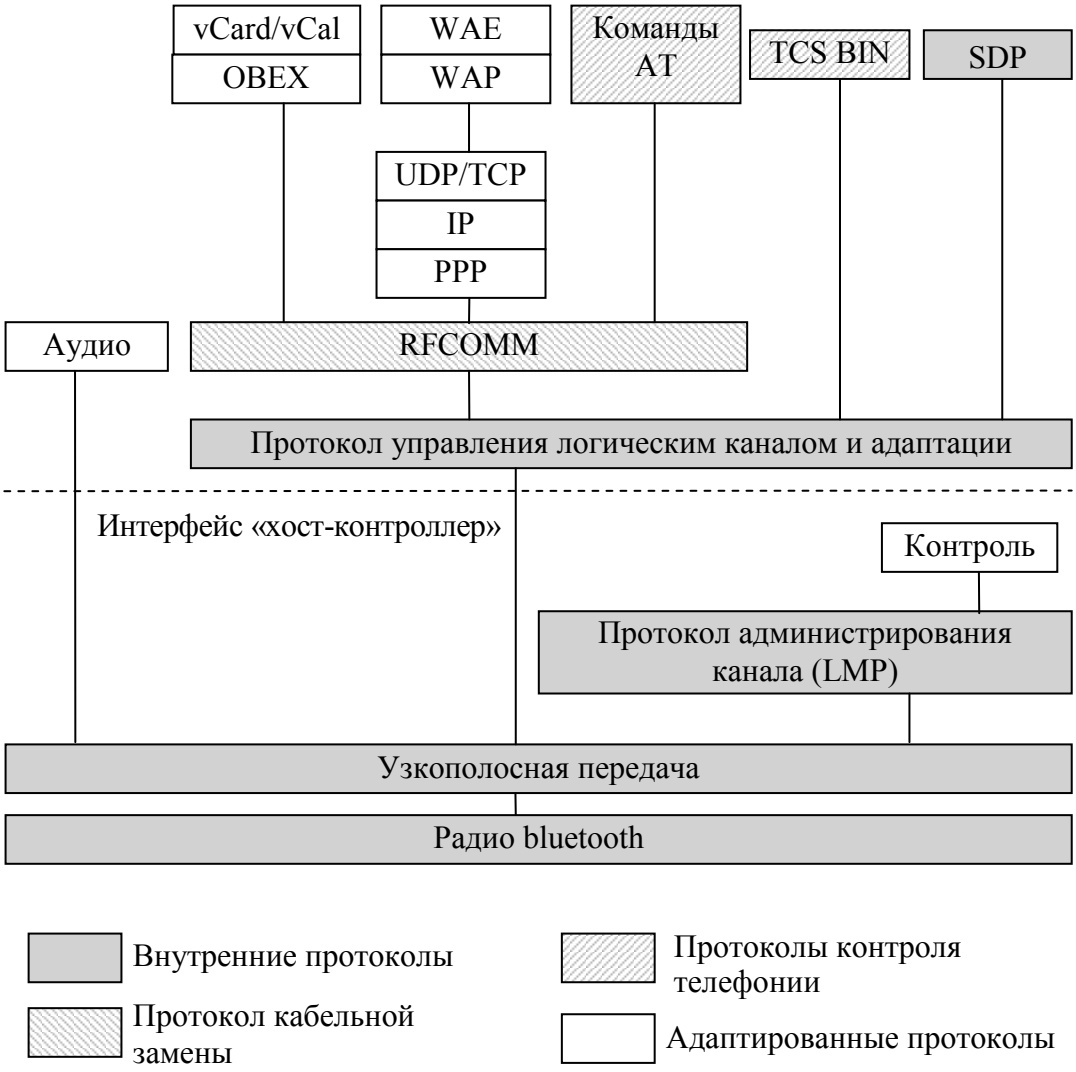


Рис. 10.8. Стек протоколов Bluetooth

Архитектура Bluetooth состоит из внутренних протоколов, протоколов замены кабеля и управления телефонией и адаптированных протоколов (*AT* – сигнальная последовательность (префикс модема); *IP* – сетевой протокол (Internet); *OBEX* – протокол

объектного обмена; *PPP* – протокол двухточечного соединения; *RFCOMM* – связь на радиочастотах; *SDP* – протокол обнаружения службы; *TCP* – транспортный протокол управления передачей; *UDP* – протокол пользовательских дейтаграмм; *TCS BIN* – спецификация управления телефонией; *vCal* – виртуальный календарь; *vCard* – виртуальная карта; *WAE* – среда беспроводных приложений; *WAP* – протокол беспроводных приложений). Внутренние протоколы формируют пятиуровневый стек.

В Bluetooth определен *протокол управления телефонией*. Протокол TCS BIN (telephony control specification binary – спецификация управления телефонией, бинарная) – это протокол с битовой структурой, который определяет передачу сигналов управления вызовами с целью установления сеансов передачи речи и данных между устройствами Bluetooth. Кроме того, он определяет процедуры управления мобильностью для управления группами устройств Bluetooth TCS.

Адаптированный протокол определяется в спецификациях, выпускаемых другими организациями по стандартизации, и вводится в общую архитектуру Bluetooth. Стратегия Bluetooth заключается в создании только необходимых протоколов при максимально возможном использовании имеющихся стандартов.

10.2.4. Модели использования Bluetooth

В документах по профилям Bluetooth определено несколько моделей использования.

Модель использования – это набор протоколов, которые реализуют конкретное приложение на основе Bluetooth.

Каждый профиль определяет протоколы и свойства протоколов, поддерживающие конкретную модель использования. Перечислим модели использования с наивысшим приоритетом.

1. *Передача файлов.* Модель поддерживает передачу каталогов, файлов, документов, изображений и потоковую информацию. Данная модель использования также содержит возможность просмотра папки с удаленного устройства.

2. *Мост Internet*. Используя данную модель, ПК связывается без проводов с мобильным телефоном или беспроводным модемом для удаленного телефонного доступа к сети или факсу.

3. *Доступ к локальной сети*. Данная модель использования позволяет устройствам пикосети получить доступ к локальной

сети. После соединения работа устройства та же, что и при проводном подключении.

4. *Синхронизация*. Данная модель обеспечивает синхронизацию содержащейся на устройствах персональной информации, такой как записи в телефонной книге, календаре, сообщения и заметки. Здесь следует упомянуть IrMC (Ir mobile communications – мобильная связь в инфракрасном диапазоне), протокол IrDA, который позволяет передавать между устройствами обновленную персональную информацию (по схеме клиент – сервер).

5. *Телефон «три в одном»*. Телефонные трубки, которые реализуют данную модель использования, могут работать как беспроводный телефон, подсоединенный к голосовой базовой станции как интерком, связанный с другими телефонами, и как сотовый телефон.

6. *Головной телефон*. Головной телефон может использоваться как устройство аудиоввода/вывода удаленного устройства.

Выводы

1. Целью разработки стандартов Bluetooth явилась необходимость унификации возможностей ближней радиосвязи. Bluetooth определяется как многоуровневая протокольная архитектура.

2. При разработке стандарта Bluetooth упор был сделан на создание только необходимых протоколов при максимально возможном использовании имеющихся, например, TCP/IP, IPX/SPX и т. д.

3. Внутренние протоколы сетей Bluetooth формируют пятиуровневый стек.

4. В документах стандарта Bluetooth определено несколько моделей использования. К моделям с наивысшим приорететом относятся: передача файлов, мост Internet, доступ к локальной сети, синхронизация.

10.3. Сверхвысокоскоростные сети

10.3.1. Общая характеристика стандарта Gigabit Ethernet

В 1996 году было объявлено о создании группы 802.3z для разработки протокола, максимально подобного Ethernet, но с битовой скоростью 1000 Мбит/с.

Первая версия стандарта была рассмотрена в 1997 году, а окончательно стандарт 802.3z был принят 29 июня 1998 года на заседании комитета IEEE 802.3.

Основная идея разработчиков стандарта **Gigabit Ethernet** состоит в максимальном сохранении идей классической технологии Ethernet при достижении битовой скорости в 1000 Мбит/с.

Избыточные связи и тестирование оборудования не поддерживаются технологией Gigabit Ethernet из-за того, что с этими задачами хорошо справляются протоколы более высоких уровней, например, Spanning Tree, протоколы маршрутизации и т. п.

Что же общего в технологии Gigabit Ethernet с технологиями Ethernet и Fast Ethernet?

Сохраняются все форматы кадров Ethernet. По-прежнему будут существовать 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, коаксиал.

Для расширения максимального диаметра сети Gigabit Ethernet в полудуплексном режиме до 200 м разработчики технологии предприняли естественные меры, основывающиеся на известном соотношении времени передачи кадра минимальной длины и времени двойного оборота.

Минимальный размер кадра был увеличен (без учета преамбулы) с 64 до 512 байт или до 4096 бит. Станция может передать подряд несколько кадров с общей длиной не более 65 536 бит или 8192 байт. Если станции нужно передать несколько небольших кадров, то она может не дополнять их до размера в 512 байт, а передавать подряд до исчерпания предела в 8192 байт (в этот предел входят все байты кадра, в том числе преамбула, заголовок, данные и контрольная сумма). Предел 8192 байт называется BurstLength.

10.3.3. Спецификации физической среды стандарта 802.3z

В стандарте 802.3z определены следующие типы физической среды:

– одномодовый волоконно-оптический кабель;

– многомодовый волоконно-оптический кабель 62,5/125;

– многомодовый волоконно-оптический кабель 50/125;

– двойной коаксиал с волновым сопротивлением 75 Ом.

Многомодовый кабель. Для передачи данных по традиционному для компьютерных сетей многомодовому волоконно-оптическому кабелю стандарт определяет применение излучателей, работающих на двух длинах волн: 1300 и 850 нм. Для *многомодового оптоволокна* стандарт 802.3z определил спецификации l000Base-SX и l000Base-LX.

В первом случае используется длина волны 850 нм (S означает Short Wavelength – короткая волна), а во втором – 1300 нм (L от Long Wavelength – длинная волна).

Для спецификации l000Base-SX предельная длина оптоволоконного сегмента для кабеля 62,5/125 составляет 220 м, а для кабеля 50/125 – 500 м.

Одномодовый кабель. Для спецификации l000Base-LX в качестве источника излучения всегда применяется полупроводниковый лазер с длиной волны 1300 нм.

Максимальная длина кабеля для *одномодового волокна* достигает 5000 м.

Для присоединения оптоволоконного трансивера к многомодовому кабелю необходимо использовать специальный адаптер.

Твинаксиальный кабель. В качестве среды передачи данных используется высококачественный твинаксиальный кабель (Twinax) с волновым сопротивлением 150 Ом (2 × 75 Ом). Максимальная длина *твинаксиального сегмента* составляет всего 25 м, поэтому такое решение подходит для оборудования, расположенного в одной комнате.

10.3.4. Gigabit Ethernet на «витой паре» пятой категории

Как известно, каждая пара кабеля категории 5 имеет гарантированную полосу пропускания до 100 МГц. Для передачи по такому кабелю данных со скоростью 1000 Мбит/с было решено организовать параллельную передачу одновременно по всем 4 парам кабеля (так же, как и в технологии 100VG-AnyLAN).

Для распознавания коллизий и организации *полнодуплексного режима* разработчики спецификации 802.3ab применили технику, используемую при организации дуплексного режима на одной паре проводов в современных модемах и аппаратуре передачи данных абонентских окончаний ISDN (*рис. 10.9*).

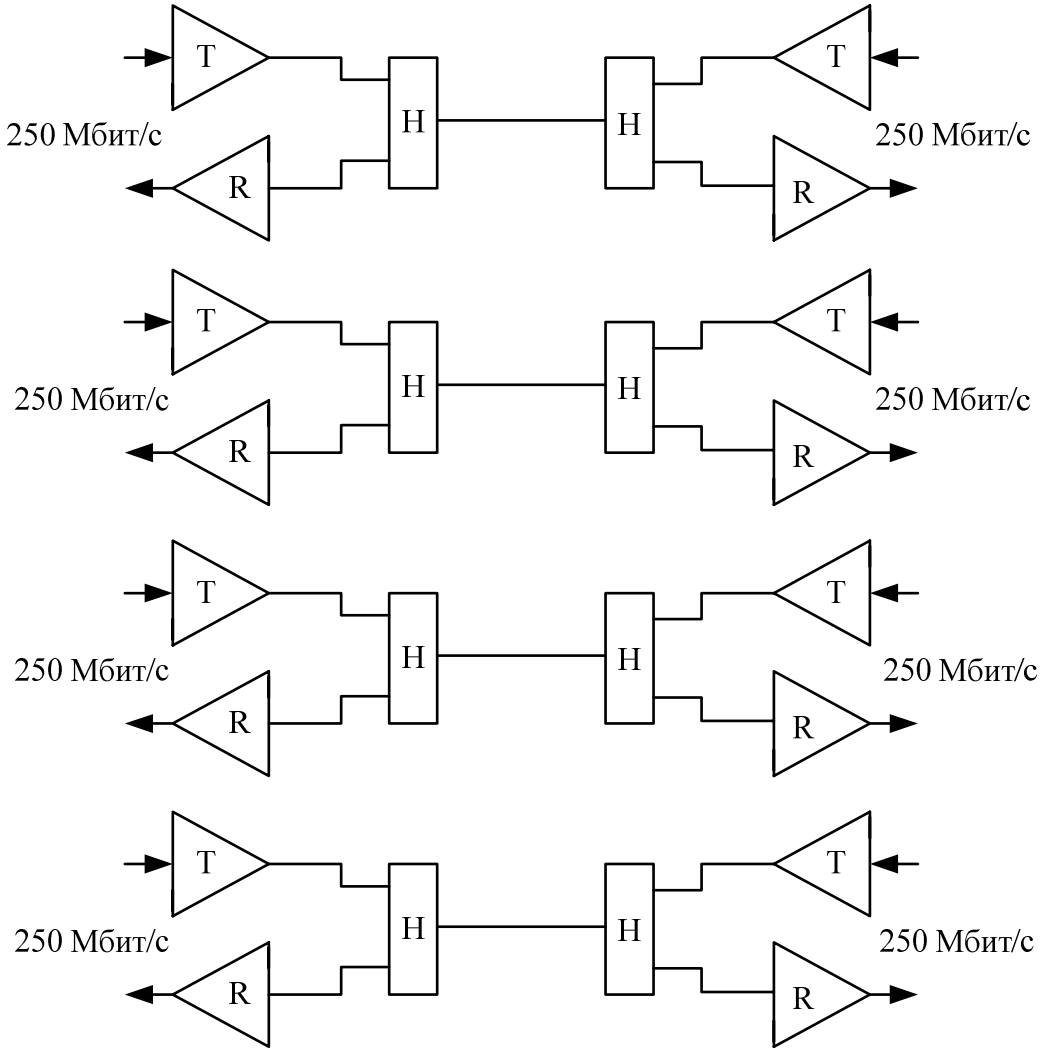


Рис. 10.9. Двунаправленная передача
по четырем парам UTP категории 5

Схема гибридной развязки (H) позволяет приемнику (T) и передатчику (R) одного и того же узла использовать одновременно витую пару и для приема и для передачи (так же, как и в трансиверах коаксиального Ethernet).

При полудуплексном режиме работы получение встречного потока данных считается коллизией, а для полнодуплексного режима работы – нормальной ситуацией.

10.3.5. Сети на основе технологии ATM

Технология ATM (Asynchronous Transfer Mode) используется как в локальных, так и в глобальных сетях. Основная ее идея – пе-

редача цифровых, голосовых и мультимедийных данных по одним и тем же каналам.

Скорость передачи – более 2488 Мбит/с. В качестве среды передачи информации в локальной сети технология ATM предполагает использование оптоволоконного кабеля и неэкранированную витую пару. Используемые коды – 4Б/5В и 8В/10В.

Вся информация передается упакованной в микропакеты (ячейки, cells) длиной всего лишь в 53 бита. Главный недостаток сетей с технологией ATM состоит в их полной несовместимости ни с одной из существующих сетей. Плавный переход на ATM в принципе невозможен, нужно менять сразу все оборудование, а стоимость его пока что очень высока.

Выводы

1. 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.

2. Разработчики технологии Gigabit Ethernet сохранили большую степень преемственности с технологиями Ethernet и Fast Ethernet. Gigabit Ethernet использует те же форматы кадров, что и предыдущие версии Ethernet, работает в полнодуплексном и полудуплексном режимах, поддерживая на разделяемой среде тот же метод доступа CSMA/CD с минимальными изменениями.

3. В 1998 году был принят стандарт 802.3z, который определяет использование в качестве физической среды трех типов кабеля: многомодового оптоволоконного (расстояние до 500 м), одномодового оптоволоконного (расстояние до 5000 м) и двойного коаксиального (twinax), по которому данные передаются одновременно по двум медным экранированным проводникам на расстояние до 25 м. Реализация Gigabit Ethernet на UTP категории 5 требует использования всех 4 пар медного кабеля данной категории.

4. В целом, Gigabit Ethernet наряду с технологией ATM является наиболее перспективным направлением развития кабельных сетей.

10.4. Виртуальные частные сети и удаленный доступ

Возможность использования удаленными пользователями ресурсов локальной сети называется **удаленным доступом** (remote access). Различают два основных вида удаленного доступа:

– *соединение по коммутируемой линии* (dial-up connection);

– *соединение с использованием виртуальных частных сетей* (Virtual Private Networks, VPN).

Оба вида соединений работают по модели «клиент – сервер».

Клиент удаленного доступа – это компьютер, который имеет возможность подключаться к удаленному компьютеру и работать с его ресурсами или с ресурсами удаленной сети так же, как с ресурсами своей локальной сети. Единственное отличие удаленной работы от локальной с точки зрения клиента – более низкая скорость соединения.

Сервер удаленного доступа (Remote Access Server, RAS) – это компьютер, способный принимать входящие запросы от клиентов удаленного доступа и предоставлять им собственные ресурсы или ресурсы своей локальной сети.

Компьютер с установленной операционной системой Windows Server 2003 может исполнять роль как клиента удаленного доступа, так и сервера. В последнем случае на нем должна быть запущена *Служба маршрутизации и удаленного доступа* (Routing and Remote Access Service, RRAS).

10.4.1. Виды коммутируемых линий

Соединения по коммутируемым линиям могут осуществляться с использованием следующих средств связи.

1. *Телефонные сети* – наиболее распространенный и дешевый вариант, хотя и самый медленный (максимальная скорость передачи данных 56,6 Кбит/с). Предполагает установку модемов на клиенте и сервере.

2. *Сети ISDN* (Integrated Services Digital Network – цифровая сеть с комплексными услугами) обеспечивают скорость передачи данных 128 Кбит/с, но их использование дороже, чем использование обычных телефонных сетей.

3. *ATM поверх ADSL* – передача трафика ATM (Asynchronous Transfer Mode – асинхронный режим передачи) посредством

линий ADSL (Asymmetric Digital Subscriber Line – асимметричная цифровая абонентская линия).

Для соединения посредством виртуальных частных сетей клиентский компьютер и сервер должны быть подключены к Интернету.

10.4.2. Протоколы удаленного доступа

Подключение клиента к серверу удаленного доступа по коммутируемым линиям состоит из следующих основных этапов:

– установка соединения;

– аутентификация и авторизация клиента удаленного доступа;

– сервер удаленного доступа выступает в роли маршрутизатора, предоставляя доступ клиенту к ресурсам локальной сети, серверам баз данных, электронной почте, файловым серверам, принтерам и т. д.

Схема подключения представлена на *рис. 10.10*.

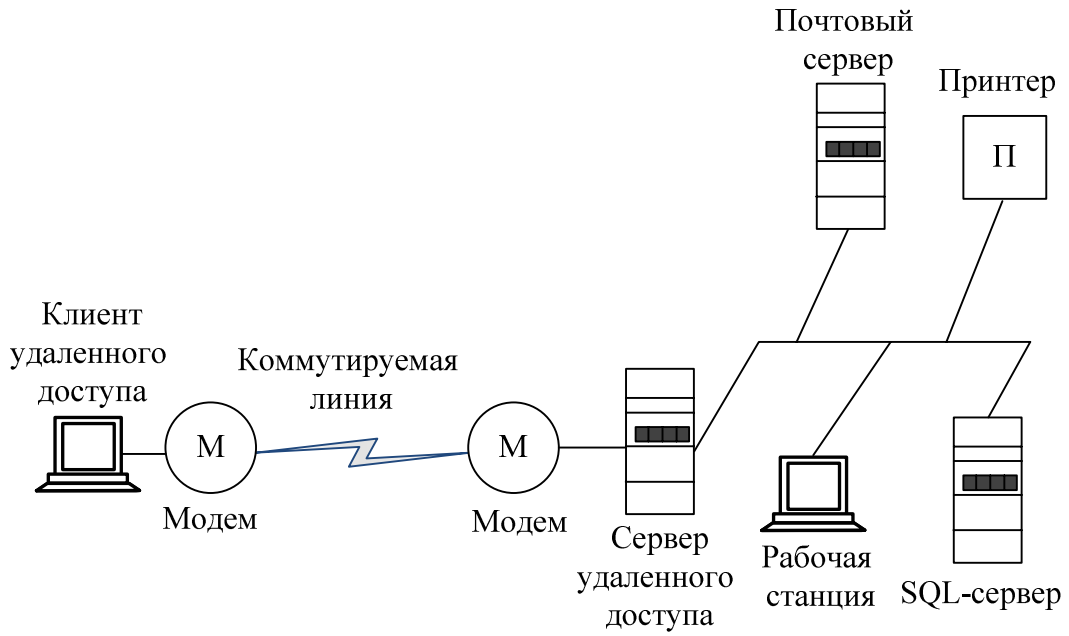


Рис. 10.10. Схема подключения удаленного доступа по коммутируемым линиям

Для соединений удаленного доступа по коммутируемым линиям было разработано несколько специальных протоколов. Например, Windows Server 2003 поддерживает два протокола удаленного доступа:

– *протокол SLIP* (Serial Line Internet Protocol – межсетевой протокол для последовательного канала);

– *протокол PPP* (Point-to-Point Protocol – протокол соединения «точка – точка»).

Протокол SLIP является одним из старейших протоколов удаленного доступа и предлагает передачу TCP/IP-пакетов без обеспечения безопасности данных и контроля целостности. Протокол описан в RFC 1055. В Windows Server 2003 поддержка протокола SLIP реализована только на уровне клиента.

Протокол PPP предназначен для коммутируемых соединений типа «точка – точка». Это означает, что в протоколе отсутствуют средства адресации, поэтому в процессе связи могут принимать участие только два компьютера – клиент и сервер.

Протокол PPP, в отличие от SLIP, обеспечивает функции безопасности и контроля ошибок. Описание протокола содержится в RFC 1332, 1661 и 1662.

Соединение «точка – точка» устанавливается в четыре этапа.

1. *Настройка параметров канального уровня*. Клиент и сервер согласовывают максимальный размер кадра, возможность сжатия, протокол аутентификации и некоторые другие параметры.

2. *Аутентификация клиента*. Сервер осуществляет аутентификацию и авторизацию клиента на основе протокола, выбранного на предыдущем этапе.

3. *Обратный вызов* (callback). В целях безопасности может использоваться процедура обратного вызова, когда сервер разрывает соединение с клиентом и сам вызывает его по определенному телефонному номеру.

4. *Настройка протоколов верхних уровней*. Сервер отправляет клиенту список протоколов верхних уровней, отвечающих за передачу данных, шифрование и сжатие. Клиент выбирает один из подходящих протоколов списка.

10.4.3. Протоколы аутентификации удаленных клиентов

Разработано несколько протоколов, используемых для аутентификации удаленных клиентов.

1. *PAP* (Password Authentication Protocol) – протокол аутентификации по паролю (описан в RFC 1334). Самый простой протокол аутентификации, в котором имя пользователя и пароль передаются открытым, незашифрованным способом. В Windows Server 2003

протокол PAP применяется только в том случае, если клиент удаленного доступа не поддерживает больше никаких протоколов.

2. *CHAP* (Challenge Handshake Authentication Protocol) – протокол аутентификации с предварительным согласованием вызова (описан в RFC 1994). В этом протоколе клиент посылает серверу пароль в виде специальной хеш-последовательности, созданной с использованием *алгоритма MD-5*. Сервер принимает *хеш (свертка) пароля клиента*, вычисляет хеш по хранимому у себя паролю и сравнивает обе последовательности. В случае совпадения соединение устанавливается, иначе происходит разрыв. Недостатком является отсутствие взаимной аутентификации, т. е. сервер аутентифицирует клиента, а клиент не получает информации о подлинности сервера.

3. *MS-CHAP* (Microsoft Challenge Handshake Authentication Protocol) – реализация протокола CHAP, разработанного Microsoft (описан в RFC 2433). Действует по принципу протокола CHAP, за исключением того, что для хеширования используется *алгоритм MD-4*, а не MD-5.

4. *MS-CHAPv2* – вторая версия протокола MS-CHAP (описан в RFC 2759), где также, как и в MS-CHAP, применяется *алгоритм хеширования MD-4*, но отличием является требование взаимной аутентификации. Между клиентом и сервером происходит обмен следующими сообщениями:

– сервер отправляет клиенту сообщение, содержащее некоторую последовательность символов, называемую ***строкой вызова***;

– клиент отправляет серверу хеш-последовательность, полученную на основе строки вызова и пароля пользователя, а также свою строку вызова для сервера;

– сервер вычисляет хеш по своей строке вызова и пользовательскому паролю, сравнивает его с полученным хешем от клиента и в случае успеха отправляет хеш, вычисленный на основе своей строки вызова, строки вызова от клиента, имени и пароля пользователя;

– клиент, получая сообщение сервера, вычисляет хеш на основе тех же данных, и в случае совпадения вычисленного хеша с полученным от сервера процесс взаимной аутентификации считается законченным успешно.

5. *EAP* (Extensible Authentication Protocol) – расширяемый протокол аутентификации (описан в RFC 2284). Отличается от вышеописанных протоколов тем, что выбор типа аутентификации EAP происходит в процессе соединения.

6. В ОС Windows Server применяются следующие типы аутентификации EAP: EAP-MD5, CHAP, EAP-TLS (Transport Level Security, безопасность на транспортном уровне), PEAP (Protected EAP, защищенный EAP).

10.4.4. Общая характеристика виртуальных частных сетей

В последние годы стоимость использования каналов связи Интернет стала уменьшаться и скоро стала ниже, чем цена использования коммутируемых линий. Однако при установлении соединения через Интернет возникла серьезная проблема – обеспечение безопасности, так как сеть является открытой и злоумышленники могут перехватывать пакеты с конфиденциальной информацией. Решением этой проблемы стала технология виртуальных частных сетей.

Виртуальные частные сети (Virtual Private Network, VPN) – это защищенное соединение двух узлов через открытые сети. При этом организуется виртуальный канал, обеспечивающий безопасную передачу информации, а узлы, связанные VPN, могут работать так, как будто соединены напрямую.

Компьютер, инициирующий VPN-соединение, называется **VPN-клиентом**. Компьютер, с которым устанавливается соединение, называется **VPN-сервером**.

VPN-магистраль – это последовательность каналов связи открытой сети, через которые проходят пакеты виртуальной частной сети.

Существует два типа VPN-соединений:

– *соединение с удаленными пользователями* (Remote Access VPN Connection);

– *соединение маршрутизаторов* (Router-to-Router VPN Connection).

Соединение с удаленными пользователями осуществляется в том случае, если одиночный клиент подключается к локальной сети организации через VPN (*рис. 10.11*). Другие компьютеры, подключенные к VPN-клиенту, не могут получить доступ к ресурсам локальной сети.

Соединение маршрутизаторов устанавливается между двумя локальными сетями, если узлы обеих сетей нуждаются в доступе к ресурсам друг друга (*рис. 10.12*). При этом один из маршрутизаторов играет роль VPN-сервера, а другой – VPN-клиента.

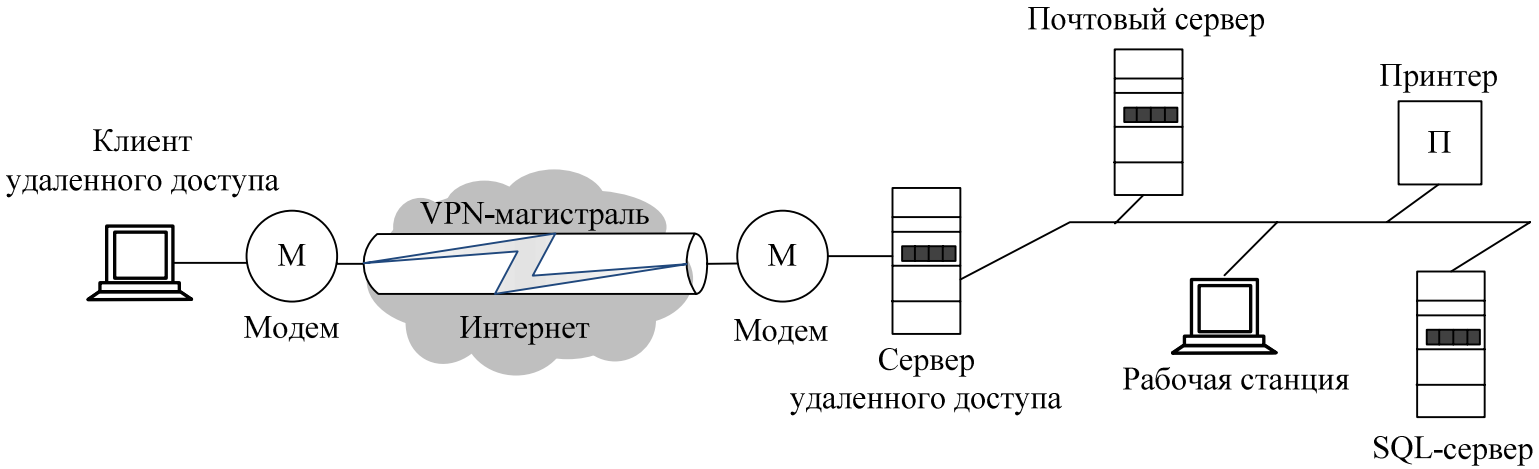


Рис. 10.11. Схема VPN-соединения с удаленным пользователем

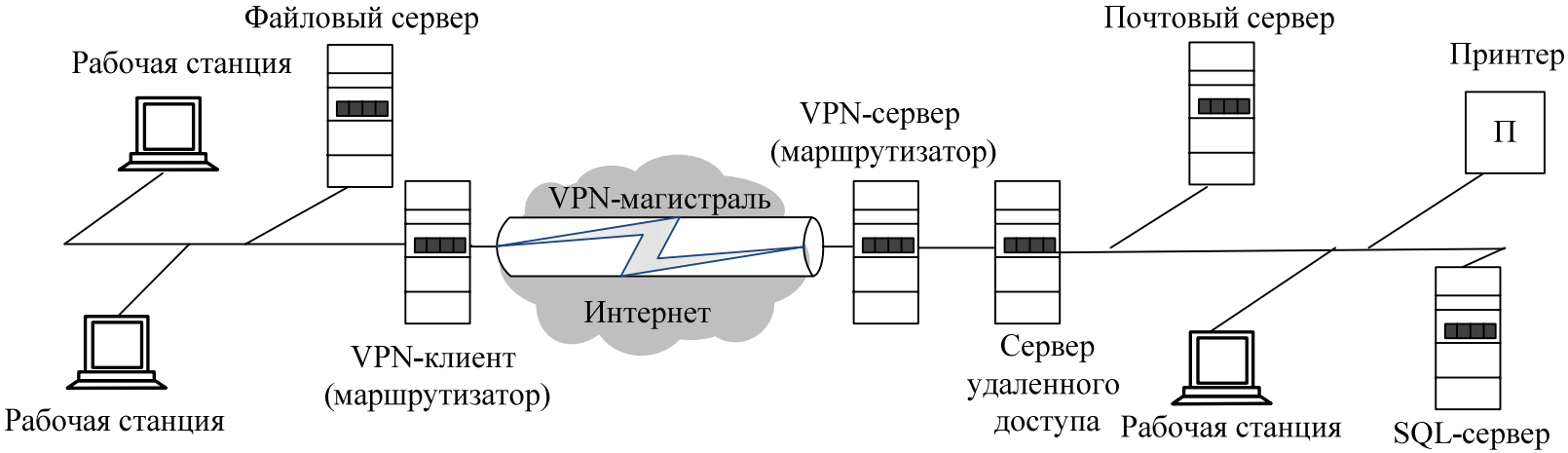


Рис. 10.12. Схема VPN-соединения между маршрутизаторами

10.4.5. Протоколы виртуальных частных сетей

Безопасность передачи IP-пакетов через Интернет в VPN реализуется с помощью туннелирования.

Туннелирование (tunneling) – это процесс включения IP-пакетов в пакеты другого формата, позволяющий передавать зашифрованные данные через открытые сети.

В современных системах Windows Server поддерживаются следующие протоколы туннелирования.

1. *PPTP* (Point-to-Point Tunneling Protocol) – *протокол туннелирования соединений «точка – точка»*, основан на протоколе PPP (описан в RFC 2637). Поддерживает все возможности, предоставляемые PPP, в частности аутентификацию по протоколам PAP, CHAP, MS-CHAP, MS-CHAPv2, EAP. Шифрование данных обеспечивается методом MPPE (Microsoft Point-to-Point Encryption), который применяет алгоритм RSA/RC4. Сжатие данных происходит по протоколу MPPC (Microsoft Point-to-Point Compression), описанному в RFC 2118.

Недостатком протокола является относительно низкая скорость передачи данных.

2. *L2TP* (Layer Two Tunneling Protocol – *туннельный протокол канального уровня*) – протокол туннелирования, основанный на протоколе L2F (Layer Two Forwarding), разработанном компанией Cisco, и протоколе PPTP (описан в RFC 2661). Поддерживает те же протоколы аутентификации, что и PPP. Для шифрования данных используется протокол IPsec. Также поддерживает сжатие данных. Имеет более высокую скорость передачи данных, чем PPTP.

Протокол PPTP остается единственным протоколом, который поддерживают старые версии Windows (Windows NT 4.0, Windows 98, Windows Me). Однако существует бесплатный VPN-клиент Microsoft L2TP/IPsec, который позволяет старым операционным системам Windows устанавливать соединение VPN по протоколу L2TP.

Выводы

1. Использование удаленными пользователями ресурсов локальной сети называется удаленным доступом.

2. Различают два основных вида удаленного доступа: соединение по коммутируемой линии; соединение с использованием виртуальных частных сетей. Оба вида соединений работают по модели «клиент – сервер».

3. Для соединений удаленного доступа по коммутируемым линиям было разработано несколько специальных протоколов, но в Windows Server поддерживается только два: протокол SLIP; протокол PPP, отличающийся обеспечением функций безопасности и контроля ошибок.

4. В современных операционных системах серверного сегмента применяются следующие протоколы аутентификации: PAP, CHAP, MS-CHAP, MS-CHAPv2, EAP.

5. Под виртуальными частными сетями понимают защищенное соединение двух узлов через открытые сети, при этом организуется виртуальный канал, обеспечивающий безопасную передачу информации, а узлы, связанные VPN, могут работать так, как будто соединены напрямую.

6. Безопасность передачи IP-пакетов через Интернет в VPN реализуется с помощью туннелирования, которое в свою очередь обеспечивается протоколами PPTP и L2TP.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что называют сотовой радиосвязью?
2. Опишите принципы организации сотовой сети.
3. Какие существуют структуры сотовых систем?
4. Опишите функционирование сотовой сети.
5. Охарактеризуйте сотовые сети первого поколения.
6. Опишите сотовые сети второго поколения.
7. Охарактеризуйте архитектуру глобальной системы мобильной связи.
8. Опишите сотовые сети третьего поколения.
9. Приведите основные характеристики сотовых систем третьего поколения.
10. Что такое сети Bluetooth?
11. Какова область применения сетей Bluetooth?
12. Опишите стек протоколов Bluetooth.
13. Какие существуют модели использования сетей Bluetooth?

14. Приведите общую характеристику стандарта Gigabit Ethernet.

15. Какие типы кабеля могут использоваться в сетях на базе технологии Gigabit Ethernet?

16. Что такое твинаксиальный кабель?

17. Какой метод доступа используется в сетях Gigabit Ethernet?

18. Опишите технологию ATM.

19. Дайте определение удаленного доступа.

20. Дайте определение виртуальных частных сетей.

21. Перечислите основные протоколы виртуальных частных сетей.

22. Назовите основные протоколы удаленного доступа.

23. Перечислите протоколы аутентификации, используемые в технологиях удаленного доступа.

11. БЕЗОПАСНОСТЬ И НАДЕЖНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ

11.1. Основные понятия и определения

Рассмотрим некоторые базовые понятия, относящиеся к изучаемой предметной области.

Теория защиты информации – система основных идей, относящихся к защите информации, дающая целостное представление о сущности проблемы защиты, закономерностях ее развития и существенных связях с другими отраслями знания, формирующаяся на основе опыта практического решения задач защиты и определяющая основные ориентиры в направлении совершенствования практики защиты информации.

Защита информации – это комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации.

Следует заметить, что наряду с термином «*защита информации*» применительно к компьютерным сетям широко используется, как правило, в близком значении, термин «*компьютерная безопасность*».

Компьютерная безопасность – одна из основных задач, решаемых любой компьютерной сетью. Проблему безопасности можно рассматривать с разных сторон – злонамеренная порча данных, конфиденциальность информации, несанкционированный доступ, хищения и т. п.

Надежность компьютерной сети – характеристика способности ее аппаратного, программного и программно-аппаратного обеспечения выполнить при определенных условиях требуемые функции в течение определенного периода времени. Повышение надежности основано на принципе предотвращения неисправностей путем снижения интенсивности отказов и сбоев за счет применения электронных схем и компонентов с высокой и сверхвысокой степенью интеграции, снижения уровня помех, облегченных режимов работы схем, обеспечения тепловых режимов их работы, а также за счет совершенствования методов сборки аппаратуры.

Главной целью повышения надежности систем является обеспечение целостности хранимых в них данных.

Отказоустойчивость – это такое свойство вычислительной системы, которое обеспечивает ей как логической машине возможность продолжения действий, заданных программой, после возникновения неисправностей. Введение отказоустойчивости требует избыточного аппаратного и программного обеспечения.

Секретность (**конфиденциальность**) информации – свойство информации быть известной только допущенным и прошедшим авторизацию субъектам системы (пользователям, программам, процессам и др.); статус, предоставленный информации и определяющий требуемую степень ее защиты.

Субъект – активный компонент системы, который может инициировать поток информации или изменить состояние системы.

Объект – пассивный компонент системы, хранящий, перерабатывающий, передающий или принимающий информацию (например, страницы, файлы, папки, директории, компьютерные программы, устройства и т. д.).

Доступ – специальный тип взаимодействия между объектом и субъектом, в результате которого создается поток информации от одного к другому.

Санкционированный доступ (СД) к информации – это доступ к информации, не нарушающий установленные правила разграничения доступа.

Несанкционированный доступ (НСД) к информации характеризуется нарушением установленных правил разграничения доступа. Несанкционированный доступ является наиболее распространенным видом компьютерных нарушений. НСД использует любую ошибку в системе защиты и возможен при нерациональном выборе средств защиты, их некорректной установке и настройке.

Пассивное вторжение (***перехват информации***) характеризуется тем, что нарушитель только наблюдает за прохождением информации по каналу связи, не вторгаясь ни в информационный поток, ни в содержание передаваемой информации.

Активное вторжение характеризуется стремлением нарушителя подменить информацию, передаваемую в сообщении. Он может выборочно модифицировать или добавлять правильное или ложное сообщение, удалять, задерживать или изменять порядок

следования сообщений, а также аннулировать или задерживать все сообщения, передаваемые по каналу.

Удаленная атака – информационное разрушающее воздействие на распределенную компьютерную сеть, программно осуществленное по каналам связи.

Интруз – физическое лицо или процесс, которые реализуют неразрешенный, или несанкционированный, доступ к информации, т. е. ***атаку*** на систему.

Авторизация – предоставление субъектам доступ к объектам системы. Доступ к объекту означает доступ к содержащейся в нем информации.

Аутентификация – проверка идентификации пользователя, устройства или другого компонента в системе (обычно для принятия решения о разрешении доступа к ресурсам системы). Частным вариантом аутентификации является установление принадлежности сообщения конкретному автору.

Целостность – состояние данных или компьютерной системы, в которой данные и программы используются установленным способом, обеспечивающим устойчивую работу системы и единство данных.

Безопасная (***защищенная***) **система** – система со средствами защиты, которые успешно и эффективно противостоят угрозам безопасности (возможным действиям, которые прямо или косвенно могут нанести ущерб системе).

11.2. Методы обеспечения надежности компьютерных сетей

Один из способов решения рассматриваемой проблемы заключается в использовании *помехоустойчивого кодирования*.

Методы помехоустойчивого кодирования относятся к классу избыточных. Определение рассматриваемых методов как «помехоустойчивые» означает, прежде всего, что они являются противодействием помехам, действующим на систему и приводящим к ошибкам в данных.

Суть этих методов состоит в преобразовании исходного информационного сообщения X_k (k – длина сообщения), называемого также *информационным словом*. К слову, X_k дополнительно

присоединяют (наиболее часто по принципу конкатенации) избыточные символы длиной r бит, составляющие *избыточное слово* X_r. Таким образом формируют *кодовое слово* X_n длиной $n = k + r$ двоичных символов: $X_n = X_k X_r$. Информацию содержит только информационное слово. Назначение слова X_r – обнаружение и исправление ошибок.

В зависимости от принципа вычисления дополнительных символов и их числа реализуются различные алгоритмы помехоустойчивого кодирования. Общим является то, что избыточное слово X_r генерируется на передающей стороне и используется принимающей для обнаружения и исправления ошибок. С учетом избыточных блоков обобщенная структурная схема системы передачи информации примет вид, показанный на *рис. 11.1*.

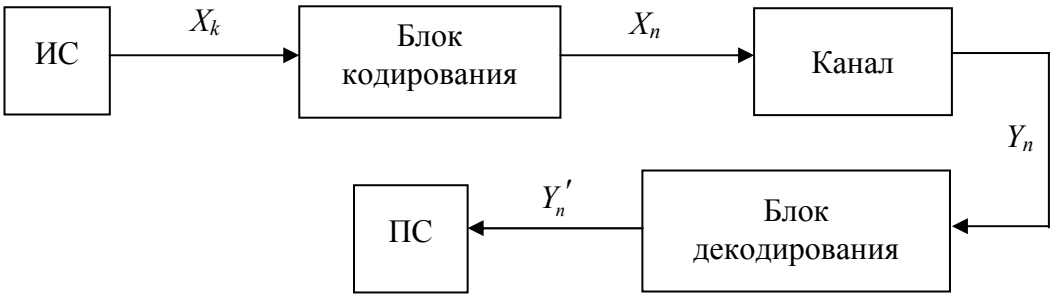


Рис. 11.1. Обобщенная структурная схема системы передачи информации с помехоустойчивым кодированием

Для дальнейшего рассмотрения необходимо упомянуть о некоторых базовых понятиях теории помехоустойчивого кодирования.

Вес по Хеммингу произвольного двоичного слова $X(w(X))$ равен количеству ненулевых символов в слове.

Пример 1. $X = 1101011$. Тогда $w(X = 1101011) = 5$.

Расстояние по Хеммингу или кодовое расстояние (d) между двумя произвольными двоичными словами (X, Y) одинаковой длины равно количеству позиций, в которых X и Y отличаются между собой.

Пример 2. $X = 101$, $Y = 110$. Очевидно, что $d(X, Y) = 2$.

Кодовое расстояние можно вычислить как вес от суммы по модулю 2 этих двух слов: $d(X, Y) = w(X \oplus Y)$.

Пример 3. $X = 1011$, $Y = 0000$; $d(X, Y) = 3$:

$$\begin{array}{r} 1011 \\ 0000 \\ \hline w(1011) = 3 \end{array}.$$

Пример 4. $X = 11111$, $Y = 11111$; $d(X, Y) = 0$.

Длина слова и *расстояние Хемминга – основополагающие понятия* в теории помехоустойчивого кодирования информации.

Все многообразие существующих кодов для обнаружения и исправления ошибок можно разделить на два больших класса: линейные и нелинейные коды.

Линейные коды базируются на использовании линейных (как правило, умножение и сложение по модулю два соответствующих символов) операций над данными, **нелинейные** – соответственно нелинейных операций.

11.2.1. Теоретические основы линейных блочных кодов

Линейные блочные коды – это класс кодов с контролем четности, которые можно описать парой чисел (n, k).

Первое из чисел определяет длину кодового слова (X_n), второе – длину информационного слова (X_k). Отношение числа бит данных к общему числу бит данных k/n именуется *степенью кодирования* (code rate) – доля кода, которая приходится на полезную информацию.

Для формирования проверочных символов (кодирования) используется **порождающая матрица** – совокупность базисных векторов, будет далее записываться в виде матрицы G размерностью $k \times n$ с единичной подматрицей (I) в первых k строках и столбцах:

$$G = [P \mid I]. \qquad (11.1)$$

Матрица G называется порождающей матрицей линейного корректирующего кода в приведенно-ступенчатой форме.

Кодовые слова являются линейными комбинациями строк матрицы G (кроме слова, состоящего из нулевых символов). Кодирование, результатом которого является кодовое слово X_n, заключается в умножении вектора сообщения длиной k (X_k) на порождающую матрицу по правилам матричного умножения (все операции выполняются по модулю два). Очевидно, что при этом первые k символов кодового слова равны соответствующим

символам сообщения, а последние r символов (X_r) образуются как линейные комбинации первых.

Для всякой порождающей матрицы G существует матрица H размерности $r \times n$, задающая базис нулевого пространства кода и удовлетворяющая равенству:

$$G \cdot H^T = 0. \tag{11.2}$$

Матрица H, называемая **проверочной**, может быть представлена так:

$$H = \left[-P^T \;\vdots\; I \right]. \tag{11.3}$$

В последнем выражении I – единичная матрица порядка r .

Кодовое слово X_n может быть получено на основе следующего тождества:

$$H \cdot (X_n)^T = 0. \tag{11.4}$$

Результат умножения сообщения (Y_n) на *транспонированную* проверочную матрицу (H) называется **синдромом** S:

$$S = (Y_n)^T \cdot H, \tag{11.5}$$

где $Y_n = y_1, y_2, \ldots, y_n$.

Слово Y_n обычно представляют в следующем виде:

$$Y_n = X_n \oplus E, \tag{11.6}$$

где $E = e_1, e_2, \ldots, e_n$ – *вектор ошибки*.

Если все r символов синдрома нулевые ($S = 0$), то принимается решение об отсутствии ошибок в принятом сообщении, в противном случае – об их наличии.

В общем случае код, характеризующийся *минимальным кодовым расстоянием* $d_{\min}$ между двумя произвольными кодовыми словами, позволяет обнаруживать t_0 ошибок, где $t_0 = \dfrac{d}{2}$, если d – четно, и $t_0 = \dfrac{d-1}{2}$, если d – нечетно. Количество исправляемых кодом ошибок ($t_и$) определяется следующим образом:

$$t_и = \begin{cases} \dfrac{d-1}{2}, \; d - \textit{нечетное}, \\ \dfrac{d-2}{2}, \; d - \textit{четное}. \end{cases} \tag{11.7}$$

Избыточный код простой четности. Простейший избыточный код основан на контроле четности (либо нечетности) единичных символов в сообщении. Количество избыточных символов r всегда равно 1 и не зависит от k. Значение этого символа будет нулевым, если сумма всех символов кодового слова по модулю 2 равна нулю.

Назначение X_r в данном алгоритме – обнаружение ошибки. Код простой четности позволяет обнаруживать все нечетные ошибки (нечетное число ошибок), но не позволяет их исправлять. Нетрудно убедиться, что данный код характеризуется минимальным кодовым расстоянием, равным 2.

Пример 5. $X_k = 10101$, тогда

$$X_r = \sum_i^n X_i = 1 \oplus 0 \oplus 1 \oplus 0 \oplus 1 = 1.$$

Проверочная матрица для данного случая будет состоять из одной строки и шести столбцов и примет следующий вид:

$$H = 11111\ 1.$$

Кодовое слово X_n, вычисленное в соответствии с (11.4), будет равно 10101 1. Как видим, $w(X_n)$ имеет четное значение.

Слово X_n будет передаваться от источника сообщения к приемнику сообщения (например, от одного компьютера к другому). Пусть на приемной стороне имеем $Y_n = 1\underline{1}101\ 1$: $Y_k = 1\underline{1}101$ и $Y_r = 1$ (ошибочный символ подчеркнут).

Для вычисления синдрома ошибки в соответствии с (11.5) достаточно выполнить следующие простые действия:

а) вычисляется дополнительное слово (в данном случае – символ) Y_r', которое является сверткой по модулю 2 слова Y_k:

$$Y_r' = 1 \oplus 1 \oplus 1 \oplus 0 \oplus 1 = 0;$$

б) вычисляется синдром $S = Y_r \oplus Y_r' = 1 \oplus 0 = 1$. Неравенство синдрома нулю означает, что получено сообщение с ошибкой (или с ошибками).

11.2.2. Код Хемминга

Рассмотрим более подробно методы помехоустойчивого кодирования на примере широкоизвестного и часто используемого кода Хемминга. Данный код характеризуется минимальным кодовым расстоянием $d_{\min} = 3$. При его использовании кодирование

сообщения также должно удовлетворять соотношению (11.4). Причем *вес столбцов подматрицы A должен быть больше либо равен 2*. Второй особенностью данного кода является то, что используется *расширенный контроль четности групп символов информационного слова*, т. е. $r > 1$. Для упрощенного вычисления r можно воспользоваться следующим простым соотношением:

$$r = \log_2 k + 1. \tag{11.8}$$

В сравнении с предыдущим кодом данный позволяет не только обнаруживать, но и исправлять одиночную ошибку в кодовом слове (см. (11.7)).

В нашем рассмотрении подматрицу A можно определить как:

$$A = \begin{bmatrix} h_{11} & h_{12} & \cdots & h_{1k} \\ h_{21} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ h_{r1} & \cdots & \cdots & h_{rk} \end{bmatrix}. \tag{11.9}$$

Элемент этой подматрицы (0 или 1) h_{ij} относится к i-й строке и j-му столбцу ($i = \overline{1,r},\ j = \overline{1,k}$).

Вычисление проверочных символов в соответствии с (11.4):

$$x_{ri} = \sum_{ij}^{rk} h_{ij} \cdot x_k \bmod 2. \tag{11.10}$$

Вычисление синдрома:

$$y_{ri} = \sum_{ij}^{rk} h_{ij} \cdot y_k \bmod 2, \qquad S = y_{ri} \oplus y'_{ri}. \tag{11.11}$$

Пример 6. Имеется информационное слово $X_k = 1001$. Проанализируем использование рассматриваемого кода.

Для начала отмечаем, что $k = 4$. В соответствии с (11.8) подсчитываем длину избыточного слова: $r \geq \log_2(4 + 1) = 3$, тогда $n = k + r = 7$.

Создаем проверочную матрицу $H_{7,4}$:

$$\underbrace{H_{7,4}}_{n \times k} = \left[\begin{array}{cccc|ccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array} \right]. \quad \begin{matrix} \\ \\ \\ \end{matrix}$$

$$\underbrace{\qquad\qquad\qquad}_{A} \quad \underbrace{\qquad\qquad}_{I}$$

Вычисляем проверочные символы, используя (11.10).

В соответствии с этим первый проверочный символ x_{r1} будет равен 1, остальные – нулю:

$$x_{r1} = h_{11} \cdot x_1 \oplus h_{12} \cdot x_2 \oplus \ldots \oplus h_{14} \cdot x_4 = 0 \cdot 1 \oplus 1 \cdot 0 \oplus 1 \cdot 0 \oplus 1 \cdot 1 = 1;$$

$$x_{r2} = h_{21} \cdot x_1 \oplus h_{22} \cdot x_2 \oplus \ldots \oplus h_{24} \cdot x_4 = 1 \cdot 1 \oplus 0 \cdot 0 \oplus 1 \cdot 0 \oplus 1 \cdot 1 = 0;$$

$$x_{r3} = h_{31} \cdot x_1 \oplus h_{32} \cdot x_2 \oplus \ldots \oplus h_{34} \cdot x_4 = 1 \cdot 1 \oplus 1 \cdot 0 \oplus 0 \cdot 0 \oplus 1 \cdot 1 = 0.$$

Таким образом, избыточное слово будет таким: $X_r = 100$, а кодовое слово $X_n = 1001\ 100$.

Рассмотрим ситуацию, когда ошибок в переданной информации нет ($t = 0$), т. е. $X_n = Y_n = 1001\ 100$.

Вычислим новый набор проверочных символов в соответствии с (11.11) и синдром:

$$Y_r' = 100;$$

$$S = Y_r \oplus Y_r' = 100 \oplus 100 = 000 \equiv 0.$$

Нулевой синдром означает безошибочную передачу (или прием) информации.

Рассмотрим ситуацию, когда возникает одиночная ошибка ($t = 1$).

Пусть ошибка произошла в служебных символах $Y_n = 1001\underline{0}00$ (ошибочный символ подчеркнут).

Синдром вычисляем по методике, приведенной для случая отсутствия ошибок. Получаем $S = 100$. Вес синдрома равен 1, и это означает, что произошла ошибка. Местоположение ошибки выявляется анализом (декодированием) синдрома. Декодирование опирается на вышеприведенное соотношение (11.5), в соответствии с которым, принимая во внимание (11.6), можем записать:

$$H \cdot (Y_n)^T = H \cdot (X_n \oplus E)^T = H \cdot (X_n)^T \oplus H \cdot (E)^T = 0 \oplus h_5, \quad (11.12)$$

где h_5 – пятый столбец матрицы, номер которого соответствует номеру ошибочного символа в принятом кодовом слове. Действительно, $h_5 = S = 100$.

В результате декодирования синдрома получается вектор ошибки (*унарный вектор*, имеющий единичный вес): $E = 0000100$. Исправление ошибочного бита достигается простым сложением по модулю два вектора E и кодового слова Y_n:

$$Y_n = E \oplus Y_n = 0000100 \oplus 1001000 = 1001100.$$

Пусть ошибка произошла в бите информационного слова:

$$Y_n = \underline{0}001100.$$

Вычислим дополнительные проверочные символы и синдром:

$$Y_r' = 111;$$

$$S = Y_r \oplus Y_r' = 011.$$

Необходимо убедиться в том, что синдром соответствует первому столбцу используемой проверочной матрицы. Это означает, что декодирование синдрома однозначно укажет на местоположение ошибочного бита:

$E = 1000000$ и $Y_n' = E \oplus Y_n = 0001100 \oplus 1000000 = 1001100 \equiv X_n$.

При возникновении ошибок кратности 2 (например, на позициях l и m) данный код не позволяет *однозначно* идентифицировать ошибки, поскольку с учетом (11.12) имеем:

$$S = h_1 \oplus h_m. \qquad (11.13)$$

Таким образом, код Хемминга с $d_{\min} = 3$ *гарантированно обнаруживает и исправляет* одиночную ошибку в любом разряде кодового слова.

Порядок следования вектор-столбцов в матрице A не имеет значения, однако важно, чтобы на передающей и на принимающей сторонах используемые матрицы были бы абсолютно идентичны.

11.3. Введение в проблему безопасности компьютерных сетей

В компьютерных сетях особую опасность представляют собой атаки на локальную сеть через подключение к сети Интернет для того, чтобы получить доступ к конфиденциальной информации, что связано с недостатками встроенной системы защиты информации в протоколах TCP/IP.

До сих пор не существует единой и общепринятой классификации угроз безопасности компьютерных сетей.

Сетевые атаки столь же разнообразны, как и системы, против которых они направлены. Некоторые атаки отличаются большой сложностью. Другие может осуществить обычный оператор, даже не предполагающий, какие последствия может иметь его деятель-

ность. Для оценки типов атак необходимо знать некоторые ограничения, изначально присущие протоколу TPC/IP.

Ввиду того, что изначально средства защиты для протокола IP не разрабатывались, все его реализации стали дополняться разнообразными сетевыми процедурами, услугами и продуктами, снижающими риски, присущие этому протоколу. Далее будут кратко рассмотрены основные типы атак, обычно применяемых против сетей IP, и перечислены способы борьбы с ними.

Сниффер пакетов (sniffer – в данном случае фильтрация) – прикладная программа, которая использует сетевую карту, работающую в режиме (promiscuous («не делающий различия») mode), в котором все пакеты, полученные по физическим каналам, сетевой адаптер отправляет приложению для обработки.

Сниффер перехватывает все сетевые пакеты, которые передаются через атакуемый домен. В настоящее время снифферы работают в сетях на вполне законном основании. Они используются для диагностики неисправностей и анализа трафика. Однако ввиду того, что некоторые сетевые приложения передают данные в текстовом формате (Telnet, FTP, SMTP, POP3 и т. д.), с помощью сниффера можно узнать полезную, а иногда и конфиденциальную информацию (например, имена пользователей и пароли).

Перехват имен и паролей 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. Таким образом, человек, конечный пользователь, оказывается самым слабым звеном системы информационной безопасности, и хакеры, зная это, умело применяют методы социальной инженерии.

Социальная инженерия – это использование хакером психологических приемов «работы» с пользователем. В самом худшем случае хакер, перехватив пароль, получает доступ к пользовательскому ресурсу на системном уровне и с его помощью создает нового пользователя, которого можно в любой момент использовать для доступа в сеть и к ее ресурсам.

Смягчить угрозу сниффинга пакетов можно с помощью следующих средств.

1. *Аутентификация*. Сильные средства аутентификации являются первым способом защиты от сниффинга пакетов. Под «сильным» понимается такой метод аутентификации, который трудно обойти. Примером такой аутентификации являются *одноразовые пароли* (OTP – One-Time Passwords).

OTP – это технология *двухфакторной аутентификации*. Типичным примером двухфакторной аутентификации является работа обычного банкомата, который опознает клиента, во-первых, по пластиковой карточке и, во-вторых, по вводимому ПИН-коду. Для аутентификации в системе OTP также требуется ПИН-код и личная карточка. Снифферы, перехватывающие другую информацию (например, сообщения электронной почты), не теряют своей эффективности.

2. *Коммутируемая инфраструктура*. Еще одним способом борьбы со сниффингом пакетов в сетевой среде является создание коммутируемой инфраструктуры. Если, к примеру, во всей организации используется коммутируемый Ethernet, хакеры могут получить доступ только к трафику, поступающему на тот порт, к которому они подключены. Коммутируемая инфраструктура не ликвидирует угрозу сниффинга, но заметно снижает ее остроту.

3. *Антиснифферы*. Третий способ борьбы со сниффингом заключается в установке аппаратных или программных средств, распознающих снифферы, работающие в вашей сети. Эти средства не могут полностью ликвидировать угрозу, но, как и многие другие средства сетевой безопасности, включаются в общую систему защиты. Так называемые «антиснифферы» измеряют время реагирования хостов и определяют, не приходится ли хостам обрабатывать «лишний» трафик. Подобного рода средства не могут полностью ликвидировать угрозу сниффинга, но крайне необходимы при построении комплексной системы защиты. Одно из таких средств, поставляемых компанией LOpht Heavy Industries, называется AntiSniff.

3. *Криптография*. Самый эффективный способ борьбы со сниффингом пакетов не предотвращает перехват и не распознает работу снифферов, но делает эту работу бесполезной. Если канал связи является криптографически защищенным, это значит, что хакер перехватывает не сообщение, а зашифрованный текст.

Например, криптография Cisco на сетевом уровне базируется на протоколе *IPSec*. IPSec представляет собой стандартный метод защищенной связи между устройствами с помощью протокола IP. К прочим криптографическим протоколам сетевого управления относятся протоколы *SSH* (Secure Shell) и *SSL* (Secure Socket Layer) (см. подраздел 11.6).

IP-спуфинг – это вид атаки, при которой хакер, находящийся внутри организации или за ее пределами, выдает себя за санкционированного пользователя.

Это можно сделать двумя способами. Во-первых, хакер может воспользоваться IP-адресом, находящимся в пределах диапазона санкционированных IP-адресов, или авторизованным внешним адресом, которому разрешается доступ к определенным сетевым ресурсам. Атаки IP-спуфинга часто являются отправной точкой для прочих атак. Классический пример – атака DoS, которая начинается с чужого адреса, скрывающего истинную личность хакера.

Если же хакеру удается поменять таблицы маршрутизации и направить трафик на ложный IP-адрес, хакер получит все пакеты и сможет отвечать на них так, будто он является санкционированным пользователем.

Полностью устранить угрозу спуфинга практически невозможно, но ее можно ослабить с помощью следующих мер.

1. *Контроль доступа*. Самый простой способ предотвращения IP-спуфинга состоит в правильной настройке управления доступом. Чтобы снизить эффективность IP-спуфинга, необходимо настроить контроль доступа на отсечение любого трафика, поступающего из внешней сети с исходным адресом, который должен располагаться внутри защищаемой сети. Заметим, что это помогает бороться с IP-спуфингом, когда санкционированными являются только внутренние адреса. Если санкционированными являются и некоторые адреса внешней сети, данный метод становится неэффективным.

2. *Фильтрация RFC 2827*. Можно пресечь попытки спуфинга чужих сетей пользователями некоторой сети. Для этого необходимо отбраковывать любой исходящий трафик, исходный адрес которого не является одним из IP-адресов данной организации. В результате отбраковывается весь трафик, который не имеет исходного адреса, ожидаемого на определенном интерфейсе.

3. *Криптография*. Наиболее эффективный метод борьбы с IP-спуфингом тот же, что и в случае со сниффингом пакетов:

необходимо сделать атаку абсолютно неэффективной. IP-спуфинг может функционировать только при условии, что аутентификация происходит на базе IP-адресов.

Отказ в обслуживании (Denial of Service, DoS). Атака DoS делает сеть недоступной для обычного использования за счет превышения допустимых пределов функционирования сети, операционной системы или приложения.

Атаки DoS, без всякого сомнения, являются наиболее известной формой хакерских атак и одной из самых молодых технологий. Против атак такого типа труднее всего создать стопроцентную защиту. Атаки DoS считаются тривиальными, а от хакера для своей организации они требуют минимум знаний и умений: все необходимое программное обеспечение вместе с описаниями самой технологии совершенно свободно доступно в Интернете. Именно простота реализации и огромный причиняемый вред привлекают к DoS пристальное внимание администраторов, отвечающих за сетевую безопасность.

О DoS-атаках широко заговорили после того, как в декабре 1999 года при помощи этой технологии были успешно атакованы web-узлы таких известных корпораций, как Amazon, Yahoo, CNN, eBay и E-Trade.

В случае использования некоторых серверных приложений (таких, например, как Web-сервер или FTP-сервер) атаки DoS могут заключаться в том, чтобы занять все соединения, доступные для этих приложений, и держать их в занятом состоянии, не допуская обслуживания обычных пользователей. В ходе атак DoS могут использоваться обычные Интернет-протоколы, такие как TCP и ICMP (Internet Control Message Protocol). Большинство атак DoS опирается не на программные ошибки или бреши в системе безопасности, а 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. Этот тип атак трудно предотвратить, так как для этого требуется координация действий с провайдером. Когда атака этого типа проводится одновременно через множество устройств, речь идет о распределенной атаке DDoS (Distributed DoS).

Наиболее известными разновидностями атак DoS являются: TCP SYN Flood, Ping of Death, Tribe Flood Network (TFN) и Tribe

Flood Network 2000 (TFN2K), Trinco, Stacheldracht, Trinity, Smurf, ICMP flood, UDP flood, TCP flood.

Рассмотрим некоторые из них более подробно.

Smurf – ping-запросы ICMP (Internet Control Message Protocol) по адресу направленной широковещательной рассылки. Используемый в пакетах этого запроса фальшивый адрес источника в результате оказывается мишенью атаки. Системы, получившие направленный широковещательный ping-запрос, отвечают на него и «затапливают» сеть, в которой находится сервер-мишень.

ICMP flood – атака, аналогичная Smurf, только без усиления, создаваемого запросами по направленному широковещательному адресу.

UDP flood – отправка на адрес системы-мишени множества пакетов UDP, что приводит к «связыванию» сетевых ресурсов.

TCP flood – отправка на адрес системы-мишени множества TCP-пакетов, что также приводит к «связыванию» сетевых ресурсов.

TCP SYN flood – при проведении такого рода атаки выдается большое количество запросов на инициализацию TCP-соединений с узлом-мишенью, которому, в результате, приходится расходовать все свои ресурсы на то, чтобы отслеживать эти частично открытые соединения.

Угроза атак типа DoS может снижаться тремя способами.

1. *Функции антиспуфинга*. Правильная конфигурация функций антиспуфинга на маршрутизаторах и межсетевых экранах помогает снизить риск DoS атак. Эти функции, как минимум, должны включать фильтрацию RFC 2827.

2. *Функции антиDoS*. Правильная конфигурация функций анти-DoS на маршрутизаторах и межсетевых экранах может ограничить эффективность атак. Эти функции часто ограничивают число полуоткрытых каналов в любой момент времени.

3. *Ограничение объема трафика* (traffic rate limiting). Организация может попросить провайдера ограничить объем трафика. Этот тип фильтрации позволяет ограничить объем некритического трафика, проходящего по сети. Обычным примером является ограничение объемов трафика ICMP, который используется только для диагностических целей. Атаки DDoS часто используют ICMP.

Парольные атаки – попытка подбора пароля легального пользователя для входа в сеть.

Хакеры могут проводить парольные атаки с помощью целого ряда методов, таких как *простой перебор* (brute force attack), *троянский конь*, *IP-спуфинг* и *сниффинг пакетов*. Хотя *логин* и *пароль* часто можно получить при помощи IP-спуфинга и сниффинга пакетов, хакеры часто пытаются подобрать пароль и логин, используя для этого многочисленные попытки доступа. Такой подход носит название простого перебора. Часто для такой атаки используется специальная программа, которая пытается получить доступ к ресурсу общего пользования (например к серверу).

Еще одна проблема возникает в случаях, когда пользователи применяют один и тот же пароль для доступа ко многим системам: корпоративной, персональной и системам Интернет.

Парольных атак можно избежать, если не пользоваться паролями в текстовой форме. Одноразовые пароли и/или криптографическая аутентификация могут практически свести на нет угрозу таких атак. К сожалению, не все приложения, хосты и устройства поддерживают указанные выше методы аутентификации.

С точки зрения администратора, существует несколько методов борьбы с подбором паролей. Один из них заключается в использовании средства *LophtCrack*, которое часто применяют хакеры для подбора паролей в среде Windows NT. Это средство быстро показывает, легко ли подобрать пароль, выбранный пользователем.

Атаки типа Man-in-the-Middle – непосредственный доступ к пакетам, передаваемым по сети.

Такой доступ ко всем пакетам, передаваемым 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, для проведения атак типа DoS, искажения передаваемых данных и ввода несанкционированной информации в сетевые сессии.

Эффективно бороться с атаками типа Man-in-the-Middle можно только с помощью криптографии.

Атаки на уровне приложений могут проводиться несколькими способами. Самый распространенный из них состоит в использовании хорошо известных слабостей серверного программного обеспечения (sendmail, HTTP, FTP). Используя эти слабости, хакеры

могут получить доступ к компьютеру от имени пользователя, работающего с приложением (обычно это бывает не простой пользователь, а привилегированный администратор с правами системного доступа). Сведения об атаках на уровне приложений широко публикуются, чтобы дать возможность администраторам исправить проблему с помощью коррекционных модулей (патчей). К сожалению, многие хакеры также имеют доступ к этим сведениям, что позволяет им учиться.

Главная проблема с атаками на уровне приложений состоит в том, что хакеры 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 предоставляет пользователям Web-страницы, межсетевой экран должен предоставлять доступ к этому порту. С точки зрения межсетевого экрана, атака рассматривается как стандартный трафик для порта 80.

Полностью исключить атаки на уровне приложений невозможно. Хакеры постоянно открывают и публикуют в Интернете все новые уязвимые места прикладных программ. Самое главное здесь – хорошее системное администрирование. Вот некоторые меры, которые можно предпринять, чтобы снизить уязвимость для атак этого типа:

– чтение лог-файлов операционных систем и сетевых лог-файлов и/или их анализ с помощью специальных аналитических приложений;

– подписка на услуги по рассылке данных о слабых местах прикладных программ;

– использование последних версий операционных систем и приложений и самых последних коррекционных модулей (патчей);

– кроме системного администрирования необходимо использование *систем распознавания атак* (IDS); существуют две взаимно дополняющие друг друга технологии IDS: первая – *сетевая система IDS* (NIDS), которая отслеживает все пакеты, проходящие через определенный домен; когда система NIDS видит пакет или серию пакетов, совпадающих с сигнатурой известной или вероятной атаки, она генерирует сигнал тревоги и/или прекращает сессию; вторая – *хост-система IDS* (HIDS), защищающая хост с помощью программных агентов; эта система борется только с атаками против одного хоста;

– в своей работе системы IDS пользуются *сигнатурами атак*, которые представляют собой профили конкретных атак или типов атак. Сигнатуры определяют условия, при которых трафик считается хакерским.

Сетевая разведка – 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* (ping sweep) 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.

Полностью избавиться от сетевой разведки невозможно.

Системы IDS на уровне сети и хостов обычно хорошо справляются с задачей уведомления администратора о ведущейся сетевой разведке, что позволяет лучше подготовиться к предстоящей атаке и оповестить провайдера, в сети которого установлена система, проявляющая чрезмерное любопытство.

Злоупотребление доверием – 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. Другим примером является система, установленная с внешней стороны *межсетевого экрана*, имеющая отношения доверия с системой, установленной 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 снизить за счет более жесткого контроля уровней доверия в пределах своей сети. Системы, расположенные с внешней стороны межсетевого экрана, никогда не должны пользоваться абсолютным доверием со стороны защищенных экраном систем. Отношения доверия должны ограничиваться определенными протоколами и, по

возможности, аутентифицироваться не только по IP-адресам, но и по другим параметрам.

Переадресация портов представляет собой разновидность злоупотребления доверием, когда взломанный хост используется для передачи через межсетевой экран трафика, который в противном случае был бы обязательно отбракован.

Представим себе межсетевой экран с тремя интерфейсами, к каждому из которых подключен определенный хост. Внешний хост может подключаться к хосту общего доступа (DMZ), но не к хосту, установленному с внутренней стороны межсетевого экрана. Хост общего доступа может подключаться и к внутреннему, и к внешнему хосту. Если хакер захватит хост общего доступа, он сможет установить на нем программное средство, перенаправляющее трафик с внешнего хоста прямо на внутренний хост. Примером приложения, которое может предоставить такой доступ, является netcat.

Основным способом борьбы с переадресацией портов является использование надежных моделей доверия.

Несанкционированный доступ не может считаться отдельным типом атаки. Большинство сетевых атак проводится ради получения несанкционированного доступа. Источник таких атак может находиться как внутри сети, так и снаружи.

Способы борьбы с несанкционированным доступом достаточно просты. Главным здесь является сокращение или полная ликвидация возможностей хакера получения доступа к системе с помощью несанкционированного протокола. В качестве примера можно рассмотреть недопущение хакерского доступа к порту telnet на сервере, который предоставляет Web-услуги внешним пользователям.

Рабочие станции конечных пользователей очень уязвимы для вирусов (компьютерных) и «троянских коней».

Вирусами называются вредоносные программы, которые внедряются в другие программы для выполнения определенной нежелательной функции на рабочей станции конечного пользователя, способные к самомодификации (мутации).

В качестве примера можно привести вирус, который прописывается в файле command.com (главном интерпретаторе систем Windows) и стирает другие файлы, а также заражает все другие найденные им версии command.com.

Троянский конь – это не программная вставка, а настоящая программа, которая выглядит как полезное приложение, а на деле причиняет вред.

Примером типичного троянского коня является программа, которая выглядит, как простая игра для рабочей станции пользователя. Однако пока пользователь играет в игру, программа отправляет свою копию по электронной почте каждому абоненту, занесенному в адресную книгу этого пользователя. Все абоненты получают по почте игру, вызывая ее дальнейшее распространение.

Борьба с вирусами и троянскими конями ведется с помощью эффективного антивирусного программного обеспечения, работающего на пользовательском уровне и, возможно, на уровне сети.

По мере появления новых вирусов и «троянских коней» организация должна устанавливать новые версии антивирусных средств и приложений.

Почтовая бомбардировка, или **бомбардировка электронной почтой** (mailbombing, мэйлбомбинг) – один из самых старых и примитивных видов интернет-атак. Суть мэйлбомбинга заключается в засорении почтового ящика «мусорной» корреспонденцией или даже выведении из строя почтового сервера интернет-провайдера.

Для этого применяются специальные программы – ***мэйлбомберы***. Они попросту засыпают указанный в качестве мишени почтовый ящик огромным количеством писем, указывая при этом фальшивые данные отправителя – вплоть до IP-адреса. Все, что нужно агрессору, использующему такую программу, указать e-mail объекта атаки, число сообщений, написать текст письма, указать фальшивые данные отправителя, если программа этого не делает сама, и нажать кнопку Отправить.

Подытоживая, отметим, что все многообразие методов и средств противодействия *несанкционированному доступу* условно можно разделить на следующие четыре группы.

1. *Организационные методы и средства* подразумевают разработку и исполнение в любой организации/лаборатории правил, регламентирующих и регулирующих доступ физических лиц к информации, хранящейся на носителях либо передаваемой внутри сети данного предприятия. В организациях, осуществляющих операции над критической информацией (правительственные, государственные, банковские, коммерческие и иные структуры), на-

значается специальное ответственное лицо – *администратор безопасности*, ответственный за реализацию и соблюдение правил на основе реализуемой политики безопасности.

2. *Правовые методы*. Гражданский правовой кодекс предусматривает наказание за компьютерные преступления. В 1983 году Организация экономического сотрудничества и развития определила под термином «*компьютерная преступность*» (или «связанная с компьютерами преступность») любые незаконные, неэтичные или неправомерные действия, связанные с автоматической обработкой или передачей информации. Практически во всех странах с развитой информационной инфраструктурой (в том числе и в Беларуси) предусматривается уголовно-правовая защита от компьютерных преступлений.

3. *Физические методы* объединяют методы ограничения *физического доступа* лиц к каналам передачи информации, устройствам ее хранения и обработки. Основаны на использовании простых замков, магнитных карт, чипов, таблеток, на анализе антропометрических и биологических параметров человека (сетчатка глаза, отпечатки пальцев и др.).

4. *Программно-технические методы* базируются на применении аппаратных и/или программных средств, позволяющих идентифицировать пользователя (либо техническое средство), а также оценить происхождение программного средства, поступающего в информационную сеть. Наиболее известным из указанных средств является использование пароля, антивирусных программ, *брандмауэров*, или «огненных стен» (*firewalls*), на входе сети, криптографического преобразования информации на основе методов шифрования.

Кроме того, при рассмотрении вопроса обеспечения безопасности компьютерных сетей часто возникает вопрос о том, к какому уровню стека протоколов относится система сетевой безопасности. Ответ является очевидным.

На каждом из уровней протоколов могут осуществляться мероприятия по защите компьютерной сети, но каждый из этих уровней, что вполне естественно, использует свои специфические методы.

На уровне передачи данных пакеты, передаваемые по двухточечной линии, могут кодироваться при передаче в линию и декодироваться при приеме. Все детали этих преобразований могут

быть известны только уровню передачи данных, причем более высокие уровни могут даже не догадываться о том, что происходит. Такой метод защиты называется *шифрованием в канале связи*. На сетевом уровне могут быть установлены брэндмауэры, позволяющие отвергать подозрительные пакеты. На этом же уровне может быть использована IP-защита. На транспортном уровне можно зашифровать соединения целиком, от одного конца до другого, поскольку максимальную защиту может обеспечить только сквозное шифрование. Проблемы аутентификации и обеспечения строгого выполнения обязательств могут решаться только на прикладном уровне.

На всех уровнях стека протоколов, за исключением физического, решение проблем защиты информации базируется на принципах криптографии.

11.4. Принципы криптографической защиты информации

Ранее было отмечено, что последний и практически непреодолимый «рубеж» защиты от несанкционированного доступа в компьютерных системах и в том числе в компьютерных сетях образует шифрование.

Шифрование данных представляет собой разновидность программных средств защиты информации и имеет особое значение на практике как единственная надежная защита информации, передаваемой по протяженным последовательным линиям, от утечки. Понятие «шифрование» часто употребляется в связи с понятием «криптография».

Криптография изучает методы преобразования информации, обеспечивающие ее конфиденциальность и аутентичность.

Аутентичность информации состоит в подлинности авторства и целостности.

В проблематике современной криптографии можно выделить следующие три типа основных задач:

- обеспечение конфиденциальности;
- создание условий для анонимности (неотслеживаемости);
- обеспечение аутентификации информации и источника сообщения.

Первый тип задач относится к защите информации от несанкционированного доступа по секретному ключу. Доступ к информации (информационным ресурсам) имеют только обладатели ключа. Второй и третий типы задач обязаны своей постановкой массовому применению электронных способов обработки и передачи информации (банковская сфера, электронная коммерция, каналы межличностной коммуникации и др.).

Криптографическое преобразование состоит из двух этапов: прямого и обратного. Прямое преобразование называют *зашифрованием* (в соответствии со стандартом ISO 7492-2, *шифрованием*, *encrypt*), обратное – *расшифрованием* (*дешифрованием*, *decrypt*).

С точки зрения криптографии **шифр**, или **криптографическая система** – совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, задаваемых *ключом* и *алгоритмом криптографического преобразования*.

Следует различать понятия *ключ* и *пароль*.

Пароль является секретной последовательностью букв алфавита, однако используется не для шифрования (как ключ), а для аутентификации субъектов.

В *симметричных криптосистемах* для зашифрования и для расшифрования используется один и тот же ключ.

В *ассиметричных криптосистемах* используются два ключа – открытый (публичный) и закрытый (секретный, тайный), которые математически связаны друг с другом.

Электронной цифровой подписью называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и целостность сообщения.

Криптостойкостью называется характеристика шифра, определяющая его стойкость к расшифрованию без знания ключа, т. е. к криптоатаке.

Удачную *криптоатаку* называют **взломом**.

11.4.1. Симметричные криптосистемы

Стандартные методы шифрования информации, передаваемой по сетям для повышения степени устойчивости к несанкционированному использованию, реализуют несколько этапов (шагов)

шифрования, на каждом из которых используются различные «классические» методы шифрования.

К числу известных *симметричных криптосистем* можно отнести стандарт шифрования США DES, алгоритм IDEA, отечественный ГОСТ 28147-89 и др.

Достаточно надежным считается алгоритм *IDEA* (International Data Encryption Algorithm), разработанный в Швейцарии и считающийся блочным шифром. Алгоритм также оперирует 64-битовыми блоками открытого текста. Несомненным достоинством IDEA является то, что его ключ имеет длину 128 бит. Один и тот же алгоритм используется и для зашифрования, и для расшифрования.

В алгоритме IDEA используются следующие математические операции:

– поразрядное сложение по модулю 2 («исключающее ИЛИ»);

– сложение беззнаковых целых по модулю 216 (модуль 65536);

– умножение целых по модулю (216 + 1) (модуль 65537), рассматриваемых как беззнаковые целые, за исключением того, что блок из 16 нулей рассматривается как 2^{16}.

Все перечисленные операции выполняются над 16-битовыми субблоками. Комбинирование этих операций обеспечивает комплексное преобразование входа, существенно затрудняя криптоанализ IDEA по сравнению с DES, который базируется исключительно на операции «исключающее ИЛИ».

К достоинствам симметричных методов шифрования относится высокая скорость шифрования и дешифрования, к недостаткам – малая степень защиты в случае, если ключ стал доступен третьему лицу.

11.4.2. Ассиметричные криптосистемы

Криптосистема с открытым ключом определяется тремя алгоритмами: *генерации ключей*, *зашифрования* и *расшифрования*. Алгоритм генерации ключей открыт, и каждый может дать ему на вход строку надлежащей длины и получить пару ключей.

Рассмотрим ассиметричные криптосистемы на примере *алгоритма RSA*. Названный в честь трех изобретателей Рона Ривеста (Ron Rivest), Ади Шамира (Adi Shamir) и Леонарда Адлемана (Leonard Adleman), этот алгоритм многие годы противостоит многочисленным попыткам криптоаналитического вскрытия.

Безопасность алгоритма основана на трудоемкости разложения на множители больших чисел. Открытый и закрытый ключи являются функциями двух больших простых чисел разрядностью 100–200 десятичных цифр. Предполагается, что *восстановление открытого текста по шифртексту и открытому ключу равносильно разложению числа на два больших простых множителя*.

Ключ состоит из тройки больших целых чисел: e, *d*, *n*. Пара чисел (*e* и *n*) является не секретной и образует *публичный* (*открытый*) *ключ*. Число *d* является секретным, и пара (*d* и *n*) образует *тайный ключ*, известный только данному пользователю. Проблема верификации пользователей на основе их открытых ключей является одной из важных.

Основные операции алгоритма

1. Для генерации двух ключей применяются два больших случайных простых числа: *p* и *q*. Для большей крипростойкости алгоритма эти числа должны иметь равную длину.

2. Рассчитывается произведение $n = p \cdot q$, и вычисляется функция $\varphi(n) = (p - 1) \cdot (q - 1)$, которая называется функцией Эйлера и указывает количество положительных целых чисел в интервале от 1 до *N*, которые взаимно просты с *N*.

3. Случайным образом выбирается число *e* такое, что *e* и $\varphi(n)$ являются взаимно простыми числами.

4. С помощью расширенного алгоритма Евклида вычисляется число *d*, такое, что $e \cdot d = 1 \bmod \varphi(n)$, другими словами

$$d = e^{-1} \bmod \varphi(n).$$

Подразумевается, что эти шаги выполняет лицо, которое генерирует для себя (или по просьбе другого лица для этого другого лица) соответствующие ключи.

Отметим, что числа *d* и *n* также являются взаимно простыми. Открытый и закрытый ключи составляют вышеуказанные пары чисел: *e* и *n*, *d* и *n* соответственно.

Зашифрование сообщения $M = m_1 m_2 \ldots m_k$ (сообщение делится на *k* блоков) выглядит просто:

$$c_i = (m_i)^e \bmod n.$$

При расшифровании каждого блока m_i сообщения *C* производится следующая операция:

$$m_i = (c_i)^d \bmod n.$$

Точно так же сообщение может быть зашифровано с помощью пары d и n и расшифровано с помощью чисел e и n. Именно такой подход используется в системах электронной цифровой подписи.

Пример 7. Пусть сообщение M представляется числом 688232. Предполагаем, что длина ключа составляет три десятичных цифры. Проиллюстрируем использование алгоритма RSA для передачи зашифрованного сообщения.

Выбираем числа $p = 47$ и $q = 71$.

Имеем $n = p \cdot q = 47 \cdot 71 = 3337$.

Вычисляем $\varphi(n) = (p - 1) \cdot (q - 1) = 46 \cdot 70 = 3220$.

Число e не должно иметь общих сомножителей с числом 3220; выбираем (случайным образом) e, равным 79.

Вычисляем d: $d = 79^{-1} \bmod 3220 = 1019$.

Имеем открытый ключ – числа 79 и 3337 (его можно разместить в общедоступных источниках) и закрытый ключ – числа 1019 и 3337 (как видим, секретным является только число d; в нашем случае – это число 1019).

Для зашифрования сообщения M разбиваем его на блоки длиной, равной длине ключа, т. е. по 3 символа: $m_1 = 688$, $m_2 = 232$. Первый блок шифруется как $688^{79} \bmod 3337 = 1570 = c_1$; второй блок – $232^{79} \bmod 3337 = 2756 = c_2$.

Шифртекст C сообщения M выглядит следующим образом: $C = 1570\ 2756$. Для обратного преобразования нужно выполнить похожие операции, однако, с использованием числа 1019 в качестве степени:

$$m_1 = 1570^{1019} \bmod 3337 = 688;$$

$$m_2 = 2756^{1019} \bmod 3337 = 232.$$

Несимметричные методы шифрования имеют преимущества и недостатки, противоположные тем, которыми обладают *симметричные методы*. В отличие от *симметричных методов шифрования*, проблема рассылки ключей в *несимметричных методах* решается проще – пары ключей (открытый и закрытый) генерируются «на месте» с помощью специальных программ. Для рассылки открытых ключей используются такие технологии, как *LDAP* (Light-weight Directory Access Protocol, протокол облегченного доступа к справочнику). Рассылаемые ключи могут быть предварительно зашифрованы с помощью одного из *симметричных методов шифрования*.

Отметим также, что помимо выбора подходящей для конкретной информации системы средств криптографической защиты информации, важной проблемой является *управление ключами*. Как бы ни была сложна и надежна сама криптосистема, она основана на использовании ключей.

Управление ключами – информационный процесс, включающий в себя три элемента:

- генерацию ключей;
- накопление ключей;
- распределение ключей.

Для получения надежных криптографических ключей используются специальные аппаратные и программные методы **генерации случайных значений ключей**.

Как правило, применяют *датчики псевдослучайных чисел* (ПСЧ). Однако степень случайности генерации чисел должна быть достаточно высокой. Идеальными генераторами являются устройства на основе «натуральных» случайных процессоров, например, на основе *белого радиошума*.

Под **накоплением ключей** понимается организация их хранения, учета и удаления. Поскольку ключ является самым привлекательным для злоумышленника объектом, открывающим ему путь к конфиденциальной информации, то вопросам накопления ключей следует уделять особое внимание. *Секретные ключи никогда не должны записываться в явном виде на носителе, который может быть считан или скопирован*. Таким образом, вся информация о ключах должна храниться в зашифрованном виде. Ключи, зашифровывающие ключевую информацию, называются *мастер-ключами*.

Распределение ключей – самый ответственный процесс в управлении ключами. К нему предъявляются следующие требования: оперативность и точность распределения, скрытность распределяемых ключей.

Распределение ключей между пользователями компьютерной сети реализуется двумя способами:

- использованием одного или нескольких центров распределения ключей;
- прямым обменом сеансовыми ключами между пользователями сети.

Задача распределения ключей сводится к построению протокола распределения ключей, обеспечивающего:

− взаимное подтверждение подлинности участников сеанса;

− подтверждение достоверности сеанса механизмом запроса-ответа или отметки времени;

− использование минимального числа сообщений при обмене ключами;

− возможность исключения злоупотреблений со стороны центра распределения ключей.

Рассмотрим в качестве примера протокол аутентификации и распределения ключей *Kerberos* (Цербер). Протокол Kerberos спроектирован для работы в сетях TCP/IP и предполагает участие в аутентификации и распределении ключей третьей доверенной стороны. Kerberos обеспечивает надежную аутентификацию в сети, разрешая законному пользователю доступ к различным машинам в сети. Протокол основывается на симметричной криптографии (реализован алгоритм DES, хотя возможно применение и других симметричных криптоалгоритомв). Kerberos разделяет отдельный секретный ключ с каждым субъектом сети. Знание такого секретного ключа равносильно доказательству подлинности субъекта сети.

Основной протокол Kerberos является вариантом протокола аутентификации и распределения ключей Нидхема – Шрёдера.

В основном протоколе Kerberos (версия 5) участвуют две взаимодействующие стороны A и B и доверенный сервер KS (Kerberos Server). Стороны A и B, каждая по отдельности, разделяют свой секретный ключ с сервером KS. Доверенный сервер KS выполняет роль *центра распределения ключей* (*ЦРК*).

Пусть сторона A хочет получить сеансовый ключ для информационного обмена со стороной B.

Сторона A инициирует фазу распределения ключей, посылая по сети серверу KS идентификаторы участников сеанса Id_A и Id_B: $A \rightarrow KS$: Id_A, Id_B. Сервер KS генерирует сообщение с временной отметкой T, сроком действия L, случайным сеансовым ключом K и идентификатором Id_A. Он шифрует это сообщение секретным ключом, который разделяет со стороной B.

Затем сервер KS берет временную отметку T, срок действия L, сеансовый ключ K, идентификатор Id_B стороны B и шифрует все это секретным ключом, который разделяет со стороной A. Оба эти зашифрованные сообщения он отправляет стороне A: $KS \rightarrow A$: $E_A(T, L, K, Id_B)$, $E_B(T, L, K, Id_A)$.

Сторона A расшифровывает первое сообщение своим секретным ключом, проверяет отметку времени T, чтобы убедиться, что это сообщение не является повторением предыдущей процедуры распределения ключей.

Затем сторона A генерирует сообщение со своим идентификатором Id_A и отметкой времени T, шифрует его сеансовым ключом K и отправляет стороне B. Кроме того, A отправляет для B сообщение от KS, зашифрованное ключом стороны B: $A \rightarrow B$: $E_K(Id_A, T)$, $E_B(T, L, K, Id_A)$.

Только сторона B может расшифровать сообщения. Сторона B получает отметку времени T, срок действия L, сеансовый ключ K, идентификатор Id_A. Затем сторона B расшифровывает сеансовым ключом K вторую часть сообщения. Совпадение значений T и Id_A в двух частях сообщения подтверждает подлинность A по отношению к B.

Для взаимного подтверждения подлинности сторона B создает сообщение, состоящее из отметки времени T плюс 1, шифрует его ключом K и отправляет стороне A: $B \rightarrow A$: $E_K(T+1)$.

Если после расшифрования сообщения сторона A получает ожидаемый результат, то она знает, что на другом конце линии связи находится действительно B.

Этот протокол успешно работает, если часы каждого участника синхронизированы с часами сервера KS. В этом протоколе необходим обмен с KS для получения сеансового ключа каждый раз, когда A желает установить связь с B. Протокол обеспечивает надежное соединение абонентов A и B при условии, что ни один из ключей не скомпрометирован и сервер KS защищен.

Система Kerberos обеспечивает защиту сети от несанкционированного доступа, базируясь исключительно на программных реализациях, и предполагает многократное шифрование передаваемой по сети управляющей информации.

Система Kerberos имеет структуру типа клиент – сервер и состоит из клиентских частей C, установленных на все машины сети и Kerberos-сервера (KS), располагающегося на каком-либо компьютере.

Область действия системы Kerberos распространяется на тот участок сети, все пользователи которого зарегистрированы под своими именами и паролями в базе данных Kerberos-сервера.

11.5. Эффективность использования пароля для защиты информации

Наиболее часто применяемыми методами идентификации и аутентификации пользователей являются методы, основанные на использовании паролей.

Пароль представляет собой некоторую последовательность символов, сохраняемую в секрете и предъявляемую при обращении к компьютерной системе.

Для ввода пароля, как правило, используется штатная клавиатура компьютерных систем (КС); при этом в процессе ввода пароль не должен отображаться на экране монитора, а чтобы пользователь мог ориентироваться в количестве введенных символов, на экран выдаются специальные символы.

При составлении и хранении пароля пользователи должны придерживаться следующих рекомендаций:

– пароль должен запоминаться субъектом доступа;

– запись пароля (на бумажном или электронном носителе) значительно повышает вероятность его компрометации (нарушения конфиденциальности);

– легко запоминаемый пароль должен быть в то же время сложным для отгадывания; не рекомендуется использовать для этой цели имена, фамилии, даты рождения и т. п.;

– желательным является наличие в пароле парадоксального сочетания букв, слов и т. п., полученного, например, путем набора русских букв пароля на латинском регистре.

Вероятность подбора пароля уменьшается также при увеличении его длины и времени задержки между разрешенными попытками повторного ввода неправильно введенного пароля. Ожидаемое время раскрытия пароля T_P можно вычислить по следующей приближенной формуле:

$$T_P = \frac{A^S \cdot t}{2}, \qquad (11.13)$$

где A – число символов в алфавите, из которых составляется пароль (например, 26 символов латинского алфавита); S – длина пароля; $t = E / R$ – время, необходимое на попытку введения пароля; E – число символов в сообщении, передаваемом в систему при попытке получить к ней доступ (включая пароль

и служебные символы); R – скорость передачи символов пароля (симв./мин).

В приведенной формуле считается, что злоумышленник имеет возможность непрерывно осуществлять подбор пароля. Например, если $A = 26$, $t = 2$ с и $S = 6$ символов, то ожидаемое время раскрытия T_P пароля приблизительно равно одному году. Если в данном примере после каждой неудачной попытки ввода пароля предусмотреть временную задержку в 10 с, то ожидаемое время раскрытия пароля увеличится в 5 раз.

Следует также отметить, что на безопасное время раскрытия пароля оказывает существенное влияние длина пароля S (в степенной зависимости). Так, если для трехсимвольного пароля, выбранного из 26-символьного алфавита, время T_P составит 3 мес., то для 4-символьного – 65 лет.

Выбор необходимой длины пароля S можно производить исходя из заданной вероятности P того, что данный пароль может быть раскрыт посторонним лицом за время M. Если необходимо построить систему, где незаконный пользователь имел бы вероятность отгадывания правильного пароля не большую, чем заданная вероятность P, то следует выбрать такое значение S, которое удовлетворяло бы *формуле Андерсена*:

$$A^S \geq (4{,}32 \cdot 10^4 \cdot R \cdot M) / (E \cdot P), \qquad (11.14)$$

где M – период времени, в течение которого предпринимаются попытки раскрытия пароля (в месяцах при ежедневном 24-часовом тестировании).

Пример 8. Допустим, требуется, используя стандартный латинский алфавит, установить пароль такой длины, чтобы вероятность его отгадывания не превысила 0,001 после трехмесячного систематического тестирования. Если за одну попытку доступа посылается 20 символов ($E = 20$), а скорость их передачи $R = 600$ симв./мин, то по формуле Андерсена получаем:

$$(4{,}32 \cdot 10^4 \cdot R \cdot M) / (E \cdot P) = (4{,}32 \cdot 10^4 \cdot 3 \cdot 10^3 \cdot 600) / 20 = 3{,}888 \cdot 10^9.$$

Для $S = 6$: $26^S = 3{,}089 \cdot 10^8$, т. е. $< 3{,}888 \cdot 10^9$.

Для $S = 7$: $26^S = 8{,}03 \cdot 10^9$, т. е. $> 3{,}888 \cdot 10^9$.

Таким образом, при данных обстоятельствах следует выбрать длину пароля $S = 7$.

При существенном увеличении длины пароля он может быть разбит на две части: запоминаемую пользователем и вводимую

вручную, а также размещенную в зашифрованном виде на специальном носителе (например, дискете, магнитной карте и т. д.) и считываемую специальным устройством.

Повышение стойкости системы защиты на этапе аутентификации можно достигнуть и увеличением числа символов алфавита, используемого при вводе пароля. Для этого при наборе символов пароля можно использовать несколько регистров клавиатуры, соответствующих, например, строчным и прописным латинским символам, а также строчным и прописным символам кириллицы.

На степень информационной безопасности при использовании простого парольного метода проверки подлинности пользователей большое влияние оказывают ограничения на минимальное и максимальное время действия каждого пароля. Чем чаще меняется пароль, тем более высокий уровень безопасности обеспечивается. Администратор службы безопасности должен постоянно контролировать своевременность смены паролей пользователей.

Таким образом, для повышения надежности аутентификации пользователей следует, по возможности, использовать нетривиальные (уникальные) пароли и, кроме того, обеспечивать более частую их смену.

С этой точки зрения являются достаточно эффективными методы, основанные на использовании динамически изменяющихся паролей. При смене пароля осуществляется его функциональное преобразование, зависящее от динамически изменяющихся параметров, например, суточного времени в часах, номера дня недели, месячной даты и т. д. Такая смена пароля производится либо периодически (ежедневно, каждые три дня или каждую неделю), либо при очередном обращении пользователя.

11.6. Методы и средства защиты от удаленных атак через сеть Интернет

Межсетевые экраны (синоним – брэндмауэр, firewall) способны решать ряд задач по отражению наиболее вероятных угроз для внутренних сетей.

Межсетевой экран призван обеспечить безопасный доступ к внешней сети и ограничить доступ внешних пользователей к внутренней сети.

Таким образом, **межсетевой экран** (МЭ) – система межсетевой защиты, позволяющая разделить сеть на две части или более и реализовать набор правил, определяющих условия прохождения пакетов с данными через границу из одной общей части сети в другую.

МЭ пропускает через себя весь трафик, принимая для каждого проходящего пакета решение – пропускать его или отбросить. Для того чтобы МЭ мог осуществить это, ему необходимо определить набор правил фильтрации.

Однако следует отметить, что ни один межсетевой экран не может гарантировать полной защиты внутренней сети при всех возможных обстоятельствах.

Основными компонентами межсетевых экранов являются: *фильтрующие маршрутизаторы*, *шлюзы сетевого уровня* и *шлюзы прикладного уровня*.

Фильтрующий маршрутизатор представляет собой маршрутизатор или работающую на сервере программу. Сконфигурирован таким образом, чтобы фильтровать входящие и исходящие пакеты.

Фильтрация пакетов осуществляется на основе информации, содержащейся в TCP- и IP-заголовках пакетов. Фильтрующий маршрутизатор обычно может фильтровать IP-пакеты на основе группы следующих полей заголовка пакета: IP-адрес отправителя, IP-адрес получателя, порт отправителя, порт получателя.

Шлюз сетевого уровня иногда называют системой трансляции сетевых адресов или шлюзом сеансового уровня модели OSI. Такой шлюз исключает прямое взаимодействие между *авторизованным клиентом* и *внешним хост-компьютером*.

Шлюз сетевого уровня принимает запрос доверенного клиента на конкретные услуги и после проверки допустимости запрошенного сеанса устанавливает соединение с внешним хост-компьютером. После этого шлюз копирует пакеты в обоих направлениях, не осуществляя их фильтрации.

Для устранения ряда недостатков, присущих фильтрующим маршрутизаторам, межсетевые экраны должны использовать дополнительные программные средства для фильтрации сообщений сервисов типа TELNET и FTP. Такие программные средства называются *полномочными серверами* (серверами-посредниками), а хост-компьютер, на котором они выполняются, – шлюзом прикладного уровня.

Шлюз прикладного уровня исключает прямое взаимодействие между авторизованным клиентом и внешним хост-компьютером.

Шлюз фильтрует все исходящие и входящие пакеты на прикладном уровне. Связанные с приложениями серверы-посредники перенаправляют через шлюз информацию, генерируемую конкретными серверами.

Для достижения более высокого уровня безопасности и гибкости шлюзы прикладного уровня могут быть объединены с фильтрующими маршрутизаторами в одном межсетевом экране.

К *программным методам защиты* в сети Интернет могут быть отнесены защищенные криптопротоколы, которые позволяют надежно защищать соединения. К основным на сегодняшний день подходам и протоколам, обеспечивающим защиту соединений, относятся SKIP-технология и протокол защиты соединения SSL.

SKIP-технология (Secure Key Internet Protocol) – стандарт защиты трафика IP-пакетов, позволяющий на сетевом уровне обеспечить защиту соединения и передаваемых данных.

Возможны два способа реализации SKIP-защиты трафика IP-пакетов:

– шифрование блока данных IP-пакета;

– инкапсуляция IP-пакета в SKIP-пакет.

SKIP-пакет похож на обычный IP-пакет. В поле данных SKIP-пакета полностью размещается в зашифрованном виде исходный IP-пакет. В этом случае в новом заголовке вместо истинных адресов могут быть помещены некоторые другие адреса. Такая структура SKIP-пакета позволяет беспрепятственно направлять его любому хост-компьютеру в сети Интернет, при этом межсетевая адресация осуществляется по обычному IP-заголовку в SKIP-пакете. Конечный получатель SKIP-пакета по заранее определенному разработчиками алгоритму расшифровывает криптограмму и формирует обычный TCP- или UDP-пакет, который и передает соответствующему модулю (TCP или UDP) ядра операционной системы.

SSL (Secure Sockets Layer, протокол защищенных сокетов) создает защищенное соединение между двумя сокетами, позволяющее: клиенту и серверу договориться об используемых параметрах; клиенту и серверу произвести взаимную аутентификацию; организовать тайное общение; обеспечить защиту целостности данных.

Идея SSL заключается в том, что, по сути дела, между прикладным и транспортным уровнями появляется новый уровень, принимающий запросы от браузера и отсылающий их по TCP для передачи серверу. После установки защищенного соединения основная задача SSL заключается в поддержке сжатия и шифрования. Если поверх

SSL используется http, то этот вариант называется HTTPS (Secure http, защищенный HTTP), несмотря на то, что это обычный HTTP.

Существует несколько версий протокола SSL. SSL состоит из двух субпротоколов, один из которых предназначен для установления защищенного соединения, а второй – для использования этого соединения.

Протокол SSL является действительно универсальным средством, позволяющим динамически защищать соединение при использовании любого прикладного протокола (FTP, TELNET, SMTP, DNS и т. д.).

К специализированным программным средствам защиты информации от несанкционированного доступа в компьютерных сетях относятся и так называемые **proxy-серверы** (proxy-servers, proxy – доверенное лицо, доверенность).

Идея использования proxy-сервера заключается в том, что весь трафик сетевого/транспортного уровней между локальной и глобальной сетями запрещается полностью – маршрутизация как таковая отсутствует, а обращения из локальной сети в глобальную происходят через специальные серверы-посредники.

Следует отметить, что, несмотря на все преимущества, этот метод не дает достаточной защиты против атак на более высоких уровнях – например, на уровне приложения (вирусы, код Java и JavaScript).

Не следует забывать также и о том, что встроенные средства защиты информации имеются также в сетевых операционных системах. Однако они не всегда могут полностью решить возникающие на практике проблемы.

В качестве примера рассмотрим некоторые из названных систем.

Система **SFT** (System Fault Tolerance – система устойчивости к отказам) компании Novell включает три основных уровня.

1. Первый уровень (SFT Level I) предусматривает, в частности, создание дополнительных копий FAT и Directory Entries Tables, немедленную верификацию каждого вновь записанного на файловый сервер блока данных, а также резервирование на каждом жестком диске около 2% от объема диска. При обнаружении сбоя данные перенаправляются в зарезервированную область диска, а сбойный блок помечается как «плохой» и в дальнейшем не используется.

2. Второй уровень (SFT Level II) содержит дополнительные возможности создания «зеркальных» дисков, а также дублирования дисковых контроллеров, источников питания и интерфейсных кабелей.

3. Третий уровень (SFT Level III) позволяет применять в локальной сети дублированные серверы, один из которых является «главным», а второй, содержащий копию всей информации, вступает в работу в случае выхода «главного» сервера из строя.

Система контроля и ограничения прав доступа в сетях NetWare (защита от несанкционированного доступа) также содержит несколько уровней:

– *уровень начального доступа* (включает имя и пароль пользователя, систему учетных ограничений, таких как явное разрешение или запрещение работы, допустимое время работы в сети, место на жестком диске, занимаемое личными файлами данного пользователя, и т. д.);

– *уровень прав пользователей* (ограничения на выполнение отдельных операций и/или на работу данного пользователя, как члена подразделения, в определенных частях файловой системы сети);

– *уровень атрибутов каталогов и файлов* (ограничения на выполнение отдельных операций, в том числе удаления, редактирования или создания, идущие со стороны файловой системы и касающиеся всех пользователей, пытающихся работать с данными каталогами или файлами);

– *уровень консоли файл-сервера* (блокирование клавиатуры файл-сервера на время отсутствия сетевого администратора до ввода им специального пароля).

Однако полагаться на эту часть системы защиты информации в ОС NetWare можно не всегда. Свидетельством тому являются многочисленные инструкции в Интернете и готовые доступные программы, позволяющие взломать те или иные элементы защиты от несанкционированного доступа.

То же замечание справедливо по отношению к более поздним версиям ОС NetWare (вплоть до последней 6-й версии) и к другим «мощным» сетевым ОС со встроенными средствами защиты информации (Windows NT, UNIX). В связи с остротой проблемы защиты информации наблюдается тенденция интеграции (встраивания) отдельных, хорошо зарекомендовавших себя и ставших стандартными средств в сетевые ОС, также разработка собственных «фирменных» аналогов известным программам защиты информации. Так, в сетевой ОС NetWare 4.1 предусмотрена возможность кодирования данных по принципу «открытого ключа» (алгоритм RSA) с формированием электронной подписи для передаваемых по сети пакетов.

ВЫВОДЫ

1. Вопросы безопасности компьютерных сетей затрагивают широкий спектр вопросов, касающихся надежной передачи информации, обеспечения конфиденциальности информации, защиты от различных атак с целью повреждения или хищения информации.

2. Для проверки целостности информации, а также исправления ошибок в сетях используют методы помехоустойчивого кодирования, базирующиеся на введении в информацию дополнительных избыточных символов. В зависимости от принципа вычисления дополнительных символов и их числа реализуются различные алгоритмы помехоустойчивого кодирования.

3. Криптография представляет собой инструмент, используемый для обеспечения конфиденциальности информации и аутентичности.

4. Все алгоритмы шифрования можно разделить на 2 вида: с симметричными закрытыми ключами и с открытыми ключами (ассиметричными). Алгоритмы с симметричными ключами искажают при шифровании значения битов последовательности итераций, параметризованных ключом. Наиболее популярные алгоритмы этого типа – DES и AES. Алгоритмы с симметричным ключом могут работать в режиме электронного шифроблокнота, потокового шифра.

5. Алгоритмы с открытым ключом отличаются тем, что для шифрования и дешифрации используют разные ключи, причем ключ дешифрации невозможно вычислить по ключу шифрования. Эти свойства позволяют делать ключ открытым. Чаще всего применяется алгоритм RSA, основанный на сложности разложения больших чисел на простые сомножители.

6. Для противодействия различным атакам в сетях в основном используются межсетевые экраны и proxy-серверы, а также криптозащищенные протоколы (технология SKIP, протокол SSL).

7. Межсетевой экран – это система межсетевой зашиты, позволяющая разделить сеть на две части или более и реализовать набор правил, определяющих условия прохождения пакетов с данными через границу из одной общей части сети в другую. Мэжсетевые экраны пропускают через себя весь трафик, принимая для каждого проходящего пакета решение – пропускать его или отбросить.

8. Идея использования proxy-сервера заключается в том, что весь трафик сетевого/транспортного уровней между локальной

и глобальной сетями запрещается полностью – маршрутизация как таковая отсутствует, а обращения из локальной сети в глобальную происходят через специальные серверы-посредники. Очевидно, что при этом обращения из глобальной сети в локальную становятся невозможными в принципе.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Дайте определения информации и защиты информации.
2. Дайте определение компьютерной безопасности.
3. Поясните суть методов помехоустойчивого кодирования.
4. Изобразите обобщенную структурную схему системы передачи информации с использованием помехоустойчивого кодирования данных. Поясните назначение и особенности элементов системы.
5. Как рассчитывается количество избыточных символов кодового слова? Приведите примеры.
6. Что такое проверочная матрица? Как она строится и каким условиям должна соответствовать?
7. Постройте проверочную матрицу кода Хемминга для $k = 4$.
8. Дайте понятие синдрома и поясните его суть на примере.
9. Опишите сниффинг как метод атаки.
10. Перечислите методы защиты от сниффинга пакетов.
11. Что такое IP-спуффинг?
12. Опишите методы снижения угроз IP-спуффинга.
13. Опишите понятие DoS-атаки. В чем ее сущность?
14. Приведите разновидности DoS-атак.
15. Поясните суть парольных атак.
16. Приведите классификацию средств противодействия несанкционированному доступу.
17. Каковы принципы криптографической защиты информации?
18. Что такое симметричные криптосистемы?
19. Что такое ассиметричные криптосистемы?
20. Приведите оценку эффективности использования пароля.
21. Опишите принцип дествия технологии SKIP.
22. В чем заключается суть прокола SSL?
23. Что такое proxy-сервер?
24. Опишите принципы функционирования межсетевых экранов.

ЛИТЕРАТУРА

1. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы: учебник / В. Г. Олифер, Н. А. Олифер. – 2-е изд. – СПб.: Питер, 2004.

2. Танненбаум, Э. Компьютерные сети / Э. Танненбаум. – СПб.: Питер, 2002.

3. Олифер, В. Г. Сетевые операционные системы / В. Г. Олифер, Н. А. Олифер. – СПб.: Питер, 2001.

4. Олифер, В. Г. Новые технологии и оборудование IP-сетей / В. Г. Олифер, Н. А. Олифер. – СПб.: БВХ-Санкт-Петербург, 2000.

5. Дженнингс, Ф. Практическая передача данных: модемы, сети и протоколы: пер. с англ. / Ф. Дженнингс. – М.: Мир, 1989.

6. Кульгин, М. В. Коммутация и маршрутизация IP/IPX трафика. АйТи / М. В. Кульгин. – М.: Компьютер-пресс, 1998.

7. Кульгин, М. В. Компьютерные сети. Практика построения. Для профессионалов / М. В. Кульгин. – 2-е изд. – СПб.: Питер, 2003.

8. Семенов, А. Б. Волоконная оптика в локальных и корпоративных сетях связи. АйТи / А. Б. Семенов. – М.: Компьютер-пресс, 1998.

9. Дилип, Н. Стандарты и протоколы Интернета: пер. с англ. / Н. Дилип. – М.: Издательский отдел «Русская Редакция» ТОО «Channel Trading Ltd.», 1999.

10. Дэвис, Дж. Microsoft Windows Server 2003. Протоколы и службы TCP/IP. Техническое руководство / Дж. Дэвис, Т. Ли. – М.: СП ЭКОМ, 2005.

11. Челлис, Дж. Основы построения сетей: учеб. пособие для специалистов MCSE / Дж. Челлис, Ч. Перкинс, М. Стриб. – М.: Лори, 1997.

12. Урбанович, П. П. Информационная безопасность и надежность систем: учеб.-метод. пособие для студентов специальности 1-40 01 02 «Информационные системы и технологии» / П. П. Урбанович, Д. М. Романенко, Е. В. Романцевич. – Минск: БГТУ, 2007.

13. Новиков, Ю. В. Локальные сети. Архитектура, алгоритмы, проектирование / Ю. В. Новиков, С. В. Кондратенко. – М.: ЭКОМ, 2000.

14. Фейт, С. TCP-IP. Архитектура, протоколы, реализация / С. Фейт. – М.: Лори, 2000.

15. Гейер, Д. Беспроводные сети. Первый шаг / Д. Гейер. – М.: Вильямс, 2005.

16. Рошан, П. Основы построения беспроводных локальных сетей стандарта 802.11 / П. Рошан, Д. Лиэри. – М.: Вильямс, 2004.

17. Якубайтис, Э. А. Информационные сети и системы. Справочная книга / Э. А. Якубайтис. – М.: Финансы и статистика, 1996.

18. Нанс, Б. Компьютерные сети: пер. с англ. / Б. Нанс. – М.: БИНОМ, 1996.

19. Титтел, Э. Networking Essentials / Э. Титтел, К. Хадсон, Дж. Майкл Стюарт. – СПб.: ПИТЕР, 1999.

20. Титтел, Э. TCP/IP / Э. Титтел, К. Хадсон, Дж. Майкл Стюарт. – СПб.: ПИТЕР, 1999.

21. Скляр, Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр. – М.: Издательский дом «Вильямс», 2002.

РУССКОЯЗЫЧНЫЕ ТЕРМИНЫ И ПОНЯТИЯ

***А**даптер* (adapter) – устройство либо программа для согласования параметров входных и выходных сигналов в целях сопряжения объектов.

Административная система (management system) – система, обеспечивающая управление сетью либо ее частью.

Адрес (address) – закодированное обозначение пункта отправления либо назначения данных.

Адрес IP – адрес, однозначно определяющий компьютер в сети (адрес состоит из 32 двоичных разрядов и не может повторяться во всей сети TCP/IP). Адрес IP обычно разбивается на четыре октета по восемь двоичных разрядов (один байт); каждый октет преобразуется в десятичное число и отделяется точкой, например, 102.54.94.97.

Аналоговый сигнал (analog signal) – сигнал, величина которого непрерывно изменяется во времени. Аналоговый сигнал обеспечивает передачу данных путем непрерывного изменения во времени.

Аналого-дискретное преобразование (analog-to-digital conversion) – процесс преобразования аналогового сигнала в дискретный.

Анонимные подключения – эта функция, которая разрешает удаленный доступ к ресурсам компьютера по учетной записи компьютера без предъявления имени и пароля с правами, определяемыми этой учетной записью.

Архитектура – концепция, определяющая модель, структуру, выполняемые функции и взаимосвязь компонентов сети. Архитектура охватывает логическую, физическую и программную структуры и функционирование сети, а также элементы, характер и топологию взаимодействия элементов.

Асинхронная передача – метод передачи, основанный на пересылке данных по одному символу. При этом промежутки между передачами символов могут быть не равными.

***Б**аза данных*, *БД* (database) – совокупность взаимосвязанных данных, организованная по определенным правилам в виде одного или группы файлов.

Базовый порт ввода/вывода (base I/O port) – адрес памяти, по которому центральный процессор и адаптер проверяют наличие сообщений, которые они могут оставлять друг для друга.

Безопасность данных (data security) – концепция защиты программ и данных от случайного либо умышленного изменения, уничтожения, разглашения, а также несанкционированного использования.

Блок данных (data unit) – последовательность символов фиксированной длины, используемая для представления данных или самостоятельно передаваемая в сети.

Бод (baud) – термин, используемый для измерения скорости модема, который описывает количество изменений состояния, происходящих за одну секунду в аналоговой телефонной линии.

Булева алгебра – алгебраическая структура с тремя операциями И, ИЛИ, НЕ.

Буфер (buffer) – временная область, которую устройство использует для хранения входящих данных перед тем, как они смогут быть обработаны на входе, или для хранения исходящих данных до тех пор, пока не появится возможность их передачи.

***В**итая пара* (twisted-pair cable) – два скрученных изолированных провода, которые используются для передачи электрических сигналов.

Виртуальная сеть (virtual network) – сеть, характеристики которой в основном определяются ее программным обеспечением.

Виртуальные локальные вычислительные сети (ВЛВС) – логические наложения на коммутируемое объединение сетей, определяющие группы пользователей. Это означает, что пользователь или система, подключенные к физическому порту, могут участвовать в нескольких ВЛВС – группах, поскольку логическая сеть не обязана подчиняться ограничениям физической. Границы ВЛВС задают область локального вещания. Обычно потоки данных в ВЛВС коммутируются на уровне 2, в то время как трафик между ВЛВС маршрутизируется с использованием внешнего маршрутизатора.

Волновое сопротивление, импеданс (impedance) – полное электрическое сопротивление переменному току, включающее активную и реактивную составляющие. Измеряется в омах.

Выделенная линия (dedicated line) – (точка – точка) частная или адресуемая линия, наиболее популярная в глобальных вычис-

лительных сетях. Обеспечивает полнодуплексную полосу пропускания с постоянным соединением каждой конечной точки через мосты и маршрутизаторы с несколькими ЛВС.

Выделенный сервер (dedicated server) – сетевой сервер, который действует только как сервер и не предназначен для использования в качестве клиентской машины.

Г*игабайт* (gigabyte) – обычно 1000 мегабайт. Точно 1024 мегабайт, где 1 мегабайт равен 1 048 576 байт.

Гиперсреда (hypermedia) – технология представления любых видов информации в виде блоков, ассоциативно связанных друг с другом, не требующая подтверждения о приеме от принимающей стороны.

Гипертекст (hypertext) – текст, представленный в виде ассоциативно связанных друг с другом блоков.

Гипертекстовый протокол HTTP – протокол сети Internet, описывающий процедуры обмена блоками гипертекста.

Главный контроллер домена (Primary Domain Controller, PDC) – компьютер, на котором устанавливается Windows NT Server в режиме PDC для хранения главной копии базы данных учетных записей.

Глобальная вычислительная сеть (Wide Area Network, WAN) – компьютерная сеть, использующая средства связи дальнего действия.

Группа (group) – совокупность пользователей, определяемая общим именем и правами доступа к ресурсам.

Д*анные* (data) – информация, представленная в формализованном виде, пригодном для автоматической обработки при возможном участии человека.

Дейтаграммы (datagrams) – сообщения, которые не требуют подтверждения о приеме от принимающей стороны. Термин, используемый в некоторых протоколах для обозначения пакета.

Дефрагментация (defragmentation) – процесс воссоздания больших PDU (пакетных блоков данных) на более высоком уровне из набора более мелких PDU с нижнего уровня.

Диагностическое программное обеспечение (diagnostic software) – специализированные программы или специфические системные компоненты, которые позволяют исследовать и наблюдать систему с целью определения корректности функционирования, при необходимости идентификации причины проблемы.

Дискретный сигнал (discrete signal) – сигнал, имеющий конечное, обычно небольшое, число значений. Практически всегда дискретный сигнал имеет два либо три значения. Нередко его называют также цифровым сигналом.

Домен (domain) – совокупность компьютеров, использующих операционную систему Windows NT Server, имеющих общую базу данных и систему защиты. Каждый домен имеет неповторяющееся имя.

Доменная система имен (Domain Name System, DNS) – система обозначений для сопоставления адресов IP и имен, понятных пользователю, используется в сети Internet. Система DNS иногда называется службой DNS.

Доступ (access) – операция, обеспечивающая запись, модификацию, чтение или передачу данных.

Драйвер (driver) – компонент операционной системы, взаимодействующий с внешним устройством или управляющий выполнением программ.

Драйвер устройства (device driver) – программа, которая обеспечивает взаимодействие между операционной системой и конкретными устройствами с целью ввода/вывода данных для этого устройства.

***Е**динообразный локатор ресурсов* (Uniform Resource Locator, URL) – идентификатор, или адрес ресурсов, в сети Internet. Обеспечивает гипертекстовые связи между документами WWW.

***Ж**есткий диск* (hard disk) – накопитель данных в вычислительных системах.

***З**аголовок кадра* (frame preamble) – служебная информация канального уровня модели OSI, добавляемая в начало кадра.

Запрос прерывания (Interrupt Request, IRQ) – сигнал, посылаемый центральному процессору от периферийного устройства. Сообщает о событии, обработка которого требует участие процессора.

Запросчик (requester, LAN requester) – (редиректор) программа, находящаяся на компьютере-клиенте. Переадресует на соответствующий сервер запросы на сетевые услуги со стороны работающих на этом же компьютере приложений.

Затухание (attenuation) – ослабление сигнала при удалении его от точки испускания.

Звезда (star topology) – вид топологии, при котором каждый компьютер подключен к центральному компоненту, называемому концентратором.

Зеркальные диски (disk mirroring) – уровень 1 технологии RAID, при которой часть жесткого диска (или весь жесткий диск) дублируется на одном или нескольких жестких дисках. Позволяет создавать резервную копию данных.

И*мпульсно-кодовая модуляция*, ИКМ (Pulse Code Modulation, PCM) – метод преобразования аналогового сигнала телефонии в дискретный сигнал.

Интернет – совокупность компьютеров, объединенных в глобальную сеть.

Информационная сеть (information network) – сеть, предназначенная для обработки, хранения и передачи данных.

Информационная система (information system) – объект, способный осуществлять хранение, обработку или передачу данных. К информационной системе относятся: компьютеры, программы, пользователи и другие составляющие, предназначенные для процесса обработки и передачи данных.

Информационно-поисковая система – (Information Retrieval System, IRS) – система, предназначенная для поиска информации в базе данных.

Информация (information) – данные, обработанные адекватными им методами.

Инфракрасный канал (infrared channel) – канал, использующий для передачи данных инфракрасное излучение. Инфракрасный канал работает в диапазоне высоких частот, где сигналы мало подвержены электрическим помехам.

К*абель* (cable) – один либо группа изолированных проводников, заключенных в герметическую оболочку.

Кадр (frame) – блок информации канального уровня.

Кадр данных (data frame) – базовая упаковка битов, которая представляет собой PDU (пакетный блок данных), посланный с одного компьютера на другой по сетевому носителю.

Канал (link) – среда или путь передачи данных.

Канал передачи данных (data channel) – кабели и инфраструктура сети.

Канальный уровень (date link layer) – второй уровень модели OSI. Здесь из последовательности битов, поступающих от физического уровня, формируются кадры.

Клиент (client) – компьютер в сети, который запрашивает ресурсы или услуги от некоторых других компьютеров.

Клиент – сервер (client – server) – модель вычислений, при которой некоторые компьютеры запрашивают услуги (клиенты), а другие отвечают на такие запросы на услуги (сервер).

Коаксиальный кабель (coaxial cable) – кабель, состоящий из изолированных друг от друга внутреннего и внешнего проводников. Коаксиальный кабель имеет один либо несколько центральных медных проводников, покрытых диэлектрической изоляцией, которая для защиты центральных проводников от внешних электромагнитных воздействий покрыта металлической оплеткой (сеткой) либо трубкой.

Коллизия (collision) – ситуация, когда две рабочие станции пытаются одновременно занять канал (использовать рабочую среду – кабель).

Коммуникационная сеть – сеть, предназначенная для передачи данных, также она выполняет задачи, связанные с преобразованием данных.

Коммутатор (switch) – устройство или программа, осуществляющие выбор одного из возможных вариантов направления передачи данных.

Коммутаторы кадров – многопортовые мосты уровня доступа к среде передачи, работающие со скоростью этой среды и гарантирующие на порядок более высокую пропускную способность при связывании клиентских и серверных систем по сравнению с концентраторами для среды с разделяемым доступом. При сегментации ЛВС коммутаторы кадров обеспечивают лучшие показатели цена/производительность и меньшие задержки, чем традиционные связки мостов и маршрутизаторов.

Коммутаторы ячеек – устройства, реализующие ATM-коммутацию данных, разделенных на короткие ячейки фиксированного размера. Ориентация на установление соединений позволяет ATM обеспечивать классы (качество) обслуживания, пригодные для всех видов мультимедийного трафика, включая данные, голос и видео.

Концентратор, или *хаб* (concentrator or hub) – связующий компонент сети, к которому подключаются все компьютеры в сети топологии звезда. Концентратор обеспечивает связь компьютеров друг с другом при использовании витой пары, также используется в сетях FDDI для подключения компьютеров в центральном узле.

Концентратор MSAU (Multi Station Access Unit) – устройство для доступа к множеству станций, которое осуществляет маршрутизацию пакета к следующему узлу в сетях с методом доступа с передачей маркера.

Корпоративная сеть (enterprise network) – крупномасштабная сеть, обычно соединяющая многие локальные сети.

Л*огический диск* (logical disk) – часть физического диска, отформатированная под конкретную файловую систему и имеющая свое буквенное наименование.

Логический канал (logical channel) – путь, по которому данные передаются от одного порта к другому. Логический канал прокладывается в одном либо последовательности физических каналов и через уровни области взаимодействия.

Локальная группа (local group) – в Windows NT Server учетная запись, определенная на конкретном компьютере. Включает учетные записи пользователей данного компьютера.

Локальная сеть (Local-Area Network) – сеть, системы которой расположены на небольшом расстоянии друг от друга.

М*агистраль* (backbone) – основной кабель, от которого кабели трансиверов идут к компьютерам, повторителям и мостам.

Манчестерское кодирование – схема передачи двоичных данных, применяемая во многих сетях. При передаче бита, равного 1, в течение временного интервала, который отведен для его передачи, значение сигнала меняется с положительного на отрицательное. При передаче бита, равного 0, в течение временного интервала, который отведен для его передачи, значение сигнала меняется с отрицательного на положительное.

Маркер (token) – уникальная комбинация битов. Когда рабочая станция в ЛВС получает маркер, она имеет право начать передачу данных.

Маршрутизатор (router) – протокол, ориентированное устройство, соединяющее две сети, иногда с абсолютно разными уровнями MAC (канальный уровень, контроль доступа к среде).

Маршрутизация (routing) – процесс определения в коммуникационной сети пути, по которому блок данных может достигнуть адресата.

Маска сети (network mask) – 32-битовое число, по которому можно определить диапазон IP-адресов, находящихся в одной IP-сети/подсети.

Масштабируемость (scalability) – это возможность увеличить вычислительную мощность Web-сайта или компьютерной системы (в частности, выполнение большего числа операций или транзакций за определенный период времени) за счет установки большего числа процессоров или их замены на более мощные.

Мегабайт (megabyte) – 1 048 576 байт.

Метод доступа (access method) – способ определения, какая рабочая станция сможет следующей использовать ЛВС. Кроме того, так называется набор правил, используемых сетевым оборудованием, чтобы направлять поток сообщений через сеть, а также один из основных признаков, по которым различают компоненты сетевого оборудования.

Метод доступа к каналу (channel access method) – правила, используемые для определения, какой компьютер может посылать данные по сети, тем самым предотвращающие потерю данных из-за коллизий.

Метод множественного доступа с прослушиванием несущей и разрешением коллизий (CSMA/CD) – метод доступа к каналу связи, который устанавливает следующий порядок: если рабочая станция хочет воспользоваться сетью для передачи данных, она сначала должна проверить состояние канала, начинать передачу станция может, если канал свободен. В процессе передачи станция продолжает прослушивание сети для обнаружения возможных конфликтов. Если возникает конфликт в случае, когда два узла попытаются занять канал, то обнаружившая конфликт интерфейсная плата, выдает в сеть специальный сигнал, и обе станции одновременно прекращают передачу.

Метод обработки запросов по приоритету (Demand Priority MA) – метод доступа к каналу связи, где всем узлам сети предоставляется право равного доступа. Концентратор опрашивает каждый порт и проверяет наличие запроса на передачу, затем решает этот запрос в соответствии с приоритетом.

Метод с передачей маркера, или полномочия (TPMA) – метод доступа к каналу связи, в котором от компьютера к компьютеру

передается маркер, дающий разрешение на передачу сообщения. При получении маркера рабочая станция может передавать сообщение, присоединяя его к маркеру, который переносит его по сети. Каждая станция, находящаяся между передающей и принимающей «видит» это сообщение, но только станция-адресат принимает его. При этом она создает новый маркер.

Микроядро (microkernel) – центральная часть операционной системы, выполняющая основные функции управления системой.

Модем (modem) – сокращение от МОДулятор-ДЕМодулятор. Устройство связи, позволяющее компьютеру передавать данные по обычной телефонной линии. При передаче преобразует цифровые сигналы в аналоговые, при приеме – аналоговые в цифровые.

Монитор сети (network monitor) – программно-аппаратное устройство, которое отслеживает сетевой трафик. Проверяет пакеты на уровне кадров, собирает информацию о типах пакетов и ошибках.

Мост (bridge) – это прибор, позволяющий рабочим станциям одной сети обращаться к рабочим станциям другой. Мосты используются для разделения ЛВС на маленькие сегменты. Выполняет соединение на канальном уровне модели OSI. Мост преобразует физический и канальный уровни различных типов. Используется для увеличения длины или количества узлов.

Мост-маршрутизатор (bridge-router) – сетевое устройство, которое объединяет лучшие функции моста и маршрутизатора.

Мультиплексор (multiplexor) – устройство, позволяющее разделить канал передачи на два или более подканала. Может быть реализован программно. Кроме того, используется для подключения нескольких линий связи к компьютеру.

Н*ейронная сеть* (neural network) – сеть, образованная взаимодействующими друг с другом нервными клетками либо моделирующими их поведение компонентами.

Несущая (carrier) – непрерывный сигнал, на который накладывается другой сигнал, несущий информацию.

Неэкранированная витая пара (Unshielded Twisted Pair, UTP) – кабель, в котором изолированная пара проводников скручена с небольшим числом витков на единицу длины. Скручивание проводов уменьшает электрические помехи извне при распространении сигналов по кабелю.

***О**болочка* (shell) – программное обеспечение, которое реализует взаимодействие пользователя с операционной системой (пользовательский интерфейс).

Обработка запросов по приоритету (demand priority) – высокоскоростной метод доступа к каналу, используемый сетями 100VG-Any LAN в топологии звезда.

Общий ресурс (shared resource) – любое устройство, данные или программа.

Одноранговая архитектура (peer-to-peer architecture) – концепция информационной сети, в которой каждая абонентская система может предоставлять и потреблять ресурсы.

Оперативная память (main memory) – память, предназначенная для хранения данных и команд, необходимых процессору для выполнения операций.

Оптический кабель (optical cable) – кабель, передающий сигналы света. Для создания оптического кабеля используются световоды, каждый из которых имеет несколько слоев защитных покрытий, улучшающих механические и оптические характеристики этих световодов.

Оптический канал (optical channel) – канал, предназначенный для передачи сигналов света.

Оптоволокно (optical fiber) – среда, по которой цифровые данные передаются в виде модулированных световых импульсов.

***П**акет* (packet) – это единица информации, передаваемой между станциями сети, используется на сетевом уровне модели OSI.

Пароль (password) – признак, подтверждающий право пользователя или прикладной программы на использование какого-либо ресурса.

Передача данных (data communications) – процесс транспортирования данных из одной системы в другую.

Повторитель, или *репитер* (repeater) – устройство, усиливающее сигналы с одного отрезка кабеля и передающее их в другой отрезок без изменения содержания. Повторители увеличивают максимальную длину трассы ЛВС.

Полномочие (token) – специальный символ или группа символов, разрешающая системе передачу кадров.

Полоса пропускания (bandwidth) – разность между максимальной и минимальной частотой в заданном диапазоне; диапазон частот, на которых может работать носитель.

Пользователь (user) – юридическое либо физическое лицо, использующее какие-либо ресурсы, возможности.

Порт (port) – точка доступа к устройству либо программе. Различают физические и логические порты.

Провайдер (provider) – организация, которая обеспечивает подключение к Internet и другие услуги за определенную плату.

Протокол (protocol) – набор правил, регламентирующих порядок сборки пакетов, содержащих данные и управляющую информацию, на рабочей станции-отправителе для передачи их по сети, а также порядок разборки пакетов по достижении ими рабочей станции-получателя.

Р*абочая станция* (*компьютер, ПК, клиент*) – это компьютеры, которые используют ресурсы сервера и предоставляют удобные интерфейсы пользователю.

Распределитель (hub) – центр ЛВС или кабельной системы с топологией звезда. В этой роли могут быть файл-серверы или концентраторы. Они содержат сетевое программное обеспечение и управляют коммуникациями внутри сети, а также могут работать как шлюзы к другим ЛВС.

Редиректор для ОС (redirector) – сетевое программное обеспечение, которое принимает запросы ввода/вывода для удаленных файлов, именованных каналов или почтовых слотов и затем переназначает их сетевым сервисам другого компьютера. Для Windows NT редиректоры выполнены как драйверы файловой системы.

Редиректор для протоколов (redirector) – компонент набора протоколов или сетевой операционной системы, ответственный за перехват запросов от приложений и распределение их между локальной или удаленной службами сети.

Реестр (registry) – архив БД Windows NT для хранения информации о конфигурации компьютера, включая аппаратные средства, установленное программное обеспечение, установки окружения и др.

С*еанс* (session) – сообщение, в котором предполагается создание логической связи для обмена сообщений. Сеанс должен быть

сначала установлен, после этого происходит обмен сообщениями. После окончания обмена сеанс должен быть закрыт.

Сегмент (segment) – часть сети, ограниченная ретранслирующими устройствами (повторителями, мостами, маршрутизаторами и шлюзами).

Сервер (server) – это компьютер сети, предоставляющий сервис другим объектам по их запросам.

Сервис (service) – процесс обслуживания объектов.

Сетевая служба (network service) – вид сервиса, предоставляемого сетью.

Сеть (network) – взаимодействующая совокупность сетевых узлов, связанных друг с другом каналами связи, предназначенная для передачи информации.

Слот адаптера (adapter slot) – гнездо, встроенное в материнскую плату.

Стандарт RS-232 – промышленный стандарт для последовательных соединений.

Т*елекоммуникация* (telecommunication) – область деятельности, предметом которой являются методы и средства передачи информации.

Терминал (terminal) – устройство ввода/вывода данных и команд в информационных системах.

Тестирование (testing) – процесс проверки правильности функционирования устройства либо программного обеспечения.

Тип кадра (frame type) – один из четырех стандартов, которые определяют структуру пакета Ethernet: Ethernet 802.3, Ethernet 802.2, Ethernet SNAP или Ethernet II.

Транзакция (transaction) – короткий во времени цикл взаимодействия объектов, включающий запрос – выполнение задания – ответ.

Трансивер (transceiver) – устройство, предназначенное осуществлять передачу данных с сетевых интерфейсных плат в физическую среду.

Трафик (traffic) – поток данных.

У*даленная регистрация* (remote logon) – подключение по сети к другому компьютеру пользователя, зарегистрированного на своем ПК по своей учетной записи.

Удаленный доступ (dial-up) – доступ к системе или по сети к другому компьютеру пользователя, зарегистрированного на своем ПК по своей учетной записи.

Утилита (utility) – программа, выполняющая какую-либо функцию сервиса.

Узел (node) – точка присоединения к сети; устройство, подключенное к сети.

Учетная запись (account) – информация, хранящаяся в базе данных Windows NT (учетная запись пользователя, компьютера, группы).

Ф*аксимильная связь* (faximile) – процесс передачи через коммуникационную сеть неподвижных изображений и текста.

Фрагментация (fragmentation) – процесс разделения длинного пакета данных с более высокого уровня на последовательность более коротких пакетов на нижнем уровне.

Ц*ентральный процессор* (central processing unit) – управляющий и вычислительный модуль компьютера. Устройство, которое интерпретирует и выполняет команды.

Циклический избыточный код (Cyclical Redundancy Check, CRC) – число, получаемое в результате математических преобразований над пакетом данных и исходными данными. При доставке пакета вычисления повторяются. Если результат совпадает, то пакет принят без ошибок.

Цифровая линия (digital line) – линия связи, передающая информацию только в двоичной (цифровой) форме.

Цифровая сеть комплексных услуг (Integrated Services Digital Network, ISDN) – цифровая сеть связи, обеспечивающая коммутацию каналов и коммутацию пакетов.

Ч*етность* (parity) – способ контроля за безошибочной передачей блоков данных с помощью добавления контрольных битов.

Ш*ина* (bus) – канал передачи данных, отдельные части которого называются сегментами.

Широковещательная передача (broadcast) – технология передачи сигналов, таких как сетевые данные, посредством использования

передатчика какого-либо типа для посылки этих сигналов по коммуникационному носителю.

Шифрование (encryption) – преобразование информации для ее защиты от несанкционированного доступа.

Шлюз (gateway) – устройство, посредством которого соединяются сети разных архитектур.

***Э**кран* (shielding) – металлическая оплетка или цилиндр, навитый из фольги. Защищает передаваемые данные, уменьшая внешние электрические помехи, которые называются шумом.

Экранированная витая пара (Shielded Twisted-Pair, STP) – витая пара, окруженная заземленной металлической оплеткой, которая служит экраном.

Электронная почта (e-mail) – компьютерная система обмена сообщениями, где текст и файлы могут быть посланы от одного пользователя к одному или многим другим пользователям в той же сети.

Эталонная модель взаимодействия открытых систем (Open System Interconnection, OSI) – семиуровневая модель, которая стандартизирует уровни услуг и виды взаимодействия между системами в информационной сети при передаче данных.

Эфир (ether) – пространство, через которое распространяются волны электромагнитного спектра и прокладываются каналы радиосетей и инфракрасных сетей. Электромагнитное поле не нуждается в специальном носителе.

***Я**зык HTML* – инструментальное программное обеспечение, использующее технологию гипертекста.

Язык описания страниц (page description language) – язык программирования, который описывает вид страницы для печати. Используется для компоновки изображения страницы.

Язык структурированных запросов (Structured Query Language, SQL) – язык управления базами данных, используемый для запроса, обновления и управления реляционными базами данных.

Ячеистая топология сети (mesh network topology) – топология, используемая в глобальных вычислительных сетях. К любому узлу существует несколько маршрутов.

СЛОВАРЬ АНГЛОЯЗЫЧНЫХ ТЕРМИНОВ И ПОНЯТИЙ

A*ccess* – доступ.

Access auditing – контроль доступа.

Addressing – адресация, способ указания объектов в сети либо в системе.

Administration – администрирование, управление сетью.

Analog network – аналоговая сеть, передающая и обрабатывающая аналоговые сигналы.

Analog-to-digital conversion – аналого-дискретное преобразование, процесс преобразования аналогового сигнала в дискретный.

Animation – анимация, виртуальная реальность, мнимый мир, создаваемый аудиовидиосистемой в воображении пользователя.

Application layer – прикладной уровень модели OSI, обеспечивающий прикладным процессам средства доступа к области взаимодействия.

Archivator – архиватор, программа, обеспечивающая сжатие данных.

Arithmetic and Logical Unit (ALU) – арифметико-логическое устройство, часть процессора, выполняющая арифметические и логические операции над данными.

Asynchronous Transfer Mode (ATM) – асинхронный способ передачи данных, пакетно-ориентированный метод скоростной передачи.

B*anyan network* – баньяновая сеть, скоростная распределительная сеть с каскадной адресацией.

Baud – бод, единица скорости передачи данных. Число бод равно количеству изменений сигнала (потенциала, фазы, частоты), происходящих в секунду. Для двоичных сигналов часто считают, что бод равен биту в секунду, например 1200 бод = 1200 бит/с.

Binary code – двоичный код, алфавит кода ограничен двумя символами (0, +1).

Bipolar code – биполярный код. Алфавит кода ограничен тремя символами (–1, 0, +1), где единицы представляются чередующимися импульсами. Отсутствие импульсов определяет состояние нуля.

Bit – бит, наименьшая единица информации в двоичной системе счисления.

Bridge – мост, сетевое оборудование для преобразования физического и канального уровней различных типов.

Broadband channel – широкополосный канал.

Broadcasting – широковещание.

Bus – шина.

Byte – байт, единица количества информации, равная 8 бит.

C*able* – кабель, длинномерное изделие для передачи сигналов.

Cache memory – кэш-память, буферное запоминающее устройство, работающее со скоростью, обеспечивающей функционирование процессора без режимов ожидания.

Carrier – несущая, непрерывный сигнал, на который накладывается другой сигнал, дающий информацию.

Cellular packet radio network – сотовая пакетная радиосеть.

Channel – канал, среда или путь, по которому передаются данные.

Circuit switching – коммутация каналов, предоставление последовательности каналов сети для монопольного использования при передаче данных во время сеанса.

Client – клиент, объект, использующий сервис, предоставляемый другими объектами.

Client – server architecture – архитектура клиент – сервер.

Clock rate – тактовая частота.

Closed channel – закрытый канал.

Communication network – коммуникационная сеть, предназначенная для передачи данных, также она выполняет задачи, связанные с преобразованием данных.

Compiler – компилятор, программа-транслятор преобразующая код в язык машинных команд (исполняемый файл).

Confidention – конфиденциальность, доверительность, секретность.

Conformance – конформность, соответствие объекта его нормативно-технической документации. Конформность объекта определяется в результате процесса его тестирования.

Connection – соединение.

Console – консоль, одна либо несколько абонентских систем для работы с платформой управления сетью.

***D**ata link layer* – канальный уровень, уровень модели OSI, отвечающий за формирование и передачу блоков данных и обеспечивающий доступ к каналу связи области взаимодействия.

Data management – управление данными.

Data processing – обработка данных.

Data protection – защита данных.

Data security – безопасность данных.

Data security architecture – архитектура безопасности данных, архитектура, определяющая методы и средства защиты данных.

Data transfer – пересылка данных.

Data unit – блок данных.

Databank – банк данных.

Database – база данных.

DataBase Management System (DBMS) – система управления базой данных (СУБД).

Database server – сервер базы данных.

Datagram – дейтаграмма, сообщение, которое не требует подтверждения о приеме от принимающей стороны.

Decoding – декодирование.

Dedicated channel – выделенный канал.

Designator – распределитель.

Determinate access – детерминированный доступ, множественный доступ.

Device – устройство.

Diagnostic – диагностика.

Dialog – диалог.

Digital network – дискретная сеть.

Digital signal – цифровой сигнал, дискретный сигнал.

Digital-to-analog conversion – дискретно-аналоговое преобразование, процесс преобразования дискретного сигнала в аналоговый.

Direct Memory Access (DMA) – прямой доступ к памяти.

Directory – каталог.

Directory network service – сетевая служба каталогов.

DirectX – набор драйверов, образующий интерфейс между программами в среде Windows и аппаратными средствами.

DirectDraw – часть набора драйверов DirectX, поддерживающих непосредственную работу с видеокартой и позволяющих осуществлять, например, прямую запись в видеопамять.

Disk drive – дисковод.

Disk Operating System (DOS) – дисковая операционная система (ДОС).

Domain – домен, группа компьютеров, находящаяся в одном месте (здание, этаж, организация) и управляемая СОС.

Driver – драйвер, компонент операционной системы, взаимодействующий с устройством либо управляющий выполнением программ.

Duplex channel – дуплексный канал, осуществляет передачу данных в обоих направлениях.

E*lectronic mail* – электронная почта, средства передачи сообщений между пользователями в сети.

Emulation – эмуляция, организация структуры одного объекта, при которой его функционирование неотличимо от другого объекта.

Encryption – шифрование, способ изменения данных с целью засекречивания.

Enterprise network – корпоративная сеть, локальная сеть большого предприятия.

Ether – эфир, пространство, через которое распространяются волны электромагнитного спектра и прокладываются каналы радиосетей и инфракрасных сетей.

Ethernet network – сеть Ethernet, тип локальной сети, предложенный корпорацией Xerox.

Explorer – браузер (программа) для просмотра Web-страниц.

External device – внешнее устройство.

External memory – внешняя память, непосредственно не доступная процессору.

F*aximile* – факсимильная связь, процесс передачи через коммуникационную сеть неподвижных изображений и текста.

Fast Ethernet – тип скоростной сети Ethernet со скоростью передачи данных 100 Мбит/с.

Fiber channel network – тип скоростной локальной сети, основанной на использовании оптических каналов.

Fiber Distributed Data Interface (FDDI) – оптоволоконный распределенный интерфейс данных.

Fiber-optic link – волоконно-оптическая линия связи.

Flash memory – флэш-память, память на основе полупроводниковой технологии.

Frame – кадр.

Frame relay – ретрансляция кадров.

Frequency band – полоса частот.

Frequency Division Multiple Access (FDMA) – множественный доступ с разделением частоты.

Frequency modulation – частотная модуляция.

Functional profile – функциональный профиль.

G*ateway* – шлюз.

Global network – глобальная сеть.

Gopher – интерактивная оболочка для поиска, присоединения и использования ресурсов и возможностей Internet. Интерфейс с пользователем осуществлен через систему меню.

Graphic interface – графический интерфейс.

H*ardware* – техническое обеспечение.

Hardware Description Language (HDL) – язык описания технических средств.

Hardware platform – аппаратная платформа.

Heterogeneous network – гетерогенная сеть, в которой работают системы различных фирм производителей.

Hierarchical addressing – иерархическая адресация, при которой адреса объединяют в группы, отражая их взаимосвязь.

High-level language – язык высокого уровня.

Host computer – главный компьютер в архитектуре терминал – главный компьютер.

Hypermedia – гиперсреда.

Hypertext – гипертекст.

Hypertext Markup Language (HTML) – гипертекстовый язык разметки.

Hypertext Transfer Protocol (HTTP) – гипертекстовый протокол передачи.

I*dentification* – идентификация.

Information – информация.

Information network – информационная сеть.

Infrared channel – инфракрасный канал.

Infrared network – инфракрасная сеть.

Infrared radiation – инфракрасное излучение.

Infrastructure – инфраструктура.

Input/output device – устройство ввода/вывода.

Input/output interface – интерфейс ввода/вывода.

Integrated Services Digital Network (ISDN) – цифровая сеть с интегральным обслуживанием.

Intelligent hub – интеллектуальный концентратор. Интеллект концентраторов состоит в том, что они могут выполнять операции мониторинга и управления сетью.

Interconnection area – область взаимодействия.

Interpreter – интерпретатор, программа, анализирующая построчно команды или операторы программы и непосредственно выполняющая их.

J*ava language* – язык Java объектно-ориентированной архитектуры, предложенный корпорацией SUN Microsystems.

JavaScript language – язык JavaScript.

K*ey* – ключ.

Knowledge base – база знаний (БЗ).

L*ight guide* – световод.

Link Access Procedure (LAP) – процедура доступа к каналу.

Loader – загрузчик, программа, выполняющая функции загрузки объектного модуля в операционную память и динамического формирования загрузочного модуля.

Local-Area Network (LAN) – локальная сеть.

Locking – блокировка.

Logical address – логический адрес, символический условный адрес объекта.

Logical channel – логический канал.

Low-level language – язык низкого уровня.

M*achine language* – машинный язык.

Macro instruction – макрокоманда.

Manageable hub – управляемый концентратор. Еще одно название для интеллектуальных хабов. Каждый порт управляемого концентратора можно независимо конфигурировать, включать или выключать, а также организовать его мониторинг.

Manchester coding – манчестерское кодирование.

Message – сообщение, единица данных на прикладном уровне.

Mirroring – зеркализация.

Modular hub – модульный концентратор. В основе модульного хаба лежит шасси, в которое помещаются специальные платы или модули. Каждый из модулей функционирует подобно автономному концентратору, а модули взаимодействуют друг с другом через шину шасси.

N*arrowband channel* – узкополосный канал.
NetWare network – сеть NetWare.
Network – сеть.
Network analyzer – анализатор сети.
Network Basic Input/Output System (NetBIOS) – сетевая базовая система ввода/вывода.
Network layer – сетевой уровень.
Network management – управление сетью.
Network Operating System (NOS) – сетевая операционная система (СОС).
Network printer – сетевой принтер.
Network service – сетевая служба.
Neural network – нейронная сеть.
Notebook personal computer – блокнотный персональный компьютер.

O*bject Linking and Embedding technology* (OLE) – технология связи и компоновки объектов.
Object-oriented architecture – объектно-ориентированная архитектура.
Object-Oriented DataBase (OODB) – объектно-ориентированная база данных.
Optical fiber – оптическое волокно.

P*acket* – пакет, единица данных на сетевом уровне.
Packet switching – коммутация пакетов.
Paging device – пейджер, устройство радиовызова.
Parity – четность.
Password – пароль.
PCI bus – шина PCI.
Peer-to-peer architecture – одноранговая архитектура.
Permission – разрешение.
Physical address – физический адрес.

Physical interconnection facility – физические средства соединения.

Physical layer – физический уровень.

Physical link – физический канал.

Physical medium – физическая среда.

Ping – утилита проверки связи с удаленной ЭВМ.

Presentation layer – представительский уровень.

Q*uantization* – квантование, разбиение диапазона значений аналогового сигнала на конечное число интервалов (квант).

Quantum – квант.

R*adio channel* – радиоканал.

Radio local-area network – локальная радиосеть.

Radio network – радиосеть.

Real-time system – система реального времени, функционирование которой зависит не только от логической корректности вычислений, но и от времени, за которое эти вычисления производятся.

Redirector – редиректор.

Relational DataBase (RDB) – реляционная база данных.

Relay system – ретрансляционная система.

Remote access – удаленный доступ.

Repeater – повторитель (репитер).

Resource – ресурс.

Resource sharing – совместное использование ресурса.

Ribbon cable – плоский кабель.

Rout – маршрут, путь.

S*erial interface* – последовательный интерфейс.

Server – сервер.

Service – сервис.

Session – сеанс.

Session layer – сеансовый уровень.

Sharing (разделение) – совместное использование.

Simulation – моделирование.

Software – программное обеспечение.

Stackable hub – стековый хаб. Стековые хабы действуют как автономные устройства с единственным отличием, они позволяют

организовать стек – группу концентраторов, работающих как одно логическое устройство. С точки зрения сети стек концентраторов является одним хабом.

Stand-alone hub – автономный хаб. Устройство с несколькими (обычно от 4 до 32) портами, способное функционировать независимо. Обычно автономные концентраторы поддерживают способ наращивания числа портов.

Switch – коммутатор.

Synchronizing – синхронизация.

T*elecommunications* – телекоммуникации.

Telefax – факс-аппарат.

Telephone mail – электронная почта.

Telephone network – телефонная сеть.

Telnet – удаленный доступ. Дает возможность абоненту работать на любой ЭВМ сети Internet как на своей собственной.

Time sharing – разделение времени.

Token – полномочие, маркер.

Topology – топология.

Traffic – трафик.

Transaction – трансакция, короткий во времени цикл взаимодействия объектов, включающий запрос – выполнение задания – ответ.

Translator – транслятор, программа, преобразующая программу, написанную на одном языке, в программу, представленную на другом языке.

Transparency – прозрачность, объект считается прозрачным для пользователя либо программы в том случае, когда они, работая через (сквозь) объект, не видят его.

Transport layer (транспортный уровень) – уровень, на котором пакеты передаются через коммуникационную сеть.

U*nauthorized access* – несанкционированный доступ.

Uninterruptible Power Supply (UPS) – источник бесперебойного питания.

Unique address – уникальный адрес.

Unipolar code – униполярный код.

Universal CODE (UNICODE) – универсальный код, стандарт 16-разрядного кодирования символов. Код идет на смену использовавшимся до сих пор 7-8-битовым обозначениям.

UNIX operating system (операционная система UNIX) – Сетевая Операционная Система (СОС), созданная фирмой Bell Laboratory.

User – пользователь, юридическое либо физическое лицо, использующее какие-либо ресурсы, возможности.

User interface – интерфейс пользователя.

Utility – утилита, программа, выполняющая какую-либо функцию сервиса.

V*erification* – верификация, процедура проведения анализа с целью установления подлинности, проверки истинности.

Video board – видеоплата, одноплатный контроллер, вставляемый в компьютер, который в режиме реального времени осуществляет аналого-дискретное преобразование.

Video bus – видеошина, предназначенная, в первую очередь, для передачи изображений.

Video conferencing – видеоконференция, способ проведения совещаний и дискуссий между группами удаленных пользователей с использованием движущихся изображений.

Viewer – визуализатор, программа просмотра документов на экране.

W*avequide* – волновод.

Whois – адресная книга сети Internet.

Workstation – рабочие станции, использующие ресурсы сервера и предоставляющие удобные интерфейсы пользователя.

АНГЛОЯЗЫЧНЫЕ СОКРАЩЕНИЯ

1000Base-LX – стандарт на сегменты сети Gigabit Ethernet на оптоволоконном кабеле с длиной волны света 1,3 мкм.

1000Base-SX – стандарт на сегменты сети Gigabit Ethernet на оптоволоконном кабеле с длиной волны света 0,85 мкм.

1000Base-CX – стандарт на сегменты сети Gigabit Ethernet на экранированной витой паре.

100Base-FX – обозначение технологии Fast Ethernet по стандарту 802.3 сети Fast Ethernet для передачи больших сообщений по многомодовому оптоволокну в полудуплексном и полнодуплексном режимах.

100Base-T4 – обозначение технологии Fast Ethernet по стандарту 802.3 со скоростью 100 Мбит/с для четырехпарной витой пары. Вместо кодирования 4B/5B в этом методе используется кодирование 8B/6T.

100Base-TX – обозначение технологии сети Fast Ethernet по стандарту 802.3 для передачи больших сообщений с использованием метода MLT-3 для передачи сигналов 5-битовых порций кода 4B/5B по «витой паре», а также функции автопереговоров (Auto-negotiation) для выбора режима работы порта.

10Base2 – обозначение технологии Ethernet по стандарту 802.3 со скоростью передачи данных 10 Мбит/с для тонкого коаксиального кабеля.

10Base5 – обозначение технологии Ethernet по стандарту 802.3 со скоростью передачи данных 10 Мбит/с для толстого коаксиального кабеля.

10Base-FL – стандарт на сегменты сети Ethernet на оптоволоконном кабеле.

10BaseT – обозначение технологии Ethernet по стандарту 802.3 со скоростью передачи данных 10 Мбит/с для кабеля «витая пара».

***A**CF* (Advanced Communications Function) – дополнительная коммуникационная функция.

ACP (ANSI Code Page) – кодовая страница ANSI.

ACPI (Advanced Configuration and Power Interface) – современный интерфейс конфигурирования и управления энергопотреблением.

ACS (Advanced Connectivity System) – дополнительные системы связи.

ADC (Analog Digital Converter) – аналогово-цифровой преобразователь (АЦП). Предназначен для преобразования аналогового сигнала в цифровой.

AFP (Apple Talk File Protocol) – файловый протокол Apple Talk, протокол удаленного управления файлами Macintosh.

ANR (Automatic Network Routing) – автоматическая сетевая маршрутизация.

ANSI (American National Standards Institute) – американский институт национальных стандартов.

API (Application Programming Interface) – интерфейс прикладных программ. Набор процедур, которые вызываются прикладной программой для осуществления низкоуровневых операций, исполняемых операционной системой.

APPC (Advanced Program-to Program Communication) – высокоуровневый протокол для взаимодействия программ.

ARP (Address Resolution Protocol) – протокол разрешения адреса.

ASCII (American Standard Code for Information Interchange) – американский стандартный код для информационного обмена.

ASMP (ASymmetric Multi Processing) – асимметричная мультипроцессорная обработка.

ASP (Active Server Page) – технология, позволяющая создавать динамические Web-приложения.

AT (Advanced Technology) – усовершенствованная технология.

ATandT (American Telephone and Telegraph) – американский телефон и телеграф.

ATM (Asynchronous Transfer Mode) – асинхронной режим передачи. Тип коммутационной технологии, при котором по сети передаются небольшие ячейки фиксированного размера.

ATP (Apple Talk Protocol) – транзакционный сеансовый протокол Apple Talk.

AUI (Attachment Unit Interface) – интерфейс подключаемого модуля. Интерфейс для подключения внешнего трансивера, установленного на магистральном коаксиальном кабеле.

B*ASE* – сокращение BASEband, основная полоса канала.

BASIC (Beginning All-purpose Symbolic Instruction Code) – система символического кодирования для начинающих.

BBS (Broadcast Bulletin System) – широковещательная система объявлений. Электронная доска объявлений, компьютерный аналог доски объявлений.

BDC (Backup Domain Controller) – вторичный контроллер домена.

BIOS (Basic Input/Output System) – базовая система ввода/вывода.

B-ISDN (Broadband-Integrated Services Digital Network) – широкополосная цифровая сеть с интегральным обслуживанием.

BNS (Broadband Network Service) – широкополосный сетевой сервис.

B-WIN (Broadband-Wissenchafts Nets) – широкополосная исследовательская сеть.

C*AS* (Column Address Strobe) – строб адреса столбца, сигнал, используемый при работе с динамической памятью.

CASE (Computer-Aided Software Engineering) – компьютерная разработка программного обеспечения.

CDMA (Code Division Multiple Access) – множественный доступ с кодовым разделением каналов.

CDPD (Cellular Digital Packet Date) – сотовые дискретные пакетные данные, сотовая пакетная радиосеть.

CD-ROM (Compact Disk Read Only Memory) – компакт-диск с памятью только для чтения.

CGI (Common Gateway Interface) – общий интерфейс шлюза.

CGM (Computer Graphics Metafile) – метафайл компьютерной графики.

CLNP (Connection Less Network Protocol) – сетевой протокол без организации соединений.

CMIP (Common Management Information Protocol) – общий протокол управления информацией.

CPI (Common Programming Interface) – общий программный интерфейс.

CPU (Central Processing Unit) – центральное процессорное устройство.

CRC (Cycle Redundancy Check) – контроль цикличной избыточности.

CSMA/*CD* (Carrier Sense Multiple Access with Collision Detection) – множественный доступ с прослушиванием несущей и разрешением коллизий.

CWIS (Campus Wide Information System) – глобальная информационная система.

D*AS* (Double Attached Station) – станция сети FDDI с двойным подключением к магистральному кольцу или концентратор.

DBMS (DataBase Management System) – система управления БД (СУБД).

DDC (Display Data Channel) – интерфейс обмена данными между компьютером и монитором.

DDE (Dynamic Date Exchange) – динамический обмен данными.

DDP (Delivery Protocol – протокол доставки дейтаграмм, протокол передачи данных Apple, используемый в Apple Talk.

DECT (Digital Enhanced Cordless Telecommunications) – стандарт беспроводной телефонии домашнего или офисного назначения.

DHCP (Dynamic Host Configuration Protocol) – протокол динамической конфигурации хоста.

DLC (Dada Link Control) – протокол управления каналом передачи данных.

DLL (Dynamic Linked Library) – динамическая библиотека.

DMA (Direct Memory Access) – прямой доступ к памяти.

DNS (Domain Name System) – доменная система имен.

DRAM (Dynamic Random Access Memory) – динамическая память прямого доступа, память, схемотехнически выполненная в виде двумерной матрицы (строки и столбцы) конденсаторов.

DVD (Digital Versatile Disk) – цифровой универсальный диск, самый современный стандарт хранения информации на оптическом (лазерном) диске.

DVI (Digital Video Interactive) – система аппаратного сжатия движущихся видеоизображений.

E*BCDIC* (Extended Binary Coded Decimal Interchange Code) – схема кодировки IBM. Используется мэйнфреймами и ПК.

ECC (Error Correction Code) – код коррекции ошибок.

EDGE (Enhanced Data rates for GSM Evolution) – цифровая технология для мобильной связи, которая функционирует как надстройка над 2G и 2.5G сетями.

EISA (Enhanced Industry Standard Architecture) – 32-разрядная архитектура системной шины для ПК на базе процессора Intel.

F*AQ* (Frequently Asked Questions) – часто задаваемые вопросы.

FDDI (Fiber Distributed Date Interface Station) – распределенный интерфейс передачи данных по волоконно-оптическому

кабелю. Технология ЛВС, использующая скорость передачи 100 Мбит/с.

FDMA (Frequency Division Multiple Access) – множественный доступ с разделением частоты.

FDSE (Full Duplex Switched Ethernet) – полнодуплексная коммутируемая сеть Ethernet.

FTAM (File Transfer, Access and Management) – протокол передачи, доступа и управления файлами.

FTP (File Transfer Protocol) – протокол передачи файлов, позволяет обмениваться файлами по сети.

G*DI* (Graphics Device Interface) – интерфейс графического устройства.

GIF (Graphics Interchange Format) – файлы растровых изображений, в которых используется не более 256 индексированных цветов.

GUI (Graphics User Interface) – графический интерфейс пользователя.

H*AL* (Hardware Abstraction Layer) – уровень аппаратных абстракций.

HDL (Hardware Description Language) – язык описания технических средств.

HDLC (High Level Data Link Control) – протокол управления каналом передачи данных высокого уровня.

HTML (Hyper Text Markup Language) – язык гипертекстовой разметки.

HTTP (Hyper Text Transfer Protocol) – протокол передачи гипертекста.

I*BM* (International Business Machines) – международные бизнес-машины.

ICMP (Internet Control Message Protocol) – протокол управления сообщениями Интернета.

IDE (Integrated Device Electronic) – интерфейс жестких дисков.

IEEE (Institute of Electrical and Electronics Engineers) – институт инженеров по электротехнике и электронике.

IIS (Internet Information Server) – компонент Microsoft Back Office, который действует как Web-сервер в среде Windows NT.

IMAP (Internet Message Access Protocol) – протокол доступа к электронной почте, разработан на смену SMTP.

IP (Internet Protocol) – протокол Internet, сетевой протокол стека TCP/IP, который предоставляет адресную и маршрутную информацию.

IPX (Internetwork Packet Exchange) – протокол межсетевого обмена пакетами, предназначенный для адресации и маршрутизации пакетов в сетях Novell.

IRQ (Interrupt ReQuest) – запрос на прерывание.

ISA (Industry Standard Architecture) – системная шина IBM PC/IT. Позволяет подключить к системе различные адаптеры, установив дополнительную плату в гнездо расширения.

ISAPI (Microsoft API) – интерфейсы прикладного программирования фирмы Microsoft.

ISDN (Integrated Services Digital Network) – цифровая сеть с интеграцией услуг.

ISO (International Standard Organization) – Международная организация по стандартизации.

J*TM* (Job Transfer and Manipulation) – сетевая служба передачи и управления заданиями.

L*AN* (Local-Area Network) – локальная сеть.

LAP (Link Access Procedure) – процедура доступа к каналу.

LAT (Local-Area Transport) – немаршрутизируемый протокол фирмы Digital Equipment Corporation.

LLC (Logical Link Control) – логический контроль связи.

M*AC* (Media Assess Control) – контроль доступа к среде.

MAPI (Messaging Application Program Interface) – интерфейс прикладных программ обработки сообщений.

MCA (Micro Channel Architecture) – 32-битная системная шина в ПК IBM PS/2.

MIB (Management Information Base) – информационная база управления информацией.

MNP (Microcom Network Protocol) – серия стандартов, предназначенная для сжатия информации и исправления ошибок при асинхронной передаче данных по телефонным линиям.

N*BP* (Name Binding Protocol) – транспортный протокол связывания имен Apple Talk.

NCP (NetWare Core Protocol) – базовый протокол сетей NetWare.

NDIS (Network Device Interface Specification) – спецификация интерфейса сетевого устройства, программный интерфейс, обеспечивающий взаимодействие между драйверами транспортных протоколов и соответствующими драйверами сетевых интерфейсов. Позволяет использовать несколько протоколов, даже если установлена только одна сетевая карта.

NetBEUI (NetBIOS Extended User Interface) – протокол ЛВС, поддерживаемый всеми СОС фирмы Microsoft, обеспечивает транспортные услуги для NetBIOS.

NetBIOS (Network Basis Input/Output System) – интерфейс прикладных программ для ЛВС, устанавливающий соединение между компьютерами, или сетевая система базового ввода/вывода.

NFS (Network File System) – сетевая файловая система.

NIS (Network Information System) – сетевая информационная система. NIS обеспечивает способ доступа к данным, благодаря которому все узлы сети могут использовать единую БД, содержащую все учетные записи пользователей сети и имена всех сетевых узлов.

NLM (NetWare Loadable Module) – загружаемый модуль NetWare.

NLSP (NetWare Link Service Protocol) – протокол канального сервиса NetWare.

NOS (Network Operating System) – сетевая операционная система.

NRZ (Non-Return to Zero) – без возврата к нулю. Метод двоичного кодирования информации, при котором единичные биты представляются положительным значением, а нулевые отрицательным.

NSAPI (Netscape API) – интерфейсы прикладного программирования фирмы Netscape.

O*DBC* (Open DataBase Connectivity) – открытый доступ к базам данных.

OLE (Object Linking and Embedding) – связь и внедрение объектов.

OME (Open Messaging Environment) – среда открытых сообщений.

OSA (Open Scripting Architecture) – архитектура открытых сценариев.

OSPM (Operating System Directed Power Management) – непосредственное управление энергопотреблением операционной системой.

OSI (Open System Interconnection) – взаимодействие открытых систем.

P*CI* (Peripheral Component Interconnect) – соединение внешних устройств, шина PCI.

PDC (Primary Domain Controller) – первичный контролер доменов, ПК под управлением Windows NT Server, на котором хранятся БД учетных записей домена.

PnP (Plug-and-Play) – технология самонастраиваемого оборудования.

PPP (Point to Point Protocol) – протокол «точка – точка», протокол, предназначенный для работы на двухточечной линии (линии, соединяющей два устройства). Протокол канального уровня.

PTM (Packet Transfer Mode) – пакетный способ передачи.

R*AID* (Redundant Arrays of Inexpensive) – избыточный массив дисков.

RAM (Random Access Memory) – память с произвольным доступом.

RARP (Reverse Address Resolution Protocol) – реверсивный протокол разрешения адреса.

RFS (Remote File System) – удаленная файловая система.

RIP (Routing Internet Protocol) – протокол взаимодействия маршрутизаторов в сети.

RPC (Remote Procedure Call) – вызов удаленных процедур.

RTOS (Real-Time Operating System) – операционная система реального времени.

RTP (Real-time Transport Protocol) – транспортный протокол передачи в реальном времени.

S*AP* (Service Access Point) – точка доступа к службе, точка, в которой услуга какого-либо уровня OSI становиться доступной ближайшему вышележащему уровню. Точки доступа именуются в соответствии с уровнями, обеспечивающими сервис.

SAS (Single Attached Station) – станция сети FDDI с одинарным подключением.

SDH (Synchronous Digital Hierarchy) – синхронная дискретная иерархия. Европейский стандарт на использование оптических кабелей в качестве физической среды для скоростных сетей передачи на большие расстояния.

SDLC (Synchronous Data Link Control) – протокол синхронной передачи данных.

SDN (Software-Defined Network) – сеть, определяемая программным обеспечением – виртуальная сеть.

SID (Security IDentification) – идентификатор безопасности.

SLIP (Serial Line IP) – IP для последовательных линий. Протокол последовательной посимвольной передачи данных. Позволяет компьютеру использовать IP (таким образом становиться полноправным членом сети), осуществляя связь с миром через стандартные телефонные линии и модемы, а также непосредственно через RS-232 интерфейс.

SMTP (Simple Mail Transfer Protocol) – простой протокол электронной почты.

SNA (System Network Architecture) – архитектура систем связи, предназначенная для обмена данными между ПК различных типов.

SNMP (Simple Network Management Protocol) – простой протокол сетевого управления. Протокол сетевого администрирования SNMP очень широко используется в настоящее время. Управление сетью входит в стек протоколов TCP/IP.

SONET (Synchronous Optical Network) – синхронная оптическая сеть.

SPX (Sequenced Packet Exchange) – протокол, который осуществляет передачу сообщений с установлением соединений в сетях Novell.

SQL (Structured Query Language) – язык структурированных запросов.

SSL (Secure Socket Layer) – протокол, который обеспечивает секретный обмен сообщениями для протоколов прикладного уровня стека TCP/IP.

STP (Spanning Tree Protocol) – протокол связывающего (остового) дерева.

T*CP* (Transmission Control Protocol) – протокол управления передачей.

TDI (Transport Driver Interface) – интерфейс транспортного драйвера.

TDMA (Time Division Multiple Access) – множественный доступ с разделением во времени.

TFTP (Trivial File Transfer Protocol) – простейший протокол передачи файлов.

TIFF (Tagged Image Format File) – спецификация формата файла изображения.

TLI (Transport Level Interface) – интерфейс транспортного уровня.

TP4 (Transmission Protocol) – протокол передачи класса 4.

TPMA (Token Passing Multiple Access) – множественный доступ с передачей полномочия, или метод с передачей маркера.

U*DP* (User Datagram Protocol) – пользовательский протокол дейтаграмм.

UMTS (Universal Mobile Telecommunication System) – универсальная система мобильной связи.

UNI (User-to-Network Interface) – сетевой интерфейс пользователя. Набор правил, определяющий взаимодействие оборудования и сети ATM с физической и информационной точек зрения.

UNS (Universal Name Convention) – стандартный метод именования в сети, имеющий вид \\сервер\общий_ресурс.

UPS (Uninterruptible Power Supply) – источник бесперебойного питания.

URL (Uniform Resource Locator) – адрес универсального указателя ресурсов.

UTP (Unsealing Twist Pare) – неэкранированная витая пара.

UUCP (Unix-to-Unix Copy Protocol) – протокол копирования от Unix к Unix.

V*ESA* (Video Electronics Standard Association) – ассоциация стандартов электронной графики.

VGA (Video Graphics Array) – видеографическая матрица.

VHDL (Very High-speed integrated circuit Hardware Description Language) – язык описания технических средств сверхскоростных интегральных схем.

W*AIS* (Wide Area Information Server) – протокол глобального информационного сервера.

WDMA (Wavelength Division Multiple Access) – множественный доступ с разделением длины волны.

WINS (Windows Internet Name Service) – сетевая служба Windows, используемая для определения IP-адреса по имени NetBIOS.

WWW (Word Wide Web) – всемирная сеть.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

С

Т

У

Учебное издание

Урбанович Павел Павлович
Романенко Дмитрий Михайлович
Кабак Елена Владимировна

КОМПЬЮТЕРНЫЕ СЕТИ

Учебное пособие

Редактор *М. А. Юрасова.* Корректор *М. А. Юрасова*
Компьютерная верстка *О. В. Трусевич*

Подписано в печать 11.02.2011. Формат $60\times84^{1}/_{16}$.
Бумага офсетная. Гарнитура Таймс. Печать офсетная.
Усл. печ. л. 23,3. Уч.-изд. л. 22,0.
Тираж 150 экз. Заказ .

Отпечатано в Центре издательско-полиграфических
и информационных технологий учреждения образования
«Белорусский государственный технологический университет».
220006. Минск, Свердлова, 13а.
ЛИ № 02330/0549423 от 08.04.2009.
ЛП № 02330/0150477 от 16.01.2009.

Переплетно-брошюровочные процессы
произведены в ОАО «Полиграфкомбинат им. Я. Коласа».
220600. Минск, Красная, 23. Заказ .