Центр учебной книги и средств обучения
РИПО

Н. М. Ковган

КОМПЬЮТЕРНЫЕ СЕТИ

Учебное пособие

Н. М. Ковган

КОМПЬЮТЕРНЫЕ СЕТИ

Учебное пособие
для учащихся учреждений образования, реализующих образовательные программы среднего специального образования по специальностям «Программное обеспечение информационных технологий», «Электронные вычислительные средства»

Учебное электронное издание

Минск
РИПО
2019

ISBN 978-985-503-947-2

УДК 681.3(075.32)
ББК 32.973.202я723
К56

Р ц н з н т ы :
к фдр информ тики УО «Минский госуд рственный
высший р диотехнический колледж» (С. Г. Буянов);
доцент к федры многопроцессорных систем и сетей
Белорусского госуд рственного университет ,
к ндид т физико-м тем тических н ук, доцент Е. Д. Р феенко.

Ковг н, Н. М.
К56 Компьютерные сети : учебное пособие [Электронный ресурс]/ Н. М. Ковг н. – Минск : РИПО, 2019. – 179 с. : ил.
ISBN 978-985-503-947-2.

Р ссмотрены общие вопросы построения компьютерных сетей: се-тевые рхитектуры, пп р тные компоненты, способы коммут ции, проверки пр вильности перед чи д нных, особенности сетевого про-гр ммного обеспечения, вз имодействие пп р тного и прогр ммного обеспечения вычислительной техники, др йверы сетевых д птеров, принципы р боты протоколов р зных уровней и дрес ции в сетях, т кже р зновидности лок льных и глоб льных компьютерных сетей. Приведены приемы и методы эксплу т ции сетей, предост вления се-тевых услуг и орг низ ции межсетевого вз имодействия.

Содержит список нглийских терминов с р сшифровкой и опис нием.

Предн зн чено для уч щихся учреждений среднего специ льного обр зо-в ния по специ льностям «Прогр ммное обеспечение информ ционных тех-нологий», «Электронные вычислительные средств ».

Текстовое электронное изд ние

Текст воспроизводится по печ тному изд нию 2014 г.

Миним льные системные требов ния:
Microsoft Internet Explorer, версия 6.0 и выше,
Adobe Acrobat Professional, версия 7.0 и выше

Для созд ния электронного изд ния использов ны
Приложение pdf2swf из ПО Swftools, ПО IPRbooks Reader,
р зр бот нное н основе Adobe Air.

Д т подпис ния к использов нию 04.07.2019. Объем 2 Мб.

ВВЕДЕНИЕ

Предметом изучения учебной дисциплины «Компьютерные сети» являются основные структуры вычислительных систем, сетей и средств коммуникации, сетевого программного обеспечения, протоколы глобальных и локальных вычислительных сетей, средства навигации и администрирования вычислительных сетей.

В предлагаемом учебном пособии раскрыты следующие основные вопросы:

- методы проектирования компьютерных сетей;
- современное сетевое оборудование и программное обеспечение;
- принцип административного управления в вычислительных сетях;
- тенденции развития вычислительных сетей;
- сетевые архитектуры: типы, топологии, методы доступа к среде передачи;
- аппаратные компоненты компьютерных сетей;
- способы коммутации, организация обработки и передачи данных в сети, принципы пакетной передачи данных;
- способы проверки правильности передачи данных, обнаружения и устранения ошибок;
- особенности сетевого программного обеспечения, методы разработки сетевого программного обеспечения;
- взаимодействие аппаратного и программного обеспечения вычислительной техники;

• методы и алгоритмы, обеспечивающие эффективное взаимодействие компонентов вычислительной сети;

• драйверы сетевых адаптеров;

• основные понятия, принципы взаимодействия, различия и особенности распространенных протоколов, установка протоколов в операционных системах;

• принципы работы протоколов разных уровней (на примере конкретного стека протоколов);

• принципы адресации в сетях;

• способы предоставления сетевых услуг и организации межсетевого взаимодействия;

• приемы и методы рациональной эксплуатации компьютерных сетей;

• взаимодействие сетевых комплексов с приложениями;

• достоверность информации, ее защита и управление доступом к информационным ресурсам.

РАЗДЕЛ 1
СТРУКТУРА КОМПЬЮТЕРНОЙ СЕТИ

1.1. ОСНОВНЫЕ ТЕРМИНЫ И ПОНЯТИЯ

В настоящее время существует множество способов и средств обмена информацией – от простейшего переноса файлов с помощью диска до всемирной компьютерной сети Интернет, способной объединить все компьютеры мира.

Компьютерная сеть – это группа соединенных компьютеров и других устройств. Основное назначение компьютерной сети – совместное использование ресурсов и постоянная связь в реальном режиме времени.

Сети являются результатом развития компьютерных технологий и представляют собой как частный случай распределенных компьютерных систем, так и средство передачи информации на большие расстояния.

При работе с сетью часто пользуются следующими терминами: ресурсы, связь, абонент, сервер, клиент, среда передачи.

Ресурсы – данные, приложения и периферийные устройства (принтеры, модемы, сканеры и т. д.).

Связь в реальном режиме времени – это обмен сообщениями. Сообщения могут быть простыми списками, документами, видеоклипами. В данное время сети позволяют целому ряду пользователей одновременно вводить данные к периферийным устройствам; если нескольким

пользователям необходимо распечатать один документ, все они обращаются к сетевому принтеру.

Абонент – это устройство, подключенное к сети и активно участвующее в информационном обмене. Чаще всего абонентом сети является компьютер. Абонентом также может быть сетевой принтер или другое периферийное устройство, имеющее возможность напрямую подключаться к сети. Далее вместо термина «абонент» будет использоваться термин «компьютер».

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

Клиент – персональный компьютер, осуществляющий доступ к сетевым ресурсам, предоставленным сервером. Компьютер-клиент также часто называют *рабочей страницей*. В принципе каждый компьютер может быть одновременно как клиентом, так и сервером.

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

Среда передачи – способ соединения персональных компьютеров.

1.2. КЛАССИФИКАЦИЯ СЕТЕЙ

Существуют следующие способы классификации компьютерных сетей:

• по территориальному признаку:

– *локальная вычислительная сеть* (LAN – Local Area Network) – объединение небольшого числа компьютеров в рамках одной организации и в ограниченном пространстве (комната, этаж, здание);

– *региональная сеть* (MAN – Metropolitan Area Network) – создается крупными организациями, банками, средствами массовой информации или территориями для обмена информацией между удаленными абонентами;

– *глобальная сеть* (WAN – Wide Area Network) – образуется в результате объединения сетей различного масштаба, использования полного комплекса средств связи и соединений и охватывает информационным полем всю земную поверхность;

• по способу управления:

– *одноранговые сети*, в которых все компьютеры и соответственно абоненты равноправны по отношению друг к другу;

– *сети на основе сервера* – имеют более крупный масштаб (или это ЛВС, в которой повышены требования к доступу и защите информации). В таких сетях для обслуживания потребностей абонентов выделяют один или несколько серверов;

• по способу соединения (топологии):

– *линейная сеть* («шина»), в которой все компьютеры подключены к общему каналу связи (кабелю), – содержит только два конечных узла и имеет только один путь между любыми двумя узлами;

– *сеть* «*кольцо*», в которой к каждому узлу подсоединены только две ветви;

– *сеть* «*звезда*», в которой имеется только один промежуточный узел;

– *сеть* «*дерево*», построенная по иерархической модели.

1.3. ОСНОВНЫЕ ТИПЫ СЕТЕЙ

Локальные сети. Термин «локальные сети» понимают буквально, т. е. как сети, которые имеют небольшие, локальные размеры и соединяют близко расположенные компьютеры. Однако по характеристикам некоторых современных локальных сетей видно, что такое определение неточно. Например, некоторые локальные сети легко обеспечивают связь на расстоянии нескольких десятков километров. Это уже размеры не комнаты, не здания, не близко расположенных зданий, а, может быть, даже целого города. С другой стороны, по глобальной сети вполне могут связываться компьютеры, находящиеся на соседних столах в одной комнате, но ее почему-то никто не называет локальной сетью. Близко расположенные компьютеры могут также связываться с помощью кабеля, соединяющего разъемы внешних интерфейсов, или даже без кабеля – по инфракрасному каналу, но такая связь тоже не называется локальной.

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

- высокая скорость передачи информации, большая пропускная способность сети;
- низкий уровень ошибок передачи;
- эффективный, быстродействующий механизм управления обменом по сети;
- заранее четко ограниченное количество компьютеров, подключаемых к сети.

Глобальные 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.

На данный момент уже нельзя провести четкую границу между локальными и глобальными сетями. Большинство локальных сетей имеет выход в глобальную сеть, но характер передаваемой информации, принципы организации обмена, режимы доступа к ресурсам внутри локальной сети, как правило, сильно отличаются от тех, что приняты в глобальной сети. И хотя все компьютеры локальной сети в данном случае включены также и в глобальную сеть, специфики локальной сети это не отменяет. Возможность выхода в глобальную сеть остается всего лишь одним из ресурсов, разделяемых пользователями локальной сети. По локальной сети может передаваться самая разная цифровая информация, данные, изображения, телефонные разговоры, электронные письма и т. д. Чаще всего локальные сети используются для разделения (совместного использования) таких ресурсов, как дисковое пространство, принтеры и выход в глобальную сеть, но это всего лишь незначительная часть тех возможностей, которые предоставляют средства локальных сетей. Например, они позволяют осуществлять обмен информацией между компьютерами разных типов. Полноценными абонентами сети могут быть не только компьютеры, но и другие устройства, например, принтеры, плоттеры, сканеры. Локальные сети дают также возможность организовать систему параллельных вычислений на всех компьютерах сети, что многократно ускоряет решение сложных математических задач. С их помощью, как уже упоминалось, можно управлять работой технологической системы или исследовательской установки с нескольких компьютеров одновременно.

Региональные сети. Нередко выделяют еще один класс компьютерных сетей – *городские*, региональные сети, которые обычно по своим характеристикам ближе

к глобальным, 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.

Одноранговые сети. В одноранговой сети все персональные компьютеры равноправны, т. е. нет иерархии среди компьютеров и нет выделенного сервера. Обычно каждый компьютер функционирует и как клиент и как сервер, следовательно, нет отдельного компьютера, ответственного за всю сеть, и пользователи сами решают, какие данные сделать доступными в сети. Одноранговые сети чаще всего объединяют не более десяти персональных компьютеров. Они относительно просты и недороги, так как нет необходимости устанавливать мощный центральный сервер и другие компоненты, обязательные для сложных сетей (этим обычно объясняется высокая стоимость).

В одноранговой сети требования производительности и защищенности сетевого программного обеспечения, как правило, ниже, чем те же требования программного обеспечения выделенных серверов.

Целесообразность применения одноранговых сетей:

– количество пользователей – не более десяти человек;
– пользователи расположены компактно;
– вопросы защиты данных не актуальны;
– в ближайшем будущем нет расширения сетей.

Сети на основе сервера. Большинство сетей имеют следующую конфигурацию – они работают на основе выделенного сервера.

Выделенным называется сервер, который работает только как сервер и не используется в качестве клиента или рабочей станции. Он оптимизирован для быстрой обработки запросов от сетевых клиентов.

Существуют специализированные серверы:
серверы файлов печати;
серверы приложений;
почтовые серверы;
серверы факсов;
коммуникационные серверы;
серверы служб каталогов.

Сервер и сетевая операционная система работают как единое целое. Именно она позволяет реализовывать весь потенциал аппаратных ресурсов сервера.

Основные преимущества сетей на основе сервера:

– выделение ресурсов – администрирование и управление доступом и данными осуществляется централизованно. Ресурсы расположены централизованно, что обеспечивает их быстрый поиск;

– защита – основным аргументом, определяющим выбор сети на основе сервера, является надежная защита данных. Проблемой безопасности может заниматься один администратор – он формирует единую политику безопасности и применяет ее в отношении каждого сетевого пользователя;

– резервное копирование данных – поскольку жизненно важная информация расположена централизованно, нетрудно проводить ее регулярное резервное копирование;

– избыточность – благодаря избыточным системам данные на любом сервере могут дублироваться в реальном режиме времени, поэтому при повреждении основного хранилища информация не будет потеряна, всегда можно воспользоваться резервной копией;

– количество пользователей в сетях – сети на основе сервера способны поддерживать тысячи пользователей;

– аппаратное обеспечение – клиентский персональный компьютер не выполняет функции сервера, требования к его характеристикам определяет сам пользователь.

Комбинированные сети сочетают лучшие качества одноранговой сети и сети на основе сервера. Комбинированные сети наиболее полно соответствуют запросам современных пользователей, но для их правильной реализации, надежной защиты необходимы определенные знания и навыки планирования.

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

- сеть требует дополнительных, иногда значительных материальных затрат на покупку сетевого оборудования, программного обеспечения, на прокладку соединительных кабелей и обучение персонала;
- сеть требует приема на работу специалиста (администратора сети), который будет заниматься контролем работы сети, ее модернизацией, управлением доступа к ресурсам, устранением возможных неисправностей, защитой информации и резервным копированием;
- сеть ограничивает возможности перемещения компьютеров, подключенных к ней, так как при этом может понадобиться перекладка соединительных кабелей;
- сети представляют собой среду для распространения компьютерных вирусов, поэтому вопросам защиты от них следует уделять гораздо больше внимания, чем в случае автономного использования компьютеров;
- сеть резко повышает опасность несанкционированного доступа к информации. Информационная защита требует проведения целого комплекса технических и организационных мероприятий.

1.4. ТОПОЛОГИЯ СЕТИ. БАЗОВЫЕ И КОМБИНИРОВАННЫЕ ТОПОЛОГИИ

При построении сетей важным является выбор физической организации связей между отдельными устройствами сети, т. е. топология сети.

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

Топология определяет требования к оборудованию, тип используемого кабеля, допустимые и наиболее удобные методы управления обменом, надежность работы, возможности расширения сети.

Сетевая топология может быть:

– физической – описывает реальное расположение и связи между узлами сети;

– логической – описывает хождение сигнала в рамках физической топологии.

Физическая топология описывает реально использующиеся способы организации физических соединений различного сетевого оборудования (кабели, разъемы и способы подключения сетевого оборудования).

Логическая топология описывает реальные пути движения сигналов при передаче данных по используемой физической топологии, т. е. пути передачи потоков данных между сетевыми устройствами. Она определяет правила передачи данных в существующей среде передачи с гарантированным отсутствием помех, влияющих на корректность передачи данных.

И хотя выбирать топологию пользователю сети приходится не часто, знать об особенностях основных топологий, их достоинствах и недостатках необходимо.

Существует три базовые топологии сети (на практике нередко используют и другие топологии локальных сетей, однако большинство сетей ориентировано именно на базовые).

Прежде чем перейти к анализу особенностей базовых сетевых топологий, необходимо выделить некоторые важнейшие факторы, влияющие на физическую работоспособность сети и непосредственно связанные с понятием «топология».

Исправность компьютеров (*абонентов*), *подключенных к сети*. В некоторых случаях поломка абонента может заблокировать работу всей сети. Иногда неисправность абонента не влияет на работу сети в целом, но мешает остальным абонентам обмениваться информацией.

Исправность сетевого оборудования, т. е. технических средств, непосредственно подключенных к сети (адаптеры, трансиверы, разъемы и т. д.). Выход из строя сетевого оборудования одного из абонентов может сказаться на всей сети, но может нарушить обмен только с одним абонентом.

Целостность кабеля сети – при обрыве кабеля сети (например, из-за механических воздействий) может нарушиться обмен информацией во всей сети или в одной из ее частей.

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

Шина – все компьютеры параллельно подключаются к одной линии связи. Информация от каждого компью-

тера одновременно передается всем остальным компьютерам (рис. 1.1).

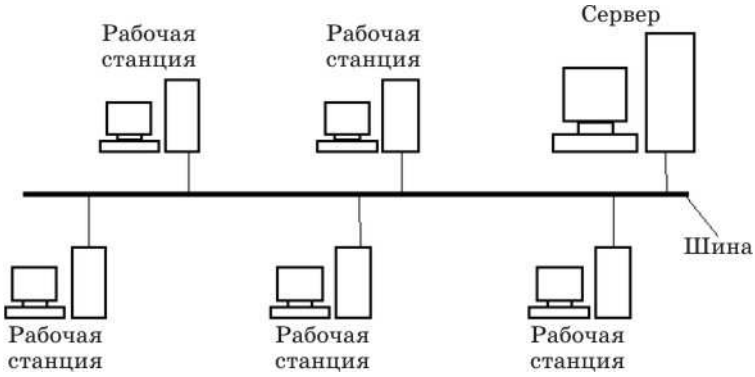

Рис. 1.1. Сетевая топология «шина»

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

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

Поскольку центральный абонент отсутствует, разрешение возможных конфликтов в данном случае ложит-

ся на сетевое оборудование каждого отдельного абонента. В связи с этим сетевая аппаратура при топологии «шина» сложнее, чем при других топологиях.

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

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

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

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

Для увеличения длины сети с топологией «шина» часто используют несколько сегментов (частей сети, каждый из которых представляет собой шину), соединенных

между собой с помощью специальных усилителей и восстановителей сигналов – *репитеров*, или *повторителей*. Однако наращивание длины сети не может продолжаться бесконечно. Ограничения по длине связаны с конечной скоростью распространения сигналов по линиям связи.

Звезда – к одному центральному компьютеру присоединяются остальные периферийные компьютеры, причем каждый из них использует отдельную линию связи (рис. 1.2). Информация от периферийного компьютера передается только центральному компьютеру, от центрального – одному или нескольким периферийным.

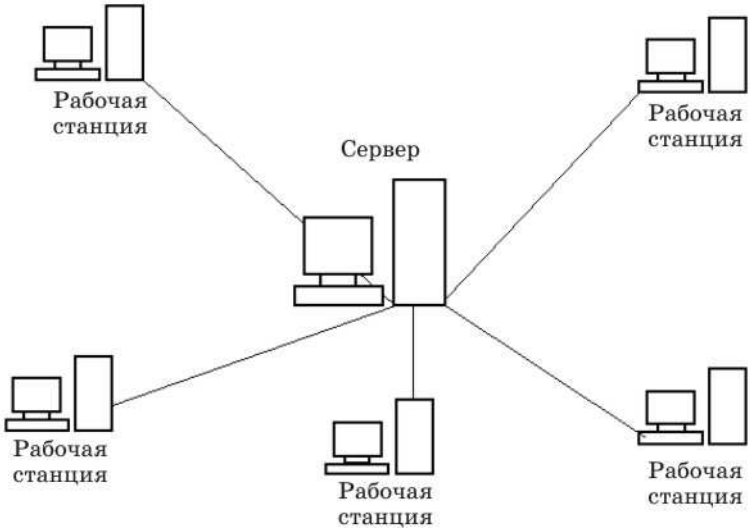

Рис. 1.2. Сетевая топология «звезда»

Звезда – это единственная топология сети с явно выделенным центром, к которому подключаются все остальные абоненты. Обмен информацией идет исключительно через центральный компьютер, на который ложится большая нагрузка, поэтому ничем другим, кроме сети, он, как правило, заниматься не может. Сетевое оборудование центрального абонента должно быть су-

щественно более сложным, чем оборудование периферийных абонентов. Равноправия всех абонентов (как в шине) в данном случае нет. Обычно центральный компьютер самый мощный, именно на него возлагаются все функции по управлению обменом. Конфликты в сети с топологией «звезда» в принципе невозможны, так как управление полностью централизовано.

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

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

В отличие от шины, в звезде на каждой линии связи находятся только два абонента: центральный и один из периферийных. Чаще всего для их соединения используется две линии связи, каждая из которых передает информацию в одном направлении, т. е. на каждой линии связи имеется только один приемник и один передатчик. Это так называемая передача точка-точка. Все это существенно упрощает сетевое оборудование по сравнению с шиной и избавляет от необходимости применения дополнительных терминаторов.

Проблема затухания сигналов в линии связи также решается в звезде проще, чем в случае шины, ведь каждый приемник всегда получает сигнал одного уровня. Предельная длина сети с топологией «звезда» может быть вдвое больше, чем в шине.

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

Звезда, показанная на рисунке 1.2, носит название *активной звезды*. Существует также топология, называемая *пассивной звездой*, которая только внешне похожа на звезду. В настоящее время она распространена гораздо более широко, чем активная звезда, и используется в сети Ethernet. В центре сети с данной топологией помещается не компьютер, а специальное устройство – концентратор, который выполняет ту же функцию, что и репитер, т. е. восстанавливает приходящие сигналы и пересылает их во все другие линии связи. Пассивная звезда дороже обычной шины (так как в этом случае требуется еще и концентратор), однако она предоставляет целый ряд дополнительных возможностей, связанных с преимуществами звезды, в частности, упрощает обслуживание и ремонт сети. Именно поэтому в последнее время пассивная звезда все больше вытесняет истинную звезду, которая считается малоперспективной топологией.

Можно выделить также промежуточный тип топологии между активной и пассивной звездой. В этом случае концентратор не только ретранслирует поступающие на него сигналы, но и производит управление обменом, однако сам в обмене не участвует.

Большое достоинство звезды (как активной, так и пассивной) состоит в том, что все точки подключения собраны в одном месте. Это позволяет легко контролировать работу сети, локализовать неисправности путем

простого отключения от центра тех или иных абонентов, а также ограничивать доступ посторонних лиц к жизненно важным для сети точкам подключения. К периферийному абоненту в случае звезды может подходить как один кабель (по которому идет передача в обоих направлениях), так и два (каждый кабель передает в одном из двух встречных направлений), причем второй вариант встречается гораздо чаще.

Общим недостатком топологий типа «звезда» (как активной, так и пассивной) является значительно больший, чем при других топологиях, расход кабеля. Например, если компьютеры расположены в одну линию (см. рис. 1.2), то при выборе топологии «звезда» понадобится в несколько раз больше кабеля, чем при выборе топологии «шина». Это существенно влияет на стоимость сети в целом и заметно усложняет прокладку кабеля.

Кольцо – компьютеры последовательно объединены в кольцо. Передача информации в кольце всегда производится только в одном направлении. Каждый из компьютеров передает информацию только одному компьютеру, следующему в цепочке за ним, а получает информацию только от предыдущего в цепочке компьютера (рис. 1.3).

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

Важная особенность кольца состоит в том, что каждый компьютер ретранслирует (восстанавливает, усиливает) приходящий к нему сигнал, т. е. выступает в роли репитера. Затухание сигнала во всем кольце не имеет никакого значения, важно только затухание между соседними компьютерами кольца. На практике размеры

кольцевых сетей достигают десятков километров. Кольцо в этом отношении существенно превосходит любые другие топологии.

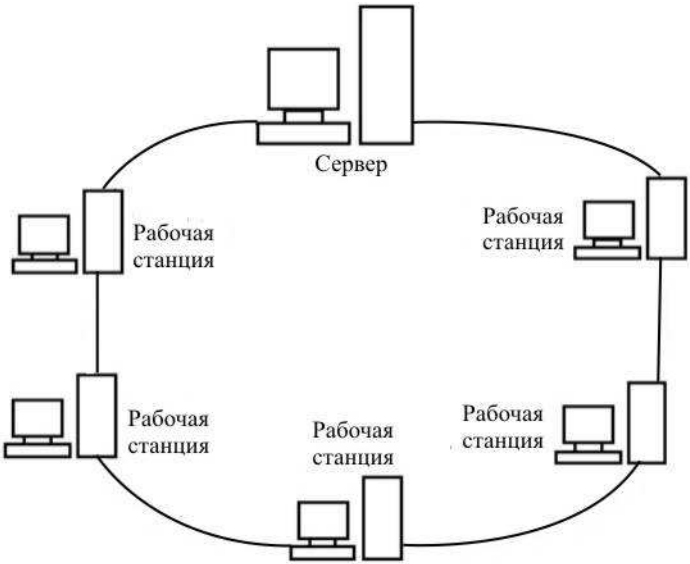

Рис. 1.3. Сетевая топология «кольцо»

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

Компьютеры в кольце не являются полностью равноправными (в отличие, например, от шинной топологии). Один из них обязательно получает информацию от компьютера, ведущего передачу в данный момент, раньше, а другие – позже. Именно на этой особенности топологии и строятся методы управления обменом по сети, специально рассчитанные на кольцо. В таких методах право

на следующую передачу переходит последовательно к следующему по кругу компьютеру. Подключение новых абонентов в кольцо выполняется достаточно просто, хотя и требует обязательной остановки работы всей сети на время подключения. Как и в случае шины, максимальное количество абонентов в кольце может быть довольно велико (до тысячи и больше). Кольцевая топология обычно обладает высокой устойчивостью к перегрузкам, обеспечивает уверенную работу с большими потоками передаваемой по сети информации, потому что в ней, как правило, нет конфликтов (в отличие от шины), а также отсутствует центральный абонент (в отличие от звезды), который может быть перегружен большими потоками информации.

Сигнал в кольце проходит последовательно через все компьютеры сети, поэтому выход из строя хотя бы одного из них (или же его сетевого оборудования) нарушает работу сети в целом. Это существенный недостаток кольца.

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

Иногда сеть с топологией «кольцо» выполняется на основе двух параллельных кольцевых линий связи, передающих информацию в противоположных направлениях, причем увеличивается скорость передачи информации по сети. К тому же при повреждении одного из кабелей сеть может работать с другим кабелем.

Кроме трех базовых широко распространена **древовидная сетевая топология** (рис. 1.4), которую можно рассматривать как комбинацию нескольких звезд, причем, как и в случае звезды, дерево может быть активным,

или истинным, и пассивным. При активном дереве в центрах объединения нескольких линий связи находятся центральные компьютеры, а при пассивном – концентраторы.

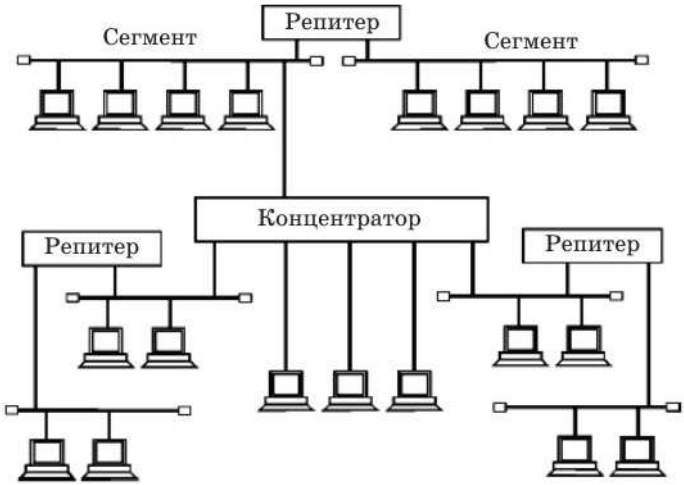

Рис. 1.4. Древовидная сетевая топология

Часто применяются и комбинированные топологии, среди которых наиболее распространены звездно-шинная и звездно-кольцевая.

В **звездно-шинной топологии** используется комбинация шины и пассивной звезды. К концентратору подключаются как отдельные компьютеры, так и целые шинные сегменты. 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, к которым, в свою очередь, с помощью звездообразных двойных линий связи подключаются компьютеры. 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, и данная топология равноценна классическому кольцу.

Сеточная топология – это топология, при которой компьютеры связываются между собой не одной, а многими линиями связи, образующими сетку.

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 – требует существенного усложнения сетевой аппаратуры, которая должна выбирать маршрут.

? *Контрольные вопросы и задания*

1. Дайте определение термину «компьютерная сеть». Раскройте основное назначение компьютерной сети.

2. Дайте определения основным понятиям раздела.

3. Опишите типы сетей.

4. Приведите классификацию сетей по территориальному признаку.

5. Перечислите основные типы сетей по способам соединения и управления.

6. Изложите основные факторы выбора сети.

7. Объясните отличия локальной сети от сети на основе сервера.

8. Опишите основные недостатки сетей.

9. Объясните, что собой представляет специализированный сервер, приведите пример.

10. Проанализируйте целесообразность выбора одноранговой сети.

11. Определите достоинства сетей на основе сервера.

12. Раскройте сущность понятия «топология сети».

13. Назовите основные факторы, влияющие на выбор топологии сети.

14. Перечислите основные топологии сети.

15. Определите наиболее характерное свойство для сети топологии «шина».

16. Выделите достоинства и недостатки топологий «шина», «звезда», «кольцо».

17. Объясните, в каких целях используются терминатор и репитер.

18. Проведите сравнительный анализ активной и пассивной звезд.

19. Создайте конструкцию звездно-кольцевой и звездно-шинной топологий.

20. Определите, в какой ситуации целесообразно использовать сеточную топологию.

21. Изучите предложенную ситуацию и найдите правильное решение.

В компании 8 человек; у каждого сотрудника свой персональный компьютер. Для того чтобы получить необходимую информацию, приходится обращаться к коллегам с устной просьбой или копировать данные с помощью флэш-накопителей. Все агенты занимаются делами только своих клиентов, и эта информация строго конфиденциальна.

Необходимо установить сеть для этой компании, выбрав оптимальные тип и топологию сети.

РАЗДЕЛ 2
ПОДКЛЮЧЕНИЕ СЕТЕВЫХ КОМПОНЕНТОВ

2.1. ОСНОВНЫЕ ВИДЫ КАБЕЛЕЙ

Линия связи состоит в общем случае из физической среды, по которой передаются информационные сигналы, аппаратуры передачи данных и промежуточной аппаратуры. На основе линии связи строится *канал связи*. В некоторой линии можно образовать несколько каналов связи, по каждому из которых передается своя информация. При этом говорят, что линия разделяется между несколькими каналами.

Физическая среда передачи данных может представлять собой *кабель* – набор проводов, изоляционных и защитных оболочек и соединительных разъемов, а также земную атмосферу или космическое пространство, через которые распространяются электромагнитные волны.

В зависимости от среды передачи данных линии связи подразделяются:

– на проводные (воздушные);

– кабельные (медные и волоконно-оптические);

– беспроводные (радиоканалы наземной и спутниковой связи).

Проводные линии связи представляют собой провода без изолирующих или экранирующих оплеток, проложенные между столбами и висящие в воздухе. По таким линиям связи традиционно передаются телефонные

или телеграфные сигналы, но при отсутствии других возможностей эти линии используются и для передачи компьютерных данных. Скоростные качества и помехозащищенность проводных линий очень низкие.

Кабельные линии состоят из проводников, заключенных в несколько слоев изоляции – электрической, электромагнитной, механической. Кроме того, кабель может быть оснащен разъемами, позволяющими быстро выполнять присоединение к нему различного оборудования.

Основными отличительными параметрами кабелей являются:

– диаметр проводников;

– диаметр проводника с изоляцией;

– количество проводников (пар);

– наличие экрана вокруг проводника (проводников);

– диаметр кабеля;

– диапазон температур, при котором качественные показатели находятся в норме;

– минимальный радиус изгиба, который допускается при прокладке кабеля;

– максимально допустимые наводки в кабеле;

– волновое сопротивление кабеля;

– максимальное затухание сигнала в кабеле.

В компьютерных сетях применяются три основных типа кабеля:

– кабели на основе скрученных пар медных проводов (витая пара);

– коаксиальные кабели с медной жилой;

– волоконно-оптические кабели.

Витая пара применяется для передачи слаботочных токов, несущих цифровую или аналоговую информацию, и является одним из самых распространенных типов кабеля связи. Кабель получил свое название из-за свитых попарно, изолированных друг от друга проводников. Скручивание проводов снижает влияние внешних помех на полезные

сигналы, передаваемые по кабелю. Витая пара существует в экранированном варианте – пара медных проводов обертывается в изоляционный экран, и неэкранированном – изоляционная обертка отсутствует (рис. 2.1).

Рис. 2.1. Витая пара

У каждой пары есть свой шаг скрутки, именно поэтому при передаче слаботочного электрического сигнала на расстояние до 150 м без использования ретранслятора достигаются такие высокие показатели. Практически все виды витой пары содержат внутреннюю нить, позволяющую легко избавлять кабель от внешней оболочки при подключении к коннекторам RJ 45 (для компьютерных сетей), RJ 11 (для телефонии) или другим соединяющим устройствам.

Существует множество видов витой пары с разным количеством проводников (1 пара – 2 проводника ... 500 пар – 1000 проводников), которые, в свою очередь, делятся на категории.

Основные виды витой пары в зависимости от категории и строения кабеля:

UTP (unfoiled twisted pair) – неэкранированная витая пара;

FTP (foiled twisted pair) – фольгированная;

STP (shielded unfoiled twisted pair) – защищенная неэкранированная;

SFTP (shielded foiled twisted pair) – защищенная экранированная.

Кабель UTP 3-й категории в основном служит для передачи аналогового сигнала в телефонии, однако случается, что он используется для передачи цифровой информации в компьютерных сетях на небольшие расстояния с относительно небольшой скоростью передачи.

Аналогом многопарного FTP категории 3 служит отечественный магистральный телефонный кабель для внешней прокладки на открытом воздухе, имеющий помехозащищающий экран.

Кабель UTP категории 5 и 5e предназначен для внутренней прокладки – это самый распространенный вид витой пары. Он имеет медные или омедненные одножильные или многожильные проводники толщиной от 0,48 до 0,52 мм^2. Изоляция и внешняя оболочка сделаны из ПВХ пластиката. UTP 5 может иметь 2, 4, 10... 300 пар проводников и может использоваться для подключения групп абонентов. Для подключения абонента к сети Интернет и для создания локальной компьютерной сети используется, как правило, UTP 2 или 4 пары, категории 5 и 5e, с медными или омедненными алюминиевыми проводниками. UTP 5e (специальная модель, которая имеет четыре пары обязательно медных проводников) получил наиболее широкое распространение среди провайдеров сети Интернет. При использовании изделий 5e и соблюдении особых условий инсталляции кабеля и оборудования провайдеры добиваются подключения абонента на скорости передачи данных 100 Мбит/с и больше. Для менее требовательных абонентов провайдеры могут использовать более экономичный вариант UTP 5-й категории – 2 пары с медными или омедненными проводниками, а также 4-парный с омедненными

алюминиевыми жилами. Для подключения абонента на скорости 2 Мбит/с достаточно использовать вариант 3-й категории.

Существует кабель UTP категории 5 и 5е для внешней прокладки, который соответственно применяется на открытом воздухе. Он имеет особую внешнюю оболочку из полиэтилена, устойчивую к низким температурам, обледенению, а также к прямому воздействию солнечных лучей. Вариант категории 5 и 5е имеет внешнюю оболочку черного цвета. За счет повышенной выносливости менее гибок, чем вариант для внутренней прокладки.

Кабель FTP категории 5 и 5е для внутренней прокладки – данный тип имеет экран из фольги, который защищает передаваемый сигнал от внешнего электромагнитного воздействия. FTP категории 5 может иметь омедненные алюминиевые жилы, изоляцию и оболочку из ПВХ пластиката, медные жилы. FTP может быть 2- и 4-парный; не подходит для передачи аналогового сигнала в видеонаблюдении, так как защитный экран может создать помеху для аналогового сигнала. FTP категории 5 и 5е для внешней прокладки – данная модификация имеет внешнюю оболочку из светостабилизированного полиэтилена, что позволяет прокладывать его на открытом воздухе с возможным прямым воздействием солнечных лучей. FTP категории 5, 5е внешние не рекомендуется подвешивать с большими пролетами без дополнительного троса, так как провод может подвергнуться значительным растягивающим усилиям за счет собственного веса или дополнительного обледенения в зимний период.

Кабель STP категории 5е – вариант защищенной неэкранированной витой пары. STP имеет 4 пары медных проводников, изоляцию и оболочку из ПВХ пластиката, а также индивидуальные экраны из фольги. Экраны в STP защищают сигнал от возможных внешних электромагнитных помех.

Кабель UTP категории 6, 6a, 4 пары – неэкранированная витая пара, сечение жил 0,57 мм^2, имеет внутренний пластиковый корд, разделяющий его внутреннее пространство на секторы, в каждом из которых располагается отдельная пара проводников.

Кабель SFTP категории 7 – защищенная экранированная витая пара. SFTP 7 имеет 4 пары медных проводников, оболочку и изоляцию из ПВХ пластиката, помимо общего экрана – индивидуальный алюминиевый экран. Благодаря отличной помехозащищенности SFTP присвоена 7-я категория.

Любая модификация витой пары бывает с маркировкой LsZh (Low smoke Zero halogen) – пониженное безгалогеновое дымовыделение при горении. Наиболее распространен UTP категории 5e, 4 pairs LsZh. Он удовлетворяет повышенным требованиям пожарной безопасности на особых объектах. Оболочка в LsZh сделана из специального ПВХ пластиката низкой горючести. LsZh не распространяет горения при групповой прокладке однотипных с ним кабелей.

Коаксиальный кабель имеет несимметричную конструкцию и состоит из внутренней медной жилы и оплетки, отделенной от жилы слоем изоляции (рис. 2.2).

Рис. 2.2. Коаксиальный кабель: *1* – центральный проводник CCS; *2* – диэлектрическая прослойка из полиуретана; *3* – экран из алюминиевой фольги; *4* – экран из алюминиевой проволоки; *5* – оболочка из УФ-стабилизированного ПВХ

Существует несколько типов коаксиального кабеля, отличающихся характеристиками и областями применения:

– для локальных сетей;

– глобальных сетей;

– кабельного телевидения.

Коаксиальный кабель классифицируют по следующим признакам:

• по *назначению*:

– кабель для систем кабельного телевидения;

– для систем связи;

– авиационной, космической техники;

– компьютерных сетей;

– бытовой техники и т. д.;

• по *волновому сопротивлению* – стандартными являются пять значений:

– 50 Ом – наиболее распространенный тип, применяется в разных областях радиоэлектроники;

– 75 Ом – распространенный тип, применяется преимущественно в телевизионной и видеотехнике;

– 100 Ом – применяется редко, в импульсной технике и для специальных целей;

– 150 Ом – применяется редко, в импульсной технике и для специальных целей, международными стандартами не предусмотрен;

– 200 Ом – применяется крайне редко, международными стандартами не предусмотрен;

• по *диаметру изоляции*:

– на субминиатюрные – до 1 мм;

– миниатюрные – 1,5...2,95 мм;

– среднегабаритные – 3,7...11,5 мм;

– крупногабаритные – более 11,5 мм;

• по *гибкости* (стойкость к многократным перегибам и механический момент изгиба кабеля):

– жесткие;

– полужесткие;

– гибкие;

– особо гибкие;

• по *степени экранирования*:

– со сплошным экраном;

– с экраном из металлической трубки;

– с экраном из луженой оплетки;

– с обычным экраном;

– с однослойной оплеткой;

– с двух- и многослойной оплеткой и с дополнительными экранирующими слоями;

– излучающие кабели, имеющие намеренно низкую (и контролируемую) степень экранирования.

Волоконно-оптический кабель состоит из тонких (5...60 микрон) волокон, по которым распространяются световые сигналы (рис. 2.3). Это наиболее качественный тип кабеля – он обеспечивает передачу данных с очень высокой скоростью (до 10 Гбит/с и выше) и к тому же лучше других типов передающей среды обеспечивает защиту данных от внешних помех.

Рис. 2.3. Волоконно-оптический кабель

Оптические волокна могут быть классифицированы по двум параметрам:

• *материал, из которого сделано волокно*:

– стеклянные волокна – имеют как стеклянную сердцевину, так и стеклянную оптическую оболочку. Стекло, используемое в данном типе волокон, состоит из сверхчистого сверхпрозрачного диоксида кремния или плавленого кварца. В стекло добавляют примеси, чтобы получить требуемый показатель преломления. Примеси

влияют также на свойства волокна, увеличивая затухание, обусловленное рассеянием и поглощением света;

– стеклянные волокна с пластиковой оптической оболочкой – имеют стеклянную сердцевину и пластиковую оптическую оболочку;

– пластические волокна – имеют пластиковую сердцевину и пластиковую оптическую оболочку. По сравнению с другими видами волокон пластиковые имеют ограниченные возможности с точки зрения затухания и полосы пропускания. Однако низкая себестоимость и простота использования делают их привлекательными там, где требования к величинам затухания и полосе пропускания не столь высоки;

• *вид профиля показателя преломления сердцевины и модовая структура света в ней.*

Мода – математическое и физическое понятие, связанное с процессом распространения электромагнитных волн в среде. Под модой достаточно понимать вид траектории, вдоль которой может распространяться свет. Число мод, допускаемых волокном, колеблется от 1 до 100 000. Таким образом, волокно позволяет свету распространяться по множеству траекторий, число которых зависит от размера и свойств волокна.

Тип оптического волокна идентифицируется по типу путей, или мод, проходимых светом в ядре волокна. Существует два основных типа волокна – многомодовое MMF (multi mode fiber) и одномодовое SMF (single mode fiber) (рис. 2.4).

Волокна отличаются диаметром сердцевины и оболочки, а также профилем показателя преломления сердцевины. *Многомодовое волокно* с относительно большой сердцевиной допускает распространение по нему нескольких или многих мод. *Одномодовое волокно* проектируется так, что в нем может распространяться только одна мода. Одномодовое волокно в отличие от многомодо-

вого имеет значительно меньший диаметр сердцевины, что позволяет распространяться по ней только одному пучку или моде света. Вследствие этого устраняются все искажения оптического сигнала, распространяющегося по одномодовому волокну, связанные с межмодовым взаимодействием.

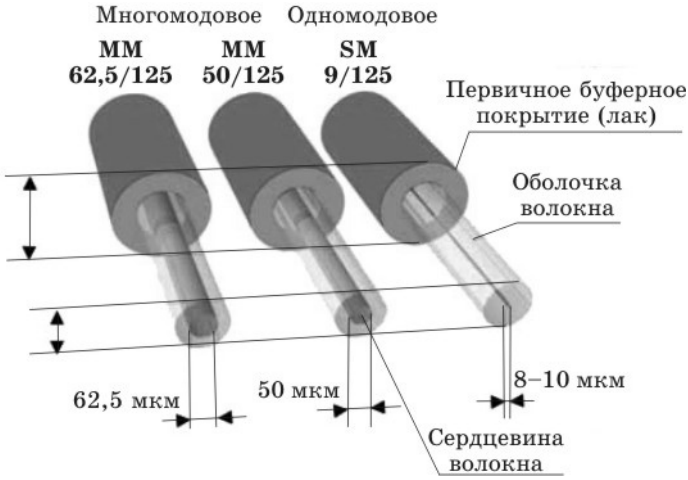

Рис. 2.4. Многомодовое и одномодовое волокно

Основные характеристики описанных кабелей приведены в таблице.

Таблица

Характеристики кабелей

Тип кабеля	Скорость передачи данных	Максимальная длина сегмента, м	Возможность восстановления при повреждении / наращивание длины	Подверженность помехам
Неэкранированная витая пара	100/10/1000 Мбит/с	100	Хорошая	Средняя
Экранированная витая пара	100/10/1000 Мбит/с	100	Хорошая	Низкая
Тонкий коаксиальный кабель	10 Мбит/с	185	Требуется пайка	Высокая

Окончание табл.

Тип кабеля	Скорость передачи данных	Максимальная длина сегмента, м	Возможность восстановления при повреждении / наращивание длины	Подверженность помехам
Толстый коаксиальный кабель	10 Мбит/с	500	Требуется пайка	Высокая
Оптоволоконный кабель	1–2 Гбит	2000	Требуется специальное оборудование	Отсутствует

В компьютерных сетях сегодня применяются практически все описанные типы физических сред передачи данных, но наиболее перспективными являются волоконно-оптические. На них сегодня строятся как магистрали крупных территориальных сетей, так и высокоскоростные линии связи локальных сетей. Популярной средой является также витая пара, которая характеризуется отличным соотношением качества и стоимости, а также простотой монтажа. С помощью витой пары обычно подключают конечных абонентов сетей на расстоянии до 100 м от концентратора. Спутниковые каналы и радиосвязь используются чаще всего в тех случаях, когда кабельные связи применить нельзя, например, при прохождении канала через малонаселенную местность или же для связи с мобильным пользователем сети.

2.2. ХАРАКТЕРИСТИКИ ЛИНИЙ СВЯЗИ

К основным характеристикам линий связи относятся:
амплитудно-частотная характеристика;
полоса пропускания;
затухание;
помехоустойчивость;
перекрестные наводки на ближнем конце линии;
пропускная способность;
достоверность передачи данных.

Амплитудно-частотная характеристика показывает, как затухает амплитуда синусоиды на выходе линии связи по сравнению с амплитудой на ее входе для всех возможных частот передаваемого сигнала. Знание амплитудно-частотной характеристики реальной линии позволяет определить форму выходного сигнала практически для любого входного сигнала.

На практике вместо амплитудно-частотной характеристики применяются другие, упрощенные характеристики, например полоса пропускания и затухание.

Полоса пропускания – это непрерывный диапазон частот, для которого отношение амплитуды выходного сигнала к входному превышает некоторый заранее заданный предел (обычно 0,5), т. е. полоса пропускания определяет диапазон частот синусоидального сигнала, при которых этот сигнал передается по линии связи без значительных искажений.

Затухание определяется как относительное уменьшение амплитуды или мощности сигнала при передаче по линии сигнала определенной частоты.

В компьютерных сетях применяются кабели, удовлетворяющие определенным стандартам, что позволяет строить кабельную систему сети из кабелей и соединительных устройств разных производителей.

2.3. СЕТЕВОЙ АДАПТЕР

Плата сетевого адаптера (ПСА) выступает в качестве физического интерфейса между компьютером и средой передачи. Плата сетевого адаптера состоит из аппаратной части и встроенных программ, записанных в постоянное запоминающее устройство.

Плату вставляют в слоты расширения всех сетевых компьютеров и серверов или интегрируют на материнскую плату (рис. 2.5).

Рис. 2.5. Плата сетевого адаптера

Для того чтобы обеспечить физическое соединение между персональным компьютером и сетью, к соответствующему разъему или порту платы подключается сетевой кабель.

Назначение платы сетевого адаптера:

– подготовка данных, поступающих от персонального компьютера, к передаче по сетевому кабелю;

– передача данных другому персональному компьютеру;

– управление потоком данных между компьютером и кабелем.

Плата принимает данные с кабеля и приводит их в форму, понятную центральному процессору персонального компьютера. Перед тем как послать данные в сеть, плата сетевого адаптера должна перевести их из формы, понятной персональному компьютеру, в форму, в которую они могут передаваться по сетевому кабелю. В сетевом кабеле данные должны перемещаться в виде потока битов.

Плата сетевого адаптера принимает параллельные данные и организует их для последовательной, побитовой передачи. Этот процесс завершается переводом цифровых данных персонального компьютера в электрические и оптические сигналы, передающиеся по сетевым

кабелям. За это преобразование отвечает **трансивер** – приемопередатчик.

Помимо преобразования данных плата должна указать свое месторасположение и адрес, чтобы ее могли отличать от остальных плат.

При приеме данных от компьютера и подготовке к передаче по сетевому кабелю плата сетевого адаптера выполняет и другие действия:

• персональный компьютер и плата сетевого адаптера должны быть связаны друг с другом, чтобы осуществлять передачу данных. Если плата может использовать прямой доступ к памяти, то компьютер выделяет ей некоторую область своей памяти;

• плата запрашивает у компьютера данные;

• шина компьютера передает данные из его памяти плате сетевого адаптера.

Часто данные поступают быстрее, чем их способна передать плата сетевого адаптера, поэтому временно они помещаются в буфер.

Перед тем как послать данные в сеть, плата проводит электронный диалог с принимающей платой, во время которого они оговаривают:

максимальный размер блока передаваемых данных;

объем данных, передаваемых без подтверждения о получении;

интервалы между передачами блоков данных;

интервал, в течение которого необходимо послать подтверждение;

объем данных, который может принять каждая плата без переполнения буфера;

скорость передачи.

Для правильной работы платы сетевого адаптера должны быть корректно установлены ее параметры:

– номер прерывания (посылая компьютеру запрос, плата сетевого адаптера организует *прерывание* – элек-

трический сигнал, который направляется центральному процессору компьютера);

– базовый адрес порта ввода/вывода;

– базовый адрес памяти;

– тип трансивера (необходимо указать трансивер, который будет использоваться, так как платы сетевого адаптера могут иметь как встроенные, так и внешние трансиверы).

Параметры платы сетевого адаптера задаются в программном обеспечении; они должны совпадать с установками, заданными на плате перемычками.

Схемы современных плат сетевого адаптера позволяют им приспособиться к медленной скорости старых плат. Каждая плата оповещает другую о своих параметрах, принимая «чужие» параметры и подстраиваясь к ним. После того как все детали определены, платы начинают обмен данными.

Для того чтобы обеспечить совместимость персонального компьютера и сети, плата сетевого адаптера должна отвечать следующим требованиям:

– соответствовать внутренней структуре персонального компьютера;

– иметь соединитель подключения сетевого кабеля.

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

1) организует физическое соединение с кабелем;

2) генерирует электрические и световые сигналы, передаваемые по кабелю;

3) следует определенным правилам, регламентирующим доступ к сетевому кабелю.

Прежде чем выбрать плату, подходящую для сети, необходимо установить тип кабелей и соединителей.

Каждый тип кабелей имеет различные физические характеристики, которым должна соответствовать пла-

та. Поэтому она рассчитана для работы с определенным типом кабеля (коаксиальным, витой парой или оптоволокном).

Некоторые платы сетевого адаптера имеют несколько типов соединителей. Например, есть платы, разъемы которых подходят для тонкого и толстого коаксиальных кабелей или для витой пары и толстого коаксиального кабеля.

Сетевым адаптерам (как и другим аппаратным устройствам) требуется драйвер для коммуникации с операционной системой.

Для подключения *внешних сетевых адаптеров* не нужно вскрывать компьютер или прокладывать к нему дома специальные сетевые кабели. Достаточно подсоединить внешний адаптер к порту USB на задней панели компьютера. Использование внешних сетевых адаптеров – это самый быстрый и простой способ установки домашней сети.

Внутренний сетевой адаптер устанавливается в гнездо расширения внутри компьютера. Большинство компьютеров оборудуются несколькими гнездами расширения PCI, что позволяет увеличивать возможности компьютера, добавляя новые компоненты оборудования, в частности, сетевые адаптеры.

Плата сетевого адаптера оказывает существенное влияние на передачу данных, поэтому от платы зависит производительность всей сети. Факторы, от которых зависит скорость передачи данных:

– прямой доступ к памяти. Данные напрямую передаются из буфера платы в память компьютера, не затрагивая при этом центральный процессор;

– разделяемая память адаптера. Плата имеет собственную оперативную память и использует ее совместно с персональным компьютером, который воспринимает эту память как часть собственной;

– разделяемая системная память. Процессор платы сетевого адаптера использует для обработки данных часть памяти компьютера;

– управление шиной. К плате сетевого адаптера временно переходит управление шиной компьютера, и, минуя центральный процессор, она передает данные непосредственно в его системную память;

– встроенный микропроцессор. Большинство сетевых плат имеют свои микропроцессоры, которые увеличивают скорость выполнения сетевых операций;

– буферизация. Для большинства плат сетевого адаптера современные скорости передачи данных по сети слишком велики, поэтому на них устанавливают *буфер* (микросхемы памяти). В случае, когда плата принимает данных больше, чем способна обработать, буфер хранит их до тех пор, пока они не будут обработаны. Буфер повышает производительность платы, не давая ей стать узким местом системы.

Специализированные платы сетевого адаптера – *платы беспроводных сетей*. Они разработаны для большинства сетевых операционных систем и могут быть использованы:

- для построения беспроводных локальных сетей;
- для беспроводного подключения станций к кабельной локально-вычислительной сети.

Платы беспроводных сетей применяются вместе с так называемым *беспроводным концентратором*. Это устройство функционирует как трансивер – для передачи и приема сигналов.

Существуют платы сетевого адаптера, снабженные специальной микросхемой постоянного запоминающего устройства удаленной загрузки, которая содержит код для загрузки компьютера и для подключения его к сети. Они применяются в тех случаях, когда необходимо иметь

другой источник загрузки программного обеспечения, запускающего компьютер и подключающего его к сети.

Работа сетевых адаптеров с конвейерной схемой обработки кадров заключается в том, что процессы приема кадра из оперативной памяти компьютера и передачи его в сеть совмещаются во времени. Таким образом, после приема первых нескольких байтов кадра начинается их передача. Это существенно (на 25...55 %) повышает производительность цепочки «оперативная память → адаптер → физический канал → адаптер → оперативная память». Эта схема очень чувствительна к порогу начала передачи, т. е. к количеству байтов кадра, которое загружается в буфер адаптера перед началом передачи в сеть. Такой сетевой адаптер 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.

В серверных вариантах сетевых адаптеров обязательно наличие мощного процессора, разгружающего центральный процессор. В них входит интегральная схема, выполняющая функции уровня доступа к среде; скорость развита до 1 Гбит/с; имеется большое количество высокоуровневых функций (поддержка агента удаленного мониторинга, схема приоритизации кадров, функции дистанционного управления компьютером).

? *Контрольные вопросы и задания*

1. Дайте определение термину «линия связи».
2. Определите физическую среду передачи данных.
3. Приведите классификацию линий связи в зависимости от среды передачи.

4. Перечислите основные характеристики линий связи.

5. Назовите основные виды кабелей.

6. Охарактеризуйте основные виды витой пары.

7. Приведите классификацию коаксиальных кабелей.

8. Приведите классификацию оптоволоконного кабеля в зависимости от материала изготовления волокна.

9. Охарактеризуйте многомодовые и одномодовые волокна.

10. Сравните достоинства и недостатки витой пары, оптоволоконных и коаксиальных кабелей.

11. Определите, в каких ситуациях применяется:

а) витая пара;

б) коаксиальный кабель;

в) волоконно-оптический кабель.

12. Назовите тип кабеля, наиболее устойчивого к радио- и электромагнитным помехам.

13. Дайте определение термину «плата сетевого адаптера».

14. Изложите основное назначение платы сетевого адаптера.

15. Опишите основные действия плат сетевого адаптера при приеме-передаче данных.

16. Определите, что обеспечивает драйвер сетевого адаптера в сетевой среде.

17. Проведите сравнительный анализ плат сетевого адаптера.

РАЗДЕЛ 3
ФУНКЦИОНИРОВАНИЕ СЕТИ

3.1. ЭТАЛОННАЯ МОДЕЛЬ ВЗАИМОДЕЙСТВИЯ ОТКРЫТЫХ СИСТЕМ (МОДЕЛЬ OSI)

Основу компьютерной сети составляет соединение различного оборудования, где одной из наиболее острых проблем является проблема совместимости. Без принятия всеми производителями общепринятых правил (стандартов) создания сетевого оборудования построение сетей в целом было бы невозможно. В компьютерных сетях идеологической основой стандартизации является многоуровневый подход к разработке средств сетевого взаимодействия. Именно на основе этого подхода была разработана стандартная (эталонная) семиуровневая модель взаимодействия открытых систем, ставшая своего рода универсальным языком сетевых специалистов.

Открытой системой может быть названа любая система (компьютер, вычислительная сеть, операционная система, программный пакет, другие аппаратные и программные продукты), которая построена в соответствии с открытыми спецификациями.

Под термином **спецификация** в вычислительной технике понимают формализованное описание аппаратных или программных компонентов, способов их функционирования, взаимодействия с другими компонентами, условий эксплуатации, ограничений и особых характеристик.

В свою очередь, под *открытыми спецификациями* понимают опубликованные, общедоступные спецификации, соответствующие стандартам и принятые в результате достижения согласия после всестороннего обсуждения всеми заинтересованными сторонами.

Организация взаимодействия между устройствами в сети является сложной задачей, которая разбивается на несколько более простых задач-модулей. Процедура разбиения (декомпозиции) включает четкое определение функций каждого модуля, решающего отдельную задачу, и интерфейсов между ними. В результате достигается логическое упрощение задачи, а также появляется возможность модификации отдельных модулей без изменения остальной части системы.

При декомпозиции часто используют многоуровневый подход. Он заключается в следующем. Все множество модулей разбивают на уровни. Уровни образуют иерархию, т. е. имеются вышележащие и нижележащие уровни. Множество модулей, составляющих каждый уровень, сформировано таким образом, что для выполнения своих задач они обращаются с запросами только к модулям непосредственно примыкающего нижележащего уровня. С другой стороны, результаты работы всех модулей, принадлежащих некоторому уровню, могут быть переданы только модулям соседнего вышележащего уровня. Такая иерархическая декомпозиция задачи предполагает четкое определение функции каждого уровня и интерфейсов между уровнями.

Интерфейс определяет набор функций, которые нижележащий уровень предоставляет вышележащему. Существуют логические и физические интерфейсы. *Физический интерфейс* – это способ электрического и механического сопряжения ЭВМ и локальных устройств управления. *Логический интерфейс* – это способ передачи информации (протокол обмена информацией) по каналу связи: способ

установления и прекращения сеансов связи, размер передаваемых сообщений.

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

Модули, реализующие протоколы соседних уровней и находящиеся в одном узле, также взаимодействуют друг с другом в соответствии с четко определенными правилами и с помощью стандартизованных форматов сообщений.

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

Модель взаимодействия открытых систем определяет различные уровни взаимодействия систем, дает им стандартные имена и указывает, какие функции должен выполнять каждый уровень. Модель OSI имеет семь уровней (рис. 3.1).

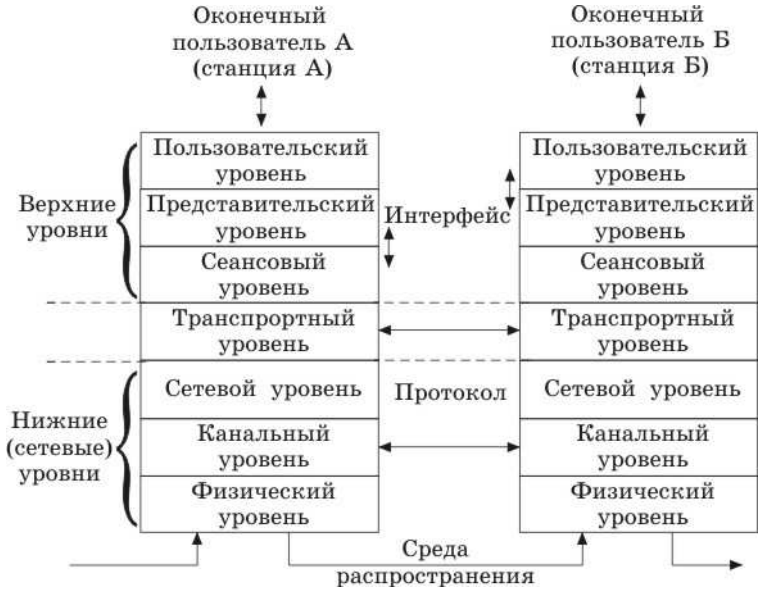

Рис. 3.1. Эталонная модель взаимодействия открытых систем

Структура модели предполагает, что:

– уровень должен быть создан по мере необходимости отдельного уровня абстракции;

– каждый уровень должен выполнять определенную функцию;

– выбор функций для каждого уровня осуществляется с учетом создания протоколов;

– границы между уровнями должны быть выбраны так, чтобы поток данных между интерфейсами был минимальным;

– количество уровней должно быть таким, чтобы архитектура не становилась громоздкой.

Физический уровень связан с передачей битов по физическим каналам связи, таким, например, как коаксиальный кабель, витая пара, оптоволоконный кабель или цифровой территориальный канал. К этому уровню имеют отношение характеристики физических сред передачи данных – полоса пропускания, помехозащищенность, волновое сопротивление и др.

Функции физического уровня реализуются во всех устройствах, подключенных к сети. Со стороны компьютера функции физического уровня выполняются сетевым адаптером или последовательным портом.

Канальный уровень. В некоторых сетях линии связи используются (разделяются) попеременно несколькими парами взаимодействующих компьютеров, и физическая среда передачи может быть занята. Поэтому одной из задач канального уровня является проверка доступности среды передачи. Другой задачей канального уровня выступает реализация механизмов обнаружения и коррекции ошибок. Для этого на канальном уровне биты группируются в наборы, называемые *кадрами*. Канальный, уровень обеспечивает корректность передачи каждого кадра, помещая специальную последовательность битов в начало и конец каждого кадра для его выделения, а также

вычисляет контрольную сумму, обрабатывая все байты кадра. При приходе кадра по сети получатель опять вычисляет контрольную сумму полученных данных и сравнивает результат с контрольной суммой из кадра – если они совпадают, кадр считается правильным и принимается; если контрольные суммы не совпадают, то фиксируется ошибка. Канальный уровень может не только обнаруживать ошибки, но и исправлять их за счет повторной передачи поврежденных кадров.

Сетевой уровень служит для образования единой транспортной системы, объединяющей несколько сетей, причем эти сети могут использовать различные принципы передачи между конечными узлами и обладать произвольной структурой связей.

Сетевой уровень решает также задачи согласования разных технологий, упрощения адресации в крупных сетях и создания надежных и гибких барьеров на пути нежелательного трафика между сетями. Сообщения сетевого уровня называют *пакетами*.

Транспортный уровень обеспечивает приложениям или верхним уровням стека – прикладному и сеансовому – передачу данных с той степенью надежности, которая им требуется. Модель OSI определяет пять классов сервиса, предоставляемых транспортным уровнем. Эти виды сервиса отличаются 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.

Сеансовый уровень обеспечивает управление диалогом: фиксирует, какая из сторон является активной в настоящий момент, предоставляет средства синхрониза-

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

Представительный уровень имеет дело с формой представления передаваемой по сети информации, не меняя при этом ее содержания. За счет уровня представления информация, передаваемая прикладным уровнем одной системы, всегда понятна прикладному уровню другой системы. С помощью средств данного уровня протоколы прикладных уровней могут преодолеть синтаксические различия в представлении данных или же различия в кодах символов. На этом уровне может выполняться шифрование и дешифрование данных, благодаря которому секретность обмена данными обеспечивается сразу для всех прикладных служб.

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

Функции всех уровней модели OSI могут быть отнесены к одной из двух групп: либо к функциям, зависящим от конкретной технической реализации сети, либо к функциям, ориентированным на работу с приложениями.

Три нижних уровня – физический, канальный и сетевой – являются сетезависимыми, т. е. протоколы этих

уровней тесно связаны с технической реализацией сети и используемым коммуникационным оборудованием.

Три верхних уровня – прикладной, представительный и сеансовый – ориентированы на приложения и мало зависят от технических особенностей построения сети. На протоколы эти уровней не влияют изменения в топологии сети, замена оборудования или переход на другую сетевую технологию.

Транспортный уровень является промежуточным, он скрывает все детали функционирования нижних уровней от верхних. Это позволяет разрабатывать приложения, не зависящие от технических средств непосредственной транспортировки сообщений.

Компьютер с установленной на нем сетевой операционной системой взаимодействует с другим компьютером с помощью протоколов всех семи уровней. Это взаимодействие компьютеры осуществляют опосредованно через различные коммуникационные устройства: концентраторы, модемы, мосты, коммутаторы, маршрутизаторы, мультиплексоры. В зависимости от типа коммуникационное устройство может работать либо только на физическом уровне (*повторитель*), либо на физическом и канальном (*мост*), либо на физическом, канальном и сетевом, иногда захватывая и транспортный уровень (*маршрутизатор*).

В модели OSI различают два основных типа протоколов. В протоколах с установлением соединения перед обменом данными отправитель и получатель должны сначала установить соединение и, возможно, выбрать некоторые параметры протокола, которые они будут использовать при обмене данными. После завершения диалога они должны разорвать это соединение.

Вторая группа протоколов – протоколы без предварительного установления соединения. Отправитель просто передает сообщение, когда оно готово. При взаимо-

действии компьютеров используются протоколы обоих типов.

3.2. IEEE PROJECT-802. МНОГОУРОВНЕВАЯ АРХИТЕКТУРА

В 1980 г. в институте IEEE был организован комитет 802 по стандартизации локальных сетей, в результате работы которого было принято семейство стандартов IEEE 802.X, содержащее рекомендации по проектированию нижних уровней локальных сетей.

Стандарты 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. Черты старших уровней (начиная с сетевого) в значительной степени общие как для локальных, так и для глобальных сетей.

Специфика локальных сетей также нашла свое отражение в разделении канального уровня на два подуровня (которые часто тоже называют уровнями):

- логической передачи данных (LLC) – скрывает различия между типами сетей, представляя сетевому уровню единый формат и интерфейс;
- управления доступом к среде (MAC).

Уровень с доступом к среде появился из-за существования в локальных сетях разделяемой среды передачи данных. Именно этот уровень обеспечивает корректное совместное использование общей среды, предоставляя ее в соответствии с определенным алгоритмом в распоряжение той или иной станции сети. После того как доступ к среде получен, ею может пользоваться более высокий уровень – уровень логической передачи данных, организующий передачу логических единиц данных, кадров информации с различным уровнем качества транспортных услуг. В современных локальных сетях получили рас-

пространение несколько протоколов уровня управления доступом к среде, реализующих различные алгоритмы доступа к разделяемой среде. Эти протоколы полностью определяют специфику таких технологий, как Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI.

Уровень логической передачи данных отвечает за передачу кадров данных между узлами с различной степенью надежности, а также реализует функции интерфейса с прилегающим к нему сетевым уровнем. Именно через этот уровень сетевой протокол запрашивает у канального уровня нужную ему транспортную операцию с нужным качеством. На нем существует несколько режимов работы, отличающихся наличием или отсутствием на этом уровне процедур восстановления кадров в случае их потери или искажения, т. е. отличающихся качеством транспортных услуг этого уровня.

Протоколы уровней управления доступом к среде и логической передачи данных взаимно независимы – каждый протокол одного уровня может применяться с любым протоколом другого уровня и наоборот.

Основные стандарты IEEE 802 приведены в таблице.

Таблица

Основные стандарты 802

Номер стандарта	Описание
802.1	Общее представление и архитектура локальных вычислительных сетей
802.2	Управление логической передачей данных
802.3	Ethernet с методом доступа – множественный доступ с контролем несущей и обнаружением коллизий (CSMA/CD);
802.4	Локальные сети с методом доступа «маркерная шина» (Token Bus)
802.5	Локальные сети с методом доступа «маркерное кольцо» (Token Ring)
802.6	Двойная двунаправленная шина (региональные сети)
802.7	Техническая консультационная группа по широкополосной передаче

Окончание табл.

Номер стандарта	Описание
802.8	Техническая консультационная группа по волоконно-оптическим сетям
802.9	Изохронные локальные вычислительные сети (для приложений реального времени)
802.10	Виртуальные локальные вычислительные сети и сетевая безопасность
802.11	Беспроводные локально-вычислительные сети
802.12	Локальные сети с методом доступа по требованию с приоритетами
802.14	Кабельные модемы
802.15	Персональные сети (Bluetooth)
802.16	Широкополосные беспроводные локальные вычислительные сети
802.17	Гибкая технология пакетного кольца

3.3. ДРАЙВЕРЫ

Связь сетевого адаптера с сетевым программным обеспечением осуществляют драйверы сетевых адаптеров. **Драйвер** – это программа, обеспечивающая обмен данными с подключенным оборудованием, с одной стороны, и с клиентским программным обеспечением – с другой.

Назначение драйвера – избавить разработчиков пользовательского программного обеспечения от рутинной реализации протоколов работы с оборудованием и предоставить дополнительный сервис и удобные средства по настройке и управлению устройствами.

Именно благодаря драйверу компьютер может не знать никаких аппаратных особенностей адаптера (его адресов, правил обмена с ним, его характеристик). Драйвер унифицирует, делает единообразным взаимодействие программных средств высокого уровня с любым адаптером данного класса. Сетевые драйверы, поставляемые вместе с сетевыми адаптерами, позволяют сетевым программам одинаково работать с платами разных поставщиков и даже с пла-

тами разных локальных сетей. В стандартной модели OSI драйверы, как правило, выполняют функцию канального уровня, хотя иногда реализуют и часть функций сетевого уровня. Например, драйверы формируют передаваемый пакет в буферной памяти адаптера, читают из этой памяти пришедший по сети пакет, дают команду на передачу, информируют компьютер о приеме пакета.

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

Прежде чем приобрести плату адаптера, необходимо ознакомиться со списком совместимого оборудования, который публикуют все производители сетевых операционных систем.

Организация взаимодействия клиентского программного обеспечения с оборудованием является важным моментом – нецелесообразно встраивать поддержку аппаратуры непосредственно в прикладную программу. Разработчики прикладных программ не в состоянии отслеживать изменения в номенклатуре подключаемых устройств, а также в модификациях этих устройств – перечень устройств и их возможностей постоянно меняется.

Архитектура драйверов представляет собой DLL-модули для MS Windows 98/NT/2000/XP/2003/Vista/7. DLL-модули драйверов могут использоваться как OLE Automation сервер (COM-объект). Данная архитектура драйверов позволяет без проблем использовать их в любых Windows-средах.

Архитектура драйверов позволяет управлять устройствами, подключенными к удаленному персональному компьютеру локальной сети. Для организации сетевой работы клиентского программного обеспечения с удаленным оборудованием через локальную сеть нет необходи-

мости менять программный код клиентского программного обеспечения. Работа с удаленным устройством ведется так же, как если бы оно было подключено к данному клиентскому персональному компьютеру.

Для *настройки драйверов* используется визуальная страница свойств, облегчающая работу с подключенными устройствами. На странице свойств можно легко настроить нужные параметры работы с оборудованием (порт подключения, скорость передачи данных и т. д.) и проверить правильность выставленных настроек. Это избавит пользователя от необходимости программировать параметры работы с оборудованием в клиентском программном обеспечении, хотя полностью и не исключит такой возможности. Драйверы обеспечивают автоматическое сохранение и восстановление настроек для работы с подключенными устройствами.

Для быстрого подключения устройств в драйверах реализована возможность поиска подключенного оборудования. После запуска поиска драйвер опрашивает все необходимые внешние порты персонального компьютера. При нахождении готового к работе устройства драйвер самостоятельно определит порт подключения, скорость подключения и другие параметры связи. Для поиска устройств реализовано удобное и простое диалоговое окно.

Драйверы могут работать с несколькими устройствами с одного рабочего места, для чего реализован механизм логических устройств. Логическое устройство представляет собой набор значений свойств драйвера (параметров соединения и др.) для работы с конкретным физическим устройством, который может быть сохранен и в дальнейшем восстановлен. Данная технология позволяет хранить заготовки настроек для разных устройств, подключенных к данному компьютеру, и оперативно переключать их для работы с нужным устройством. Визуально, на странице свойств драйвера, или программным

образом – с помощью методов и свойств можно создать и настроить нужное количество логических устройств и подключать оборудование, используя предопределенные параметры соединения.

Драйверы разработаны таким образом, что при подключении оборудования другой модели нет необходимости изменять или дописывать приложение. Достаточно поменять модель оборудования на визуальной странице свойств драйвера или установить новую модель через его свойства. Драйвер проанализирует подключенное устройство и автоматически адаптируется для работы с ним.

3.4. ПЕРЕДАЧА СИГНАЛОВ ПО СЕТИ. ФУНКЦИИ, СТРУКТУРА, ФОРМИРОВАНИЕ ПАКЕТОВ

Данные обычно содержатся в больших по размерам файлах. Однако сети не будут нормально работать, если персональный компьютер передает этот блок данных целиком. Существует две причины, замедляющие работу при передаче по кабелю больших блоков данных:

1) такой блок, посылаемый одним компьютером, заполняет кабель и связывает работу всей сети, препятствуя взаимодействию остальных сетевых компонентов;

2) возникновение ошибок при передаче крупных блоков приведет к повторной передаче всего блока; при повреждении небольшого блока данных придется повторно передать только этот небольшой блок, что значительно сэкономит время.

Для быстрой передачи данных по сети необходимо разбить их на небольшие управляемые блоки – пакеты или кадры.

Пакет – основная единица информации в компьютерных сетях. При разбиении данных на пакеты скорость передачи их возрастает настолько, что каждый персональный компьютер в сети получает возможность принимать и передавать данные практически одновре-

менно с другими компьютерами. На целевом персональном компьютере (компьютере-получателе) пакеты накапливаются и выстраиваются в определенном порядке для восстановления исходного вида данных.

При разбиении данных на пакеты сетевая операционная система добавляет каждому пакету специальную управляющую информацию, которая обеспечивает:

– передачу исходных данных небольшими блоками;

– сбор данных в определенном порядке (при их получении);

– проверку данных на наличие ошибок (после сборки).

Пакеты могут содержать несколько типов данных:

– информацию (сообщения или файлы);

– определенные виды данных и команд, управляющих персональным компьютером;

– коды управления сеансом (запрос на повторную передачу для исправления ошибки).

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

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

Чаще всего пакет содержит следующие основные поля или части (рис. 3.2):

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

Рис. 3.2. Типичная структура пакета

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

• *сетевой адрес* (*идентификатор*) *передающего абонента* – 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* (*управляющая*) *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*) – 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. Управля-

ющие 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 и обеспечивает выход аппаратуры приемника из состояния приема. Это поле может отсутствовать, если используется самосинхронизирующийся код, позволяющий определять момент окончания передачи пакета.

Часто в структуре пакета выделяют всего три поля:

– начальное управляющее поле пакета (*заголовок пакета*), т. е. поле, включающее 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.

Формат и размер пакета зависят от типа сети, а максимальный размер пакета определяет, в свою очередь, количество пакетов, которое будет создано сетевой операционной системой для передачи большого блока данных.

Большинство пакетов в сети адресуется конкретному компьютеру, и, как результат, только он один реагирует на них. Каждая плата сетевого адаптера видит

все пакеты, передаваемые по сегменту кабеля, но только при совпадении адреса пакета с адресом компьютера она прерывает его работу. Используется также широковещательная адресация: на пакет с таким типом адреса реагирует множество персональных компьютеров в сети.

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 рисунке 3.3.

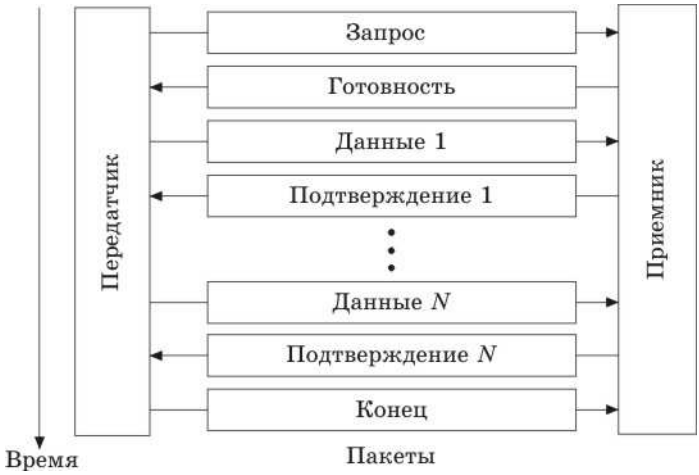

Рис. 3.3. Пример обмена пакетами при сеансе связи

Сеанс обмена начинается с запроса передатчиком готовности приемника принять данные. Для этого используется управляющий пакет «Запрос». Если приемник не готов, он отказывается от сеанса специальным управляющим пакетом. В случае, когда приемник готов, он посылает в ответ управляющий пакет «Готовность». Затем начинается собственно передача данных. При этом

на каждый полученный информационный пакет приемник отвечает управляющим пакетом «Подтверждение». В случае, когда пакет данных передан с ошибками, в ответ на него приемник запрашивает повторную передачу. Заканчивается сеанс управляющим пакетом «Конец», которым передатчик сообщает о разрыве связи. Существует множество стандартных протоколов, которые используют как передачу с подтверждением (с гарантированной доставкой пакета), так и передачу без подтверждения (без гарантии доставки пакета).

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

Крупномасштабные сети, покрывающие огромные территории, могут передавать данные по нескольким маршрутам. Наилучший из маршрутов определяют коммутирующие и соединяющие сетевые компоненты, используя адресную информацию пакетов.

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

Первая система сводится к тому, что при установке сети каждому абоненту пользователь присваивает индивидуальный адрес по порядку, к примеру, от 0 до 30 или от 0 до 254. Присваивание адресов производится программно или с помощью переключателей на плате адаптера.

Достоинства данного подхода – малый объем служебной информации в пакете, а также простота аппаратуры адаптера, распознающей адрес пакета. Недостатки – трудоемкость задания адресов и возможность ошибки (например, двум абонентам сети может быть присвоен один и тот

же адрес). Контроль уникальности сетевых адресов всех абонентов возлагается на администратора сети.

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

В данном случае **маршрутизатор** – устройство, которое собирает информацию о топологии межсетевых соединений и на ее основании пересылает пакеты в сеть назначения, а **маршрут** – последовательность маршрутизаторов, через которые проходит пакет.

Сетевые компоненты используют адресную информацию пакетов и для других целей, в частности, чтобы направлять пакеты к месту назначения и не допускать их в те области сети, к которым они не относятся. В правильной рассылке пакетов ключевую роль играют две функции:

1) продвижение пакетов;

2) фильтрация пакетов.

Персональный компьютер может отбирать определенные пакеты на основе некоторых критериев, например адреса.

3.5. МЕТОДЫ ДОСТУПА

Метод доступа – набор правил, которые определяют, как персональный компьютер должен отправлять и принимать данные по сетевому кабелю.

Обычно несколько компьютеров в сети имеют совместный доступ к кабелю. Однако если два компьютера попытаются передавать данные одновременно, их пакеты столкнутся и будут испорчены – возникнет так называемая *коллизия*.

Передача данных по сети включает две задачи:

1) поместить данные в кабель без столкновения с данными, уже передаваемыми по нему;

2) принять данные с достаточной степенью уверенности в том, что при передаче они не были повреждены в результате коллизии.

Все сетевые персональные компьютеры должны использовать один и тот же метод доступа, иначе произойдет сбой сети, когда отдельные компьютеры, чьи методы будут доминировать, не позволят остальным осуществлять передачу.

Методы доступа предотвращают одновременный доступ к кабелю нескольких компьютеров, упорядочивая передачу и прием данных по сети и гарантируя, что в каждый момент времени только один персональный компьютер может передавать данные.

Существует три способа предотвратить одновременную попытку использовать кабель, другими словами, три основных метода доступа к нему:

- множественный доступ с контролем несущей и обнаружением (либо предотвращением) коллизий;
- доступ с передачей маркера;
- доступ по приоритету запроса.

***Множественный доступ с контролем несущей и обнаружением коллизий* (CSMA/CD).** Название этого метода доступа раскрывает его суть. Персональные компьютеры как бы «прослушивают» кабель – производят контроль несущей. Чаще всего несколько компьютеров в сети «хотят» передать данные, отсюда – множественный доступ. Передавая данные, они «прослушивают» кабель

для того, чтобы, обнаружив коллизии, некоторое время переждать, а затем возобновить передачу, отсюда – обнаружение коллизий. В то же время способность обнаруживать коллизии ограничивает область действия самого CSMA/CD. При длине кабеля больше 2,5 км сигнал ослабевает, и механизм обнаружения коллизий становится неэффективным. Иными словами, если расстояние до передающего персонального компьютера превышает его ограничение, то некоторые из них могут «не услышать» сигнал и начнут передачу данных, что приведет к коллизии и разрушению пакетов данных.

CSMA/CD известен как состязательный метод, поскольку сетевые персональные компьютеры «состязаются» (конкурируют) между собой за право передавать данные. Он кажется очень громоздким, но современные реализации CSMA/CD настолько быстры, что пользователи даже не замечают, что их сеть работает по состязательному методу доступа.

***Множественный доступ с контролем несущей и предотвращением коллизий* (CSMA/CA).** Этот метод не так популярен как множественный доступ с контролем несущей и обнаружением коллизий или передачей маркера. Используя этот доступ, каждый компьютер перед передачей данных в сеть сигнализирует о своем намерении, поэтому остальные узнают о готовящейся передаче и могут избежать коллизий.

Однако широковещательное оповещение увеличивает общий трафик сети и уменьшает ее пропускную способность. Отсюда следует, что множественный доступ с контролем несущей и предотвращением коллизий работает медленнее, чем множественный доступ с контролем несущей и обнаружением коллизий.

***Маркерный метод доступа*.** К маркерным методам относятся два наиболее известных типа передачи данных по локальной сети: маркерная шина (стандарт IEEE 802.4) и маркерное кольцо (стандарт IEEE 802.5).

В сетях с маркерным методом доступа право на доступ к среде передается циклически от станции к станции по логическому кольцу. Кольцо образуется отрезками кабеля, соединяющими соседние станции. Таким образом, каждая станция связана с предшествующей и последующей станциями и может непосредственно обмениваться данными только с ними. Для обеспечения доступа станций к физической среде по кольцу циркулирует кадр специального формата и назначения – маркер.

Маркер – управляющая последовательность битов, передаваемая компьютером по сети. Маркер предназначен для управления доступом к сети компьютеров в маркерных методах доступа и включает в себя три поля длиной в один байт каждое:

1) *начальный ограничитель*, представляющий собой уникальную последовательность, которую нельзя спутать ни с одной битовой последовательностью внутри кадра;

2) *управление доступом*, состоящее, в свою очередь, из четырех полей – битов приоритета, бита маркера, бита монитора, резервных битов;

3) *конечный ограничитель*, а также два бита признаков, указывающих, является кадр последним в серии кадров или промежуточным – признак ошибки.

Получив маркер, станция анализирует его, при необходимости модифицирует 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 последовательно по битам выдает в кольцо кадр данных установленного формата, содержащий следующие поля: начальный ограничитель, управление кадром, адрес назначения, адрес источника, данные, контрольная сумма, конечный ограничитель, статус кадра. Переданные данные проходят

по кольцу всегда в одном направлении, от одной станции к другой.

При поступлении кадра данных к одной или нескольким станциям эти станции копируют для себя этот кадр и вставляют в него подтверждение приема. Станция, выдавшая кадр данных в кольцо, при обратном его получении с подтверждением приема изымает этот кадр из кольца и выдает новый маркер для обеспечения возможности другим станциям сети передавать данные.

Так как в каждый момент времени только один персональный компьютер будет использовать маркер, в сети не возникнет ни состязания, ни коллизий, ни временных задержек.

Время удержания одной станцией маркера ограничивается *тайм-аутом удержания маркера*, по истечении которого станция обязана передать маркер далее по кольцу.

Каждая станция имеет механизмы обнаружения и устранения неисправностей сети, возникающих в результате ошибок передачи или переходных явлений (например, при подключении и отключении станции). Не все станции в кольце равны. Одна из станций обозначается как *активный монитор*, что означает дополнительную ответственность по управлению кольцом. Активный монитор осуществляет управление тайм-аутом в кольце, порождает новые маркеры, чтобы сохранить рабочее состояние, и генерирует диагностические кадры при определенных обстоятельствах. Активный монитор выбирается, когда кольцо инициализируется, и в этом качестве может выступить любая станция сети. Если монитор отказал по какой-либо причине, существует механизм, с помощью которого другие станции (*резервные мониторы*) могут договориться, какая из них будет новым активным монитором.

Доступ по приоритету запроса. Это относительно новый метод, разработанный для сети со скоростью передачи данных 100 Мбит/с. Он стандартизирован IEEE в категории 802.12. Этот метод доступа учитывает своеобразную конфигурацию сетей, которые строятся только из концентраторов и оконечных узлов. Концентраторы управляют доступом к кабелю, последовательно опрашивая каждый узел в сети и выявляя запросы на передачу. Концентратор должен знать все адреса связи и узлы и проверять их работоспособность. Оконечным узлом, в соответствии с сетью, может быть персональный компьютер, мост, маршрутизатор, коммутатор.

Получив одновременно два запроса, концентратор вначале отдаст предпочтение запросу с более высоким приоритетом; если приоритеты одинаковы, то они будут выполнены в произвольном порядке. В сетях с использованием метода доступа по приоритету запроса каждый персональный компьютер может одновременно передавать и принимать данные, так как для этих сетей разработана специальная схема кабеля. В них применяется 8-проводной кабель, по каждой паре проводов сигналы передаются с частотой 25 МГц.

Коммутаторы направляют пакеты по доступным соединениям и маршрутам. Для различных видов сообщений передаваемым данным могут назначаться различные приоритеты.

3.6. ПРОТОКОЛЫ

Передача данных по сети, с технической точки зрения, должна быть разбита на ряд последовательных шагов, каждому из которых соответствуют свои правила и процедуры, или протокол.

Протокол – это набор правил и процедур, регулирующих порядок осуществления некоторой связи. Про-

токолы позволяют нескольким персональным компьютерам при объединении в сеть общаться друг с другом.

Существует множество протоколов, и хотя все они участвуют в реализации связи, каждый протокол имеет различные цели, выполняет различные задачи, обладает своими преимуществам и ограничениями. Протоколы работают на разных уровнях OSI, причем функции протокола определяются уровнем, на котором он работает.

Несколько протоколов могут работать совместно. В этом случае они образуют набор протоколов, или стек.

С помощью протоколов сохраняется строгая очередность в выполнении конкретных действий. Кроме того, эти действия должны быть выполнены в одной и той же последовательности на каждом сетевом персональном компьютере.

Компьютер-отправитель в соответствии с протоколом выполняет следующие действия:

– разбивает данные на небольшие блоки (пакеты), с которыми может работать протокол;

– добавляет к пакетам адресную информацию, чтобы компьютер-получатель мог определить, что эти данные предназначены именно ему;

– подготавливает данные к передаче через плату сетевого адаптера и далее – по сетевому кабелю.

Компьютер-получатель в соответствии с протоколом выполняет те же действия, но только в обратном порядке:

– принимает пакеты данных из сетевого кабеля;

– через плату сетевого адаптера передает пакеты в персональный компьютер;

– удаляет из пакета всю служебную информацию, добавленную компьютером-отправителем;

– копирует данные из пакета в буфер для их объединения в исходный блок данных;

– передает приложению блок данных в том формате, который оно использует.

Для совпадения поступивших данных с исходными компьютеру-отправителю и компьютеру-получателю необходимо выполнять действия одинаковым способом. Если, например, два протокола будут по-разному разбивать данные на пакеты и добавлять несовпадающую информацию, то компьютер, использующий один из этих протоколов, не сможет успешно связаться со следующим, на котором работает другой протокол.

Несколько протоколов, которые работают в сети одновременно, обеспечивают следующие операции с данными:

– подготовку;
– передачу;
– прием;
– последующие действия.

Работа различных протоколов должна быть скоординирована так, чтобы исключить конфликты или незаконченные операции. Этого можно достичь с помощью разбиения стеков протоколов на уровни.

Существует несколько *стандартных наборов протоколов*, получивших наиболее широкое распространение:

– ISO/OSI;
– IBM System Network Architecture;
– Digital DECnet;
– Novell NetWare;
– набор протоколов глобальной сети Internet, TCP/IP.

Стек протоколов – некоторая комбинация протоколов. Каждый уровень стека определяет различные протоколы для управления функциями связи и подсистемами. Каждому уровню присущ свой набор правил:

прикладной – инициация / прием запроса;

представительный – добавление в пакет форматирующей и отображающей информации;

сеансовый – добавление информации о трафике с указанием момента отправки пакета;

транспортный – добавление информации для обработки ошибок;

сетевой – добавление адресной информации и информации о месте пакета в последовательности передаваемых пакетов;

канальный – добавление информации для проверки ошибок и подготовка данных для передачи по физическому соединению;

физический – передача пакета как потока битов.

Разработанные на основе общих принципов стеки отличаются по своей реализации и поэтому несовместимы.

В протоколах используется несколько основных методов решения проблем связи:

- для восстановления исходного порядка передачи пакетов и устранения дубликатов применяется упорядочение;
- для предотвращения потери пакетов используется подтверждение и повторная передача;
- для предотвращения воздействия посторонних пакетов применяются уникальные идентификаторы сеансов;
- для управления потоком данных применяется передача с остановками или механизм скользящего окна;
- для предотвращения заторов в сети уменьшается частота выработки.

В сетевой системе без установления логического соединения отдельные пакеты могут проходить по разным маршрутам и поэтому поступать в ином порядке по сравнению с тем, в каком они были отправлены. Для решения проблемы доставки в ином порядке в транспортных протоколах используется *метод упорядочения*. Отправитель добавляет к каждому пакету порядковый номер. Получатель хранит порядковый номер не в том порядке: если пакет является очередным ожидаемым пакетом (т. е. поступил по порядку), то программное обеспечение протокола доставляет этот пакет на следующий выше-

стоящий уровень и проверяет список, чтобы определить, можно ли также доставить недостающие пакеты.

Потеря пакета – одна из основных проблем компьютерных сетей, поскольку ошибки при передаче могут вызвать искажение битов, в результате чего весь пакет становится недействительным. При обнаружении получателем подобных искажений отбрасывается весь пакет. Для обеспечения надежной передачи (т. е. передачи без потерь) в протоколах используется *метод подтверждения с повторной передачей*: если пакет поступил в неизменном виде, то программное обеспечение протокола получателя передает отправителю небольшое сообщение об успешном приеме, называемое **подтверждением**. После передачи пакета протокол отправителя запускает таймер. Если подтверждение поступает до истечения установленного времени, то программное обеспечение отменяет отсчет по таймеру; если же установленный тайм-аут истекает до поступления подтверждения, то программное обеспечение отправителя отправляет еще одну копию пакета (повторная передача) и снова запускает таймер. Повторная передача часто приводит к появлению дубликатов пакетов. Поскольку отправитель не имеет возможности определить, был ли пакет потерян или просто задержался, то может передать повторную копию, не дождавшись подтверждения. Поэтому в протоколах, использующих повторную передачу, необходимо также решить проблему дубликатов пакетов.

Одна из проблем задержки в системе коммутации пакетов вызвана применением промежуточного накопления. Пакет, поступивший в коммутатор пакетов, помещается в очередь. Если пакеты поступают быстрее, чем может перенаправить коммутатор, очередь ожидающих пакетов будет большой и задержка может оказаться чрезмерной, что может привести к появлению ошибок,

связанных с воздействием задержавшихся в очереди пакетов. Можно рассмотреть последовательность событий:

• два персональных компьютера согласовывают между собой сеанс связи в 13:00;

• один компьютер отправляет последовательность из десяти пакетов на другой;

• в результате сбоя аппаратного обеспечения третий пакет задерживается;

• для устранения нарушения передачи данных изменяются маршруты;

• программное обеспечение протокола компьютера-отправителя повторно передает третий пакет, и он вместе с остальными пакетами передается без ошибок;

• в 13:05 оба персональных компьютера снова согласовывают между собой сеанс обмена данными;

• после прибытия второго пакета поступает задержанная копия третьего пакета, принадлежащая к предыдущему сеансу связи.

К сожалению, если протокол не был тщательно спроектирован, то пакет из предыдущего сеанса связи может быть принят в следующем сеансе, а правильный пакет отброшен как дубликат.

Посторонние пакеты также могут появляться при передаче управляющих пакетов. Например, в протоколах часто применяется комплект специальных управляющих пакетов для прекращения сеанса обмена данными. Получение копии запроса на разрыв связи из предыдущего сеанса может заставить программное обеспечение протокола преждевременно прервать текущий сеанс.

Для предотвращения воздействия пакетов, принадлежащих к другим сеансам, в протоколах предусматривается обозначение каждого сеанса уникальным *идентификатором*, *и этим идентификатором обозначается каждый пакет*. Программное обеспечение протокола отбрасывает все поступившие пакеты, которые содержат

неправильный идентификатор. Идентификатор не должен использоваться повторно до истечения достаточно большого интервала времени.

Не все компьютеры работают с одинаковой скоростью. Если компьютер-отправитель передает данные по сети быстрее, чем может обработать компьютер-получатель, то возникает переполнение данными, что приводит к их утере. Для устранения этой проблемы применяют такие методы управления потоком данных, как *метод передачи с остановками* и *скользящее окно*. В системе передачи с остановками отправитель ожидает разрешения на передачу каждого пакета и, когда получатель готов к передаче следующего пакета, отправляет управляющее сообщение, обычно в форме подтверждения. Этот метод неэффективен при использовании пропускающей способности сети, хотя такие протоколы передачи предотвращают переполнение данными.

Метод управления передачей данных, называемых скользящим окном, позволяет достичь наиболее высокой производительности. Суть данного метода заключается в следующем: отправитель и получатель запрограммированы на использование окна постоянного размера – так называется максимальный объем данных, который может быть передан до получения подтверждения.

Заторы представляют одну из основных проблем в системах коммуникации пакетов. Они обычно возникают в тех участках сети, где данные одновременно передаются компьютеру-получателю сразу несколькими компьютерами-отправителями через один и тот же сегмент сети. Коммутатор пакетов помещает входящие пакеты с узла в очередь до тех пор, пока не появится возможность их отправки. Поскольку поступает больше пакетов, чем может быть отправлено, очередь растет и увеличивается; если затор не удается устранить, коммутатор пакетов исчерпывает всю доступную память и начинает отбрасы-

вать пакеты. Хотя для восстановления потерянных пакетов может применяться повторная передача, для нее нужно также дополнительное время. Более того, если такая ситуация сохраняется, вся сеть может стать неработоспособной. Это называется выходом сети из строя в связи с затором. В протоколах предусматривается наблюдение за сетью и быстрое реагирование на первые признаки затора. Для этого могут применяться два подхода:

1) передача коммутатором предупреждений отправителю пакетов при возникновении затора;

2) оценка качества затора на основе информации о потере пакетов.

Первая схема реализуется либо путем применения в коммутаторах специального сообщения, которое передается отправителю при возникновении затора, либо путем установки коммутаторами специального бита в заголовке каждого пакета, который задержан в связи с затором. Если бит в заголовке установлен, то персональный компьютер, получивший пакет, включает информацию об этом в подтверждение, которое посылается отправителю пакета.

В некоторых протоколах на появление затора предусмотрен механизм управления частотой передачи пакетов. При возникновении затора программное обеспечение протокола уменьшает частоту выработки пакетов. В протоколах со скользящим окном можно достичь того же эффекта, временно уменьшив размер окна.

? *Контрольные вопросы и задания*

1. Поясните, что называют открытой системой.

2. Дайте определение термину «спецификация».

3. Опишите эталонную модель взаимодействия открытых систем.

4. Перечислите основные уровни модели OSI и изложите их функции.

5. Опишите подуровни канального уровня.

6. Перечислите основные стандарты 802.

7. Опишите назначение драйвера.

8. Объясните процесс настройки драйвера.

9. Дайте определение понятию «пакет».

10. Назовите основные типы данных, содержащихся в пакете.

11. Охарактеризуйте основные поля пакета.

12. Опишите процесс обмена информацией.

13. Назовите основные подходы к адресации в сети.

14. Дайте характеристику методам доступа CSMA/CD, CSMA/CA. Раскройте основные преимущества и недостатки этих методов доступа.

15. Определите состав маркера.

16. Опишите суть маркерного доступа.

17. Сформулируйте определение понятия «протокол».

18. Перечислите стандартные наборы протоколов.

19. Опишите процесс обеспечения надежности передачи пакетов.

20. Изложите схему избежания заторов в сети.

21. Определите, какой метод доступа целесообразно использовать:

- для учебной компьютерной аудитории;
- сети населенного пункта протяженностью не более 2,5 км.

Ответ аргументируйте.

РАЗДЕЛ 4
СЕТЕВЫЕ ТЕХНОЛОГИИ

4.1. СЕТИ ШИННОЙ ТОПОЛОГИИ. СЕТЬ ETHERNET

В топологии «логическая шина» последовательности данных (кадры) в виде сигналов распространяются одновременно во всех направлениях по существующей среде передачи. Каждая станция в сети проверяет каждый кадр данных для определения того, кому адресованы эти данные. По достижении сигналом конца среды передачи он автоматически гасится терминаторами. Такое уничтожение сигнала на концах среды передачи данных предотвращает отражение сигнала и его обратное поступление в среду передачи.

В топологии «логическая шина» среда передачи совместно и одновременно используется всеми устройствами передачи данных. Для предотвращения помех при попытках одновременной передачи данных несколькими станциями только одна станция в любой момент времени имеет право передавать данные. Таким образом, должен существовать метод определения того, какая станция имеет право передавать данные в каждый конкретный момент времени.

Наиболее часто используемым при организации топологии «логическая шина» методом контроля доступа к среде передачи является метод прослушивания несущей с организацией множественного доступа и обнаружени-

ем коллизий. Сеть, базирующаяся на топологии «логическая шина», может также использовать и технологию передачи маркера для контроля доступа к среде передачи данных.

Топология «логическая шина» базируется на использовании физических топологий «шина» и «звезда». Метод контроля доступа и типы физических топологий выбираются в зависимости от требований к проектируемой сети.

Обычный **Ethernet** является одним из самых простых и дешевых в построении из когда-либо разработанных стандартов локальных сетей. Ethernet создан на базе экспериментальной сети Ethernet Network, предложенной фирмой Xerox в 1975 г. В сетях Ethernet все компьютеры имеют непосредственный доступ к общей шине, поэтому она может быть использована для передачи данных между любыми двумя узлами сети. Одновременно все компьютеры имеют возможность немедленно получить данные, которые любой из компьютеров начал передавать на общую шину. Простота подключения и передачи информации компьютерами – одна из причин, которые привели стандарт Ethernet к успеху. Иногда такое построение сети называют *методом коллективного доступа*.

Прежде чем перейти к непосредственному рассмотрению типов организации локальной сети, необходимо сказать несколько слов о *технологических классах*, на которые делятся сети стандарта Ethernet. Данные классы различаются, прежде всего, пропускной способностью линий, типом используемого кабеля, топологией и некоторыми иными характеристиками. Каждый из классов сетей Ethernet имеет собственное обозначение, отражающее его технические характеристики. Такое обозначение имеет вид XBaseY, где X – пропускная способность сети; обозначение Base говорит о методе передачи сигнала

(baseband – основополосный); число Y отображает максимальную длину сегмента сети в сотнях метров либо обозначает тип используемого в такой системе кабеля, который и накладывает ограничения на максимально возможное расстояние между двумя узлами сети исходя из собственных технических характеристик. Например, сеть класса 10Base-2 имеет пропускную способность 10 Мбит/с, использует метод передачи данных baseband и допускает максимальную длину сегмента 200 м.

В зависимости от типа физической реализации различают следующие типы Ethernet:

• 10Base-5 (толстый коаксиальный кабель). За счет своей толщины (внешний диаметр составляет около 10 мм) кабель неудобен в использовании. Кроме того, недостатками этого типа построения являются высокая стоимость и небольшое максимально допустимое количество станций – не более 100. Достоинства – высокая защищенность от внешних воздействий и сравнительно большая длина сегмента – до 500 м. Данный стандарт разработан фирмой Xerox и считается классическим Ethernet;

• 10Base-2 (тонкий коаксиальный кабель) – один из самых простых в установке и дешевых типов сети. Тонкий коаксиальный кабель (до 5 мм) прокладывается вдоль расположения компьютеров сети. На конце каждого сегмента располагается терминатор, предотвращающий возникновение эффекта отражения волны. К недостаткам данного типа сети Ethernet относят выход из строя сети при повреждении кабеля и сравнительно трудоемкое обнаружение отказавшего отрезка кабеля (возможно только с помощью кабельного тостера), низкая защита от помех, максимальное число компьютеров в сети – не более 1024. Максимальная длина сегмента данного стандарта без использования повторителей составляет 185 м;

• 10Base-T (витая пара) – сети на основе витой пары, на сегодняшний день они наиболее распространены, так как строятся на основе витой пары и используют топологию типа «звезда». За счет этого конфигурировать локальную сеть становится значительно удобнее и рациональнее. Основные недостатки: слабая помехозащищенность и восприимчивость к электрическим помехам, что не дает возможности использовать такие сети в непосредственной близости к источникам электромагнитных излучений;

• 10Base-F (волоконно-оптический канал) – технология, использующая в качестве носителя волоконно-оптический кабель. По строению она аналогична Ethernet 10Base-T, т. е. использует топологию «звезда». Использование волоконно-оптического кабеля приводит к тому, что такое построение сетей обеспечивает почти полную помехозащищенность от электромагнитных излучений. Однако этот метод построения Ethernet имеет следующие недостатки: волоконно-оптический кабель хрупкий, поэтому монтаж его очень затруднен; кроме того, это самый дорогой из всех видов кабеля.

Топология для всех четырех типов практически не различается. Данные в локальной сети передаются со скоростью до 10 Мбит/с, о чем говорит первая цифра в названии типа сети.

В сетях Ethernet используется *метод коллективного доступа к среде передачи данных с опознаванием несущей и обнаружением коллизий* (CSMA/CD).

Четкое распознавание коллизий всеми станциями сети является необходимым условием корректной работы сети Ethernet. Если какая-либо передающая станция не распознает коллизию и решит, что кадр данных ею передан верно, то этот кадр данных будет утерян, так как информация кадра исказится из-за наложения сигналов при коллизии и он будет отбракован прини-

мающей станцией. Конечно, скорее всего, искаженная информация будет повторно передана каким-либо протоколом верхнего уровня, например, транспортным или прикладным, работающим с установлением соединения и нумерацией своих сообщений. Повторная передача сообщения протоколами верхних уровней произойдет через гораздо более длительный интервал времени (десятки секунд) по сравнению с микросекундными.

Величина интервала отсрочки в стандарте 802.3 рассчитана для максимальной длины коаксиального кабеля 2,5 км и определена равной 512 битовым интервалам. Величина 512 определяет и минимальную длину кадра в 64 байта, так как при кадрах меньшей длины станция может передать кадр и не успеть заметить факт возникновения коллизии из-за того, что искаженные коллизией сигналы дойдут до станции в наихудшем случае после завершения передачи. Такой кадр будет просто потерян.

Время паузы после N-й коллизии полагается равным L интервалам отсрочки, где L – случайное целое число, равномерно распределенное в диапазоне $[0, 2N]$. Величина диапазона растет только до десятой попытки (напомним, что их не может быть больше 16), а далее диапазон остается равным [0, 210], т. е. [0, 1024]. Значения основных параметров процедуры передачи кадра стандарта 802.3 приведены в таблице.

Таблица

Значения основных параметров процедуры передачи кадра стандарта 802.3

Битовая скорость	10 Мб/с
Интервал отсрочки	512 битовых интервалов
Межкадровый интервал	9,6 мкс
Максимальное число попыток передачи	16
Максимальное число возрастания диапазона паузы	10

Окончание табл.

Длина *j* am-последовательности	32 бит
Максимальная длина кадра (без преамбулы)	1518 байт
Минимальная длина кадра (без преамбулы)	64 байт (512 бит)
Длина преамбулы	64 бит

Учитывая приведенные параметры, можно рассчитать максимальную производительность сегмента Ethernet в таких единицах, как число переданных пакетов минимальной длины в секунду. Количество обрабатываемых пакетов Ethernet в секунду часто используется при указании внутренней производительности мостов и маршрутизаторов, вносящих дополнительные задержки при обмене между узлами. Поэтому необходимо знать максимальную производительность сегмента Ethernet в идеальном случае, когда на кабеле нет коллизий и нет дополнительных задержек, вносимых мостами и маршрутизаторами.

С увеличением скорости передачи кадров, что имеет место в новых стандартах, базирующихся на том же методе доступа CSMA/CD, например Fast Ethernet, максимальная длина сети уменьшается пропорционально увеличению скорости передачи. В стандарте Fast Ethernet она составляет 210 м, а в гигабитном Ethernet ограничена 25 м.

Независимо от реализации физической среды все сети Ethernet должны удовлетворять двум ограничениям, связанным с методом доступа:

- максимальное расстояние между двумя любыми узлами не должно превышать 2500 м;
- в сети не должно быть более 1024 узлов.

Кроме того, каждый вариант физической среды добавляет к этим ограничениям свои ограничения, которые также должны выполняться.

4.2. НАСЛЕДУЕМЫЕ ТЕХНОЛОГИИ ETHERNET. FAST ETHERNET

Технология **Fast Ethernet** принята в 1995 г. в качестве стандарта 802.3u и является эволюционным развитием классической технологии Ethernet.

Основные достоинства технологии Fast Ethernet:

– увеличение пропускной способности сегментов сети до 100 Мб/с;

– сохранение метода случайного доступа Ethernet;

– сохранение звездообразной топологии сетей и поддержка традиционных сред передачи данных – витой пары и оптоволоконного кабеля.

Технология Fast Ethernet подразделяется:

– на 100Base-TX (две витые пары);

– 100Base-T4 (четыре витые пары);

– 100Base-FX (волоконно-оптический канал).

Стандарт 100Base-TX используется в сетях, построенных по топологии «звезда» и в качестве физической среды использующих кабель «витая пара» UTP не ниже 5-й категории. Это позволяет оборудованию работать как в полудуплексном, так и в дуплексном режиме. При этом дуплексный режим обеспечивает максимально возможную для стандарта скорость передачи данных – 100 Мбит/с.

Стандарт 100Base-TX требует выполнения следующих условий:

• для передачи данных используется только кабель «витая пара» 5-й категории;

• длина кабеля «витая пара» для подключения рабочей станции не должна превышать 100 м;

• для увеличения диаметра сети может применяться не более двух репитеров, при этом максимальный радиус сети составляет 205 м;

• длина кабеля между репитерами не должна превышать 5 м;

• все рабочие станции подключаются к центральному управляющему устройству, в качестве которого могут использоваться концентратор, коммутатор и т. д.;

• максимальное количество подключений – 1024.

Влияние на широкое распространение 100Base-TX произвела стандартизация материнских плат (ATX), которая сделала наличие сетевого адаптера на материнской плате обязательным.

Стандарт 100Base-T4 относится к серии 100-мегабитных. Он также подразумевает использование топологии «звезда» и кабеля «витая пара» (UTP). Однако в отличие от 100Base-TX данный стандарт позволяет в качестве среды передачи данных использовать кабель ниже 5-й категорий. Данный факт является наибольшим плюсом этого стандарта. Так, пользователи локальной сети стандарта 10Base-T, которая подразумевает применение кабеля «витая пара» 3-й категории, могут перейти на сеть со скоростью передачи данных 100 Мбит/с, просто заменив используемое оборудование на поддерживающее стандарт 100Base-T4, а также изменив обжим кабеля.

Для применения стандарта 100Base-T4 должны выполняться следующие условия:

• для передачи данных используется кабель «витая пара» 3, 4 и 5-й категорий;

• длина кабеля «витая пара», применяемого для подключения рабочей станции, не должна превышать 100 м;

• для увеличения диаметра сети может использоваться не более двух репитеров, при этом максимальный радиус сети составляет 205 м;

• максимальное количество сегментов – не более трех;

• длина кабеля между репитерами не должна превышать 5 м;

• все рабочие станции подключаются к центральному управляющему устройству, в качестве которого могут применяться концентратор, коммутатор и т. д.;

• максимальное количество подключений – 1024.

Главным минусом стандарта 100Base-T4 является работа в полудуплексном режиме, поэтому данный стандарт сегодня используется достаточно редко.

Стандарт 100Base-FX, принятый в середине 90-х гг. прошлого века, стал логическим продолжением стандартов серии 100Base. Он используется в сетях с топологией «звезда», при этом в качестве среды передачи данных применяется многомодовый оптоволоконный кабель. Благодаря свойствам оптоволоконного кабеля длина сегмента ограничена лишь уровнем затухания сигнала в кабеле и мощностью используемых передатчиков, что позволило добиться скорости передачи данных 100 Мбит/с на достаточно большие расстояния.

Стандарт 100Base-FX предусматривает соблюдение следующих правил функционирования сети:

- для передачи данных используется многомодовый оптоволоконный кабель;
- максимальное расстояние между коммутатором и рабочей станцией или между двумя коммутаторами не должно превышать 412 м в полудуплексном режиме и 2000 м в дуплексном режиме;
- все рабочие станции подключаются к центральному управляющему устройству, в качестве которого могут выступать концентратор, коммутатор и т. д.;
- максимальное количество подключений – 1024.

Особенностью стандарта 100Base-FX является возможность использования очень длинных сегментов кабеля.

Все отличия технологии Fast Ethernet от Ethernet сосредоточены на физическом уровне. Уровни MAC и LLC в Fast Ethernet остались абсолютно теми же.

В новой технологии Fast Ethernet коаксиальный кабель не используется. Так как на небольших расстояниях витая пара 5-й категории позволяет передавать данные с той же скоростью, что и коаксиальный кабель,

сеть получается более дешевой и удобной в эксплуатации. На больших расстояниях оптическое волокно обладает гораздо более широкой полосой пропускания, чем коаксиальный кабель, а стоимость сети получается ненамного выше, особенно если учесть затраты на поиск и устранение неисправностей в крупной коаксиальной системе.

Сети Fast Ethernet всегда имеют иерархическую древовидную структуру, построенную на концентраторах, как сети 10Base-T/10Base-F. Основным отличием конфигураций сетей Fast Ethernet является сокращение диаметра сети примерно до 200 м, что объясняется уменьшением времени передачи кадра минимальной длины в 10 раз за счет увеличения скорости передачи в 10 раз по сравнению с 10-мегабитным Ethernet.

При использовании коммутаторов протокол Fast Ethernet может работать в полнодуплексном режиме, в котором нет ограничений на общую длину физических сегментов, соединяющих соседние устройства (адаптер–коммутатор или коммутатор–коммутатор). Поэтому при создании магистралей локальных сетей большой протяженности технология Fast Ethernet также активно применяется, но только в полнодуплексном варианте, совместно с коммутаторами.

По сравнению с вариантами физической реализации Ethernet в Fast Ethernet отличия каждого варианта от других глубже – меняются как количество проводников, так и методы кодирования.

По некоторым причинам в дополнение к основному стандарту многие производители рекомендуют пользоваться другими запатентованными носителями – например, для увеличения расстояния между точками сети используется оптоволоконный кабель.

Большинство Ethernet-карт и других устройств имеет поддержку нескольких скоростей передачи данных,

используя автоопределение скорости и дуплексности для достижения наилучшего соединения между двумя устройствами. Если автоопределение не срабатывает, скорость подстраивается под партнера и включается режим полудуплексной передачи. Например, наличие в устройстве порта Ethernet 10/100 говорит о том, что через него можно работать по технологиям 10Base-T и 100Base-TX, а порт Ethernet 10/100/1000 поддерживает стандарты 10Base-T, 100Base-TX и 1000Base-T.

4.3. СЕТИ КОЛЬЦЕВОЙ ТОПОЛОГИИ. СЕТЬ TOKEN RING. FDDI

Кольцевую топологию используют технологии Token Ring и FDDI, способные автоматически контролировать работоспособность сети.

Технология Token Ring была разработана компанией IBM в 1984 г. Данная сеть обладает начальными свойствами отказоустойчивости и является реализацией протокола физического уровня IEEE 802.5 с физической топологией «звезда».

Логическая топология локальной сети на основе маркерного кольца (Token Ring) строится на кольцевой архитектуре, что подразумевает индивидуальные соединения «точка-точка». Управляющая последовательность генерирует специальное сообщение – маркер и последовательно передает его всем компьютерам. Правом передачи данных обладает единственный компьютер, располагающий маркером. Как только маркер достигает станции, которая собирается передавать данные, последняя «присваивает» маркер себе и изменяет его статус на «занято». Затем маркер дополняется всей информацией, которую предполагалось передать, и снова отправляется в сеть. Маркер будет циркулировать в сети до тех пор, пока не достигнет адресата информации. Получающая сторона обрабатывает полученную вместе с маркером информа-

цию и опять передает маркер в сеть. Когда маркер возвращается к исходной станции, он удаляется, после чего генерируется новый маркер. Циркуляция начинается заново (рис. 4.1).

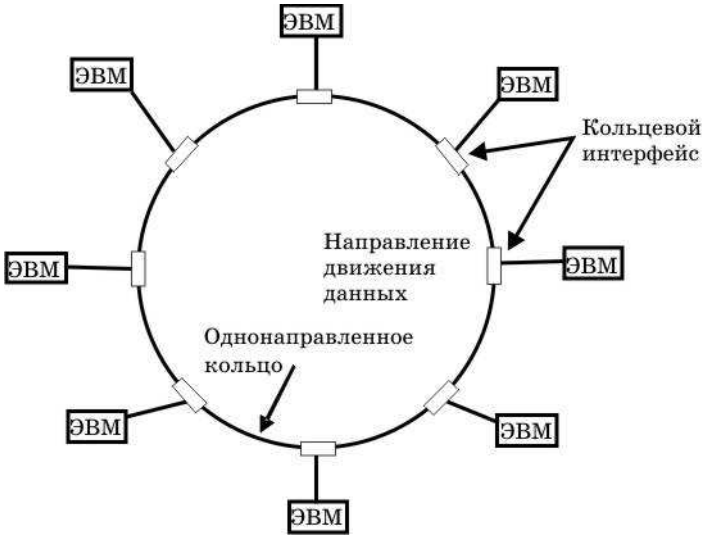

Рис. 4.1. Логическая топология сети на основе маркерного кольца

Серьезным недостатком такого типа построения сетей является то, что разрыв кабеля в одной точке приводит к полной остановке работоспособности сети.

На основе маркерного кольца строятся две локальные сети Token Ring с пропускной способностью 4 и 16 Мбит/с.

В сетях Token Ring 16 Мбит/с используется несколько другой алгоритм доступа к кольцу, называемый *алгоритмом раннего освобождения маркера*. В соответствии с ним станция передает маркер доступа следующей станции сразу же после окончания передачи последнего бита кадра, не дожидаясь возвращения по кольцу этого кадра с битом подтверждения приема. В этом случае пропускная способность кольца используется более эффективно и приближается к 80 % от номинальной.

FDDI – распределенный интерфейс передачи данных по волоконно-оптическим каналам, является высокоскоростной волоконно-оптической системой со скоростью передачи данных 100 Мбит/с. Кроме большой территории, сеть FDDI способна поддерживать несколько тысяч пользователей.

Данная сеть поддерживает метод доступа «маркерное кольцо», но в отличие от Token Ring система FDDI использует для передачи данных два кольца, передача информации по которым осуществляется в противоположных направлениях, причем второе кольцо является резервным (рис. 4.2, *а*).

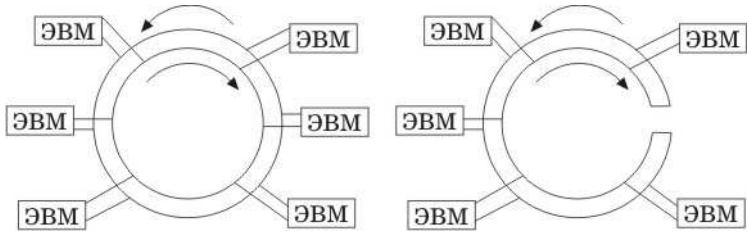

Рис. 4.2. Структура сети FDDI: *а* – обычная передача данных; *б* – передача данных при разрыве канала связи

В случае разрыва по каким–либо причинам первого кольца информация считывается со второго, что увеличивает надежность работоспособности сети. Если произошел разрыв сразу обоих колец в одном и том же месте, имеется возможность объединить два кольца в одно с помощью специальных переключателей (рис. 4.2, *б*).

В качестве среды передачи данных в FDDI рекомендуется волоконно-оптический кабель, однако можно применять и медный кабель (в таком случае используется сокращение CDDI).

4.4. ВНЕДРЕНИЕ И ИСПОЛЬЗОВАНИЕ СОВРЕМЕННЫХ СЕТЕВЫХ ТЕХНОЛОГИЙ. СЕТЬ GIGABIT ETHERNET. ПЕРСПЕКТИВЫ РАЗВИТИЯ

В 1997 г. был принят стандарт IEEE **802.3z Gigabit Ethernet** со скоростью 1000 Мбит/с для передачи по оптоволокну и еще через два года – для передачи по витой паре. В 1998 г. комитет принял стандарт **1000Base-X**, объединивший в себе сразу четыре гигабитных стандарта: 1000Base-LX, 1000Base-CX, 1000Base-LH и 1000Base-LX.

При использовании данных стандартов с кабелем «витая пара» возникают определенные проблемы, связанные со слишком сильными наводками между соседними парами проводников, что не позволяет передавать данные на большой скорости, ограничиваясь только четырьмя парами проводников. Однако возможности оптоволоконной среды еще не раскрыты до конца, поэтому она представляет наибольший интерес.

Все эти стандарты, кроме 1000Base-CX, подразумевают использование оптоволоконного кабеля в качестве среды передачи данных. При этом в зависимости от стандарта максимальная длина сегмента составляет от 500 м (1000Base-SX, многомодовый кабель) до 10 000 м (1000Base-LH, одномодовый кабель).

Гигабит Ethernet (Gigabit Ethernet, 1 Гбит/с) имеет стандарты:

• 1000Base-T, IEEE 802.3ab – стандарт, использующий витую пару категорий 5e или 6; в передаче данных участвуют все четыре пары, скорость передачи данных – 250 Мбит/с по одной паре;

• 1000Base-TX – был создан Ассоциацией телекоммуникационной промышленности и опубликован в марте 2001 г. как «Спецификация физического уровня дуплексного Ethernet 1000 Мб/с (1000Base-TX) симметричных кабельных систем категории 6 (ANSI/TIA/EIA-854-2001)». Стандарт использует раздельную приемопередачу (две пары на передачу, две пары на прием, по каждой паре

данные передаются со скоростью 500 Мбит/с), что существенно упрощает конструкцию приемопередающих устройств. Для стабильной работы по такой технологии требуется кабельная система высокого качества, поэтому 1000Base-TX может использовать только кабель 6-й категории. Еще одним существенным отличием 1000Base-TX является отсутствие схемы цифровой компенсации наводок и возвратных помех, в результате чего сложность, уровень энергопотребления и цена процессоров становятся ниже, чем у процессоров стандарта 1000Base-T. На основе данного стандарта практически не было создано продуктов, хотя 1000Base-TX использует более простой протокол, чем стандарт 1000Base-T, соответственно более простой может быть и электроника;

• 1000Base-X – общий термин для обозначения стандартов со сменными приемопередатчиками GBIC или SFP;

• 1000Base-SX, IEEE 802.3z – стандарт, использующий многомодовое оптоволокно; дальность прохождения сигнала без повторителя до 550 м;

• 1000Base-LX, IEEE 802.3z – стандарт, использующий одномодовое оптоволокно; дальность прохождения сигнала без повторителя до 80 км;

• 1000Base-CX – стандарт для коротких расстояний (до 25 м), использующий экранированную витую пару (STP) с волновым сопротивлением 150 Ом (заменен стандартом 1000Base-T и сейчас не используется);

• 1000Base-LH (Long Haul) – стандарт, использующий одномодовое оптоволокно; дальность прохождения сигнала без повторителя до 100 км.

Новый стандарт **10 Гигабит Ethernet** включает семь стандартов физической среды для LAN, MAN и WAN. В настоящее время он описывается IEEE 802.3ae:

• 10GBase-CX4 – технология 10 Гигабит Ethernet для коротких расстояний (до 15 м), используются медный кабель CX4 и коннекторы InfiniBand;

• 10GBase-SR – технология 10 Гигабит Ethernet для коротких расстояний (до 26 или 82 м, в зависимости от типа кабеля), используется многомодовое оптоволокно; также поддерживает расстояния до 300 м с использованием нового многомодового оптоволокна (2000 МГц/км);

• 10GBase-LX4 – использует уплотнение по длине волны для поддержки расстояний от 240 до 300 м по многомодовому оптоволокну; также поддерживает расстояния до 10 км при использовании одномодового оптоволокна;

• 10GBase-LR и 10GBase-ER – эти стандарты поддерживают расстояния до 10 и 40 км соответственно;

• 10GBase-SW, 10GBase-LW и 10GBase-EW – эти стандарты используют физический интерфейс, совместимый по скорости и формату данных с интерфейсом OC-192/STM-64 SONET/SDH. Они подобны стандартам 10GBase-SR, 10GBase-LR и 10GBase-ER соответственно, так как используют те же самые типы кабелей и расстояния передачи;

• 10GBase-T, IEEE 802.3an-2006 – принят в июне 2006 г. после 4-летней разработки; использует экранированную витую пару, расстояние – до 100 м.

1000Base-T – полноценный гигабитный стандарт, который используется в сетях, построенных с применением топологии «звезда» и кабеля «витая пара» выше пятой категории. Поскольку именно эта топология и среда передачи данных получили наибольшее распространение, не удивителен тот факт, что 1000Base-T приходит на смену интегрированному на материнской плате сетевому контроллеру стандарта 100Base-TX.

При передаче данных используются все четыре пары проводников, при этом передача данных ведется на более высокой частоте. Это дает некоторый запас в величине уровня сигнала, что позволяет производить коррекцию возникающих ошибок.

Стандарт 1000Base-T требует выполнения следующих условий:

– для передачи данных используется неэкранированный кабель «витая пара» 5, 6 и 7-й категорий;

– длина кабеля «витая пара», применяемого для подключения рабочей станции, не должна превышать 100 м;

– для увеличения диаметра сети может использоваться не более двух репитеров, при этом максимальный радиус сети составляет 205 м;

– все рабочие станции подключаются к центральному управляющему устройству, в качестве которого могут применяться концентратор, коммутатор и т. д.;

– максимальное количество подключений – 1024.

Переход со стандарта 100Base-TX на 1000Base-T требует только замены оборудования, поскольку очень часто при построении сети используется кабель категории 5.

4.5. БЕСПРОВОДНЫЕ СЕТИ. МОБИЛЬНЫЕ, СОТОВЫЕ СЕТИ, МИКРОВОЛНОВЫЕ СИСТЕМЫ

Беспроводная среда может ввести в заблуждение, поскольку означает полное отсутствие проводов в сети. В большинстве случаев это не совсем так. Обычно беспроводные компоненты взаимодействуют с сетью, в которой в качестве среды передачи используется кабель. Такая сеть со смешанными компонентами называется *гибридной*.

Идея беспроводной среды весьма привлекательна, так как ее компоненты:

– обеспечивают временное подключение к кабельной сети;

– помогают организовать резервное копирование в кабельную сеть;

– гарантируют определенный уровень мобильности;

– позволяют снять ограничения на максимальную протяженность в сети, накладываемые медными и даже оптоволоконными кабелями.

Беспроводные сети можно разделить на три типа:

1) локальные вычислительные сети;

2) расширенные локальные вычислительные сети;

3) мобильные сети.

Локальные вычислительные сети и расширенные локальные вычислительные сети используют передатчики и приемники, принадлежащие той организации, в которой функционируют сети.

Для переносных персональных компьютеров средой передачи служат общедоступные сети – Internet, телефонная сеть.

Локальная вычислительная сеть – это типичная беспроводная сеть, которая выглядит и функционирует практически так же, как и кабельная, за исключением среды передачи.

Беспроводной сетевой адаптер с трансивером установлен в каждом персональном компьютере, и пользователи работают так, будто их компьютеры соединены кабелем (рис. 4.3).

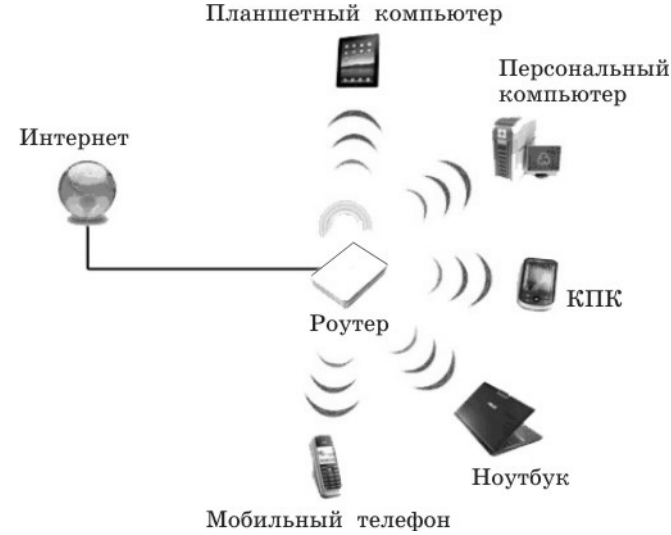

Рис. 4.3. Беспроводная локальная сеть

Беспроводные локальные вычислительные сети используют следующие способы передачи данных:

1) инфракрасное излучение;

2) лазерное излучение;

3) радиопередача в узком диапазоне;

4) радиопередача в рассеянном спектре;

5) микроволновые системы.

Инфракрасные технологии функционируют на очень высоких частотах, которые приближаются к частотам видимого света. Их используют для установления двухсторонней или широковещательной связи на близких расстояниях.

В подобных системах необходимо генерировать очень сильный сигнал, так как в противном случае значительное влияние будут оказывать другие источники. Этот способ позволяет передавать сигналы с большой скоростью, поскольку инфракрасный свет имеет широкий диапазон частот.

Существует четыре типа инфракрасных сетей:

– сети прямой видимости;

– сети на рассеянном инфракрасном излучении;

– сети на отраженном инфракрасном излучении;

– модулированные оптические сети.

Основные недостатки инфракрасных сетей – трудности при передаче сигнала на расстояние более 30 м; подверженность помехам со стороны сильных источников света.

Лазерная технология похожа на инфракрасную, так как требует прямой видимости между передатчиком и приемником – если по каким-либо причинам луч будет прерван, то передача прекратится.

Беспроводные линии связи (радиоканалы наземной и спутниковой связи) образуются с помощью передатчика и приемника радиоволн.

Радиопередача в узком диапазоне напоминает вещание обыкновенной радиостанции. Пользователи настраивают передатчик и приемники на определенную частоту, при этом прямая видимость не обязательна. Площадь вещания составляет 46 500 м^2. Однако поскольку используется сигнал высокой частоты, он не проникает через металлические или железобетонные преграды. Доступ к такому способу связи осуществляется через поставщика услуг. Связь относительно медленная – 4,8 Мбит/с.

Радиопередача в рассеянном спектре дает возможность передавать сигналы на нескольких частотах, что позволяет избежать проблем, присущих одночастотной передаче. Доступные частоты разделены на каналы. Адаптеры в течение определенного промежутка времени настроены на определенный канал, после чего переключаются на другой. Переключение всех персональных компьютеров в сети происходит синхронно. Данный способ передачи обладает некоторой защитой. Если необходимо усилить защиту – применяют кодирование. Связь относят к разряду самых медленных.

Существует большое количество различных типов радиоканалов, отличающихся как используемым частотным диапазоном, так и дальностью канала. Диапазоны коротких, средних и длинных волн (КВ, СВ и ДВ), называемые также диапазонами амплитудной модуляции (АМ) – по типу используемого в них метода модуляции сигнала, обеспечивают дальнюю связь, но при невысокой скорости передачи данных. Более скоростными являются каналы, работающие на диапазонах ультракоротких волн (УКВ), для которых характерна частотная модуляция (FM), а также на диапазонах сверхвысоких частот (СВЧ). В диапазоне СВЧ (свыше 4 ГГц) сигналы уже не отражаются ионосферой Земли, и для устойчивой связи требуется наличие прямой видимости между передатчиком и приемником. Поэтому такие частоты используют

спутниковые каналы или радиорелейные каналы, где это условие выполняется.

Некоторые типы беспроводных компонентов способны функционировать в расширенной локальной вычислительной сети, так же как их аналоги в кабельных сетях. Беспроводной мост соединяет сети, находящиеся на расстоянии до 5 км друг от друга.

В беспроводных **мобильных сетях** в качестве среды передачи выступают телефонные сети и общедоступные служебные; при этом используются:

– пакетные радиосоединения;

– сотовые сети;

– спутниковые станции.

При использовании *пакетных радиосоединений* данные разбиваются на пакеты, в которых содержится следующая информация: адрес источника, адрес приемника информации для коррекции ошибок. Пакеты передаются на спутник, который транслирует их в широковещательном режиме, затем устройство с соответствующим адресом принимает эти пакеты.

Сотовые цифровые пакеты данных используют ту же технологию, что и сотовые телефоны, – передают данные по существующим для передачи речи сетям в те моменты, когда эти сети не заняты. Они, как и другие беспроводные сети, должны быть подключены к кабельной сети.

Микроволновые системы помогают организовывать связь между зданиями, расположенными на ограниченной территории. Микроволновая технология – способ передачи данных на большие расстояния, он идеален при взаимодействии таких двух точек, как спутник и наземная станция.

Беспроводные локальные вычислительные сети описаны стандартом **802.11**, который предполагает работу сети в двух режимах – с базовой станцией и без базовой

станции. В первом случае связь осуществляется через базовую станцию – точку доступа; во втором – компьютеры общаются непосредственно друг с другом.

В 2009 г. был принят стандарт IEEE **802.11n**, который начал новую эру в развитии беспроводных сетей. Использование оборудования данного стандарта позволяет достигать значительных скоростей передачи данных – до 300 Мбит/с (по некоторым данным до 600 Мбит/с). Такая скорость передачи данных стала возможной благодаря оптимальному использованию полос радиочастот, а также применению более качественных аналоговых чипов обработки сигналов с раздельным приемным и передающим трактами. Новый стандарт использует деление доступного частотного диапазона на полосы шириной 40 МГц с параллельной передачей данных сразу по нескольким полосам.

Стандарт IEEE 802.11n предусматривает следующие правила:

– беспроводное оборудование работает в диапазонах частот 2,4 и 5 ГГц, выбор которых происходит в зависимости от режима работы. Он зависит от стандартов оборудования, которое работает в локальной сети. Например, если в сети используется оборудование разных стандартов, то будет выбран режим совместимости с предыдущими стандартами, и скорость передачи данных при этом будет гораздо ниже стандартной. Если же применяется только оборудование стандарта IEEE 802.11n, то будет выбран режим с максимальной скоростью передачи данных;

– радиус сети не превышает 450 м;

– скорость передачи данных зависит от режима использования оборудования и составляет от 54 Мбит/с (в режиме совместимости со стандартами IEEE 802.11a, IEEE 802.11b и IEEE 802.11g) до 300 Мбит/с (при использовании устройств стандарта IEEE 802.11n);

– для обработки сигнала применяются усовершенствованный метод ортогонального частотного мультиплексирования OFDM и технология многоканальных антенных систем MIMO.

На сегодняшний день стандарт IEEE 802.11n является наиболее перспективным, тем более что стоимость оборудования этого стандарта вполне доступна.

Основной метод доступа в 802.11 MAC – множественный доступ с детектированием несущей и предупреждением коллизий (CSMA/CA). Протокол CSMA/CA опционально позволяет минимизировать коллизии в канале связи за счет использования последовательности: «запрос на передачу», «разрешение на передачу», передача данных и подтверждение приема. Протокол CSMA/CA работает по принципу «слушаю, потом говорю». Станция, желающая передать пакет, должна «послушать» радиоканал на предмет наличия передачи от другой станции. Если радиоканал свободен, станция может передавать пакет. В протоколе CSMA/CA используются небольшие временные интервалы между передаваемыми пакетами от конкретной станции. Передающая станция после окончания передачи пакета переходит в состояние ожидания на короткий интервал времени, прежде чем начать новую передачу.

? *Контрольные вопросы и задания*

1. Раскройте сущность топологии «логическая шина».
2. Поясните, что отражает обозначение классов сетей Ethernet.
3. Перечислите основные типы Ethernet.
4. Проведите сравнительный анализ 10Base-5, 10Base-2, 10Base-T, 10Base-F.
5. Перечислите ранние модификации Ethernet.
6. Сформулируйте основные достоинства технологии Fast Ethernet.
7. Перечислите основные категории Fast Ethernet.

8. Проанализируйте отличия Fast Ethernet и Ethernet.

9. Опишите использование коаксиального кабеля в Fast Ethernet.

10. Опишите процесс построения сети на основе маркерного кольца.

11. Приведите структуру сети на основе маркерного кольца.

12. Сравните основные характеристики сетей Token Ring и FDDI.

13. Перечислите основные характеристики Gigabit Ethernet.

14. Изложите возможности компонентов беспроводной среды.

15. Назовите способы передачи данных.

16. Прокомментируйте основные недостатки инфракрасных сетей.

17. Изложите правила стандарта IEEE 802.11n.

РАЗДЕЛ 5
РАСШИРЕНИЕ ЛВС И ГЛОБАЛЬНЫЕ СЕТИ

5.1. МОДЕМЫ. МЕЖДУНАРОДНЫЕ СТАНДАРТЫ МОДЕМОВ

Модем (аббревиатура, составленная из слов модулятор-демодулятор) – устройство, применяющееся в системах связи и выполняющее функцию модуляции и демодуляции. Модулятор осуществляет модуляцию, т. е. изменяет характеристики несущего сигнала в соответствии с изменениями входного информационного сигнала, демодулятор осуществляет обратный процесс. Частным случаем модема является широко применяемое периферийное устройство для компьютера, позволяющее ему связываться с другим компьютером, оборудованным модемом, через телефонную сеть (телефонный модем) или кабельную сеть (кабельный модем).

Типы модемов для компьютеров:

• по исполнению:

внешние – подключаются к COM- или USB-порту, обычно имеют внешний блок питания (существуют USB-модемы, питающиеся от USB, и LPT-модемы);

внутренние – устанавливаются внутрь компьютера в слот ISA, PCI, PCMCIA, AMR, CNR;

встроенные – являются внутренней частью устройства, например ноутбука или док-станции;

• по принципу работы:

аппаратные – все операции преобразования сигнала, поддержка физических протоколов обмена производятся встроенным в модем вычислителем (например, с использованием контроллера). Также в аппаратном модеме присутствует постоянное запоминающее устройство, в котором записана микропрограмма, управляющая модемом;

винмодемы – аппаратные модемы, лишенные постоянного запоминающего устройства с микропрограммой. Микропрограмма такого модема хранится в памяти компьютера, к которому подключен модем. Винмодем работоспособен только при наличии драйверов, которые были написаны исключительно под операционные системы семейства MS Windows;

полупрограммные – часть функций модема в них выполняет компьютер, к которому подключен модем;

программные – все операции по кодированию сигнала, проверке на ошибки и управление протоколами реализованы программно и производятся центральным процессором компьютера; при этом в модеме находятся аналоговая схема и преобразователи: АЦП, ЦАП, контроллер интерфейса (например USB);

• по типу:

аналоговые – наиболее распространенный тип модемов для обычных коммутируемых телефонных линий;

ISDN – модемы для цифровых коммутируемых телефонных линий;

DSL – используются для организации выделенных (некоммутируемых) линий через обычную телефонную сеть. Отличаются от коммутируемых модемов кодированием сигналов. Обычно позволяют одновременно с обменом данными осуществлять использование телефонной линии в обычном порядке;

кабельные – используются для обмена данными по специализированным кабелям, к примеру, через кабель коллективного телевидения по протоколу DOCSIS;

радио;

спутниковые;

PLC – используют технологию передачи данных по проводам бытовой электрической сети.

Наиболее распространены в настоящее время:

– внутренний программный модем;

– внешний аппаратный модем;

– встроенные в ноутбуки, нетбуки модемы.

Перечислим основные составные устройства модема:

порты ввода-вывода – схемы, предназначенные для обмена данными между телефонной линией и модемом, с одной стороны, и модемом и компьютером – с другой. Для взаимодействия с аналоговой телефонной линией зачастую используется трансформатор;

сигнальный процессор – обычно модулирует исходящие сигналы и демодулирует входящие на цифровом уровне в соответствии с используемым протоколом передачи данных;

контроллер – управляет обменом с компьютером;

микросхемы памяти:

• ROM – энергонезависимая память, в которой хранится микропрограмма управления модемом – прошивка, включающая наборы команд и данных для управления модемом, все поддерживаемые коммуникационные протоколы и интерфейс с компьютером. Обновление прошивки модема доступно в большинстве современных моделей (в руководстве пользователя имеется описание специальной процедуры). Для обеспечения возможности перепрошивки для хранения микропрограмм применяется флеш-память (EEPROM). Флеш-память позволяет легко обновлять микропрограмму модема, исправляя ошибки разработчиков и расширяя возможности устройства. В некоторых моделях внешних модемов она также используется для записи входящих голосовых и факсимильных сообщений при выключенном компьютере;

• NVRAM – энергонезависимая электрически перепрограммируемая память, в которой хранятся настройки модема. Пользователь может изменять установки, например, используя набор AT-команд;

• RAM – оперативная память модема, используется для буферизации принимаемых и передаваемых данных, работы алгоритмов сжатия и прочего.

Существуют модемы с дополнительными возможностями:

• *факс-модем* – позволяет компьютеру, к которому он присоединен, передавать и принимать факсимильные изображения на другой факс-модем или обычную факс-машину;

• *голосовой модем* – имеет функцию оцифровки сигнала с телефонной линии и воспроизведения произвольного звука в линию. Часть голосовых модемов имеет встроенный микрофон.

Международные стандарты модемов также называются протоколами, наборами правил, которые управляют информационным обменом взаимодействующих устройств.

Все протоколы, регламентирующие те или иные аспекты функционирования модемов, могут быть отнесены к двум большим группам:

1) международные;

2) фирменные.

С функциональной точки зрения модемные протоколы могут быть разделены на следующие группы:

– протоколы, определяющие нормы взаимодействия модема с каналом связи (V.2, V.25);

– протоколы, регламентирующие соединение и алгоритмы взаимодействия модема и DTE (V.10, V.11, V.24, V.25, V.25bis, V.28);

– протоколы модуляции, определяющие основные характеристики модемов, предназначенных для коммутируемых и выделенных телефонных каналов. К ним

относятся такие протоколы, как V.17, V.22, V.32, V.34, HST, ZyX, и большое количество других;

– протоколы защиты от ошибок (V. 41, V. 42, MNP1–MNP4);

– протоколы сжатия передаваемых данных, такие как MNP5, MNP7, V.42bis;

– протоколы, определяющие процедуры диагностики модемов, испытания и измерения параметров каналов связи (V.51, V.52, V.53, V.54, V.56);

– протоколы согласования параметров связи на этапе ее установления, например V.8.

Приставки bis и ter в названиях протоколов обозначают соответственно вторую и третью модификации существующих протоколов или протокол, связанный с исходным протоколом. При этом исходный протокол, как правило, остается поддерживаемым.

5.2. РАСШИРЕНИЕ ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ. СОЗДАНИЕ БОЛЬШИХ СЕТЕЙ. МОСТЫ, МАРШРУТИЗАТОРЫ, ШЛЮЗЫ

Сигнал при перемещении по сети ослабевает. Для того чтобы противодействовать этому ослабеванию, можно использовать повторители и (или) усилители, которые усиливают сигналы, проходящие через них по сети.

Повторители используются в сетях с цифровым сигналом и обеспечивают надежную передачу сигнала на большие расстояния, нежели обычно позволяет тип носителя. При получении ослабленного сигнала повторитель его очищает, увеличивая мощность, и посылает дальше, к следующему сегменту.

Повторитель является многопортовым устройством для объединения нескольких сегментов сети (рис. 5.1).

Усилители используют аналоговый сигнал. Аналоговые сигналы могут переносить как голос, так и данные – носитель делится на несколько каналов, так что разные

частоты могут передаваться параллельно. Усилители и повторители действуют на физическом уровне OSI.

Рис. 5.1. Повторитель

Мост (рис. 5.2) функционирует, в первую очередь, как повторитель – он может получать данные из любого сегмента, однако более разборчив в передаче сигналов, чем повторитель. Если получатель пакета находится в том же физическом сегменте, что и мост, то мост знает, что пакет уже достиг цели и мост больше не нужен. Однако если получатель пакета находится в другом физическом сегменте, мост знает, что его надо переслать. Эта обработка помогает уменьшить загрузку сети (например, сегмент не получает не относящиеся к нему сообщения).

Рис. 5.2. Мост

Мосты могут соединять сегменты, которые используют разные типы носителей (кабелей), и сети с разными видами доступа к носителю – например, сеть Internet и сеть Token Ring. Примером таких устройств являются мосты *трансляторы*, которые осуществляют преобразование между различными методами доступа к носителю, позволяя связывать сети разных типов. Другой специальный тип моста – *прозрачный*, или *интеллектуальный*, мост – периодически изучает, куда направлять получаемые им пакеты. Он делает это посредством непрерывного построения специальных таблиц, добавляя в них по мере необходимости элементы.

Недостатком мостов является то, что они передают данные дольше, чем повторители, так как проверяют адрес сетевой карты получателя пакета.

Концентратор – устройство, к которому подключаются сетевые объекты при топологии «звезда»; играет роль разделителя сигналов (рис. 5.3). Концентратор принимает сигнал, поступивший в него из одного порта, и распределяет его по всем остальным своим портам. Некоторые концентраторы перед тем, как передать поступивший слабый сигнал, усиливают его.

Рис. 5.3. Концентратор

Концентраторы бывают трех типов: пассивные, активные и интеллектуальные. *Пассивный концентратор* – самое простое устройство, он получает пакеты, приходящие из одного порта, и отправляет их во все остальные. *Активный концентратор*, обладая всеми свойствами пассивного концентратора, использует функцию «сохранить и отправить», которая позволяет считывать данные перед

отправкой, восстанавливает некоторые «поврежденные» пакеты и перераспределяет отправку остальных, может усилить сигнал перед дальнейшей отправкой. Некоторые активные концентраторы могут сообщить о некорректно работающих устройствах в сети – произвести некоторую диагностику локальной сети. *Интеллектуальный концентратор* имеет ряд преимуществ перед пассивным и активным концентраторами. Помимо всех свойств и функций, которые доступны первым двум типам, интеллектуальный концентратор позволяет централизованно управлять локальной сетью. Он может автоматически изменять скорость передачи данных для подключенных к нему устройств.

В отличие от концентраторов, которые полностью воплощают в себе идеологию общей разделяемой среды и превращают сеть в единый домен, **коммутаторы** – более интеллектуальные устройства, способные анализировать адрес назначения кадра и передавать его не всем станциям, а только адресату.

До появления коммутатора задача разделения сети на сегменты полностью решалась с помощью мостов, которые в настоящее время практически не используются. Основной же принцип действия мостов и коммутаторов остался неизменным. Именно поэтому коммутаторы иногда называют многопортовыми мостами.

Конструктивно коммутатор представляет собой устройство для деления сети на множество сегментов (рис. 5.4). В сети Internet коммутаторы используют в своей работе алгоритм прозрачного моста. Алгоритм прозрачного моста подразумевает, что коммутатор «обучается» в процессе своей работы. Коммутатор строит свою адресную таблицу на основе пассивного наблюдения за трафиком, циркулирующим в сети. В начальный момент времени коммутатор не знает ничего об адресах подключенных к его портам компьютеров. По мере того как подключенные к портам

коммутатора узлы начинают проявлять активность, коммутатор анализирует содержимое адресов отправителя кадров, что позволяет делать вывод о принадлежности того или иного узла к тому или иному порту коммутатора.

Рис. 5.4. Коммутатор

В начальный момент времени коммутатор работает в неразборчивом режиме, передавая полученные кадры на все порты. Построив таблицу адресов, коммутатор может передавать полученные кадры не на все порты, а только по адресу назначения; если на порт коммутатора поступает кадр с адресом назначения, приписанным к другому порту коммутатора, то кадр передается между портами. Этот процесс называется *продвижением кадра между портами*. Если же коммутатор определяет, что адрес назначения приписан к тому порту, на который поступил данный кадр, то кадр отбрасывается или отфильтровывается, т. е. удаляется из буфера порта. Такой процесс называется *фильтрацией*.

Коммутаторы позволяют строить изолированные друг от друга локальные сети. Изоляция виртуальных сетей друг от друга происходит на канальном уровне. Это означает, что передача кадров между различными виртуальными сетями на основании адреса канального уровня невозможна.

При построении нескольких изолированных друг от друга сетей можно задействовать несколько коммутаторов. Но следует учитывать, что использование одного коммутатора не только снижает стоимость сети, но и по-

зволяет более гибко и рационально использовать порты коммутатора. Поскольку узлы различных сетей изолированы друг от друга на канальном уровне, для объединения таких сетей в единую сеть требуется привлечение сетевого, или 3-го уровня. Понятие 3-го уровня соответствует градации уровня сетевой модели OSI. Для обеспечения таких связей используются специальные коммутаторы, получившие название «коммутаторы 3-го уровня». По аналогии коммутаторы, работающие только на канальном уровне, называют коммутаторами 2-го уровня.

Для обеспечения высокой сквозной пропускной способности сети и соответствующего качества обслуживания необходимо, чтобы загрузка оптимально распределялась между всеми элементами сети и поток данных между клиентами и серверами был равномерным.

Коммутаторы 2-го и 3-го уровней не всегда справляются с нагрузкой. Технология коммутации на 4-м уровне включает возможности управления производительностью и трафиком коммутаторов первых двух уровней, дополняя их новыми интеллектуальными функциями, в том числе возможностями управления серверами и приложениями.

Коммутаторы 4-го уровня используют информацию, которая содержится в заголовках пакетов и относится к уровню 3 и 4 стека протоколов (такую, как IP-адреса источника и приемника). На основании этой информации они могут принимать интеллектуальные решения о перенаправлении трафика того или иного сеанса.

Маршрутизатор представляет собой сетевое коммуникативное устройство, которое может связывать два и более сетевых сегмента (или подсети) (рис. 5.5).

Рис. 5.5. Маршрутизатор

Маршрутизатор реализует протоколы физического, канального и сетевого уровней. Специальные сетевые процессы соединяют части маршрутизатора в единое целое. Поэтому соединение пар коммуникационных сетей производится через маршрутизаторы, которые осуществляют необходимые преобразования указанных протоколов. Сетевые процессы выполняют взаимодействие соединяемых сетей. Маршрутизатор, работая с несколькими каналами, направляет в какой-нибудь из них очередной блок данных. Маршрутизаторы обмениваются данными об изменении структуры сетей, трафике и его состоянии. Благодаря этому выбирается оптимальный маршрут следования блока данных в разных сетях от абонентской системы к системе-получателю.

Маршрутизатор для фильтрации информации использует не адрес сетевой карты компьютера, а информацию о сетевом адресе, передаваемую в относящиеся к сетевому уровню части пакета (посредством стандарта).

Коммутационная панель – одна из составных частей структурированной кабельной системы, которая представляет собой множество соединительных разъемов, расположенных на лицевой стороне панели; на тыльной стороне находятся контакты для фиксированного соединения с кабелями (рис. 5.6). Коммутационная панель является пассивным сетевым оборудованием.

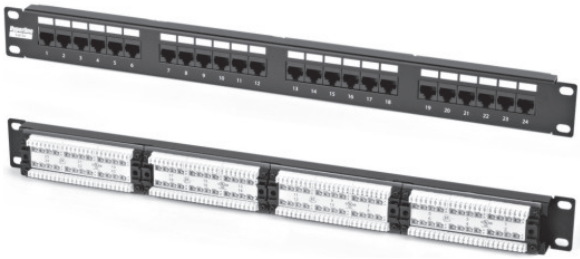

Рис. 5.6. Коммутационная панель

Трансивер – устройство для передачи и приема сигнала между двумя физически разными средами системы связи (рис. 5.7).

Рис. 5.7. Трансивер

Шлюз (рис. 5.8) является наиболее сложной ретрансляционной системой, обеспечивающей взаимодействие сетей с различным набором протоколов всех семи уровней. В свою очередь, наборы протоколов могут опираться на различные типы физических средств соединения.

Рис. 5.8. Шлюз

Шлюзы оперируют на верхних уровнях модели OSI и представляют наиболее развитый метод подсоединения

сетевых сегментов и компьютерных сетей. Необходимость в сетевых шлюзах возникает при соединении двух систем, имеющих различную архитектуру. Например, шлюз приходится использовать при соединении сетей с протоколами TCP/IP и SNA.

В качестве шлюза чаще всего выступает отдельный компьютер, на котором запускается шлюзовое программное обеспечение и производятся преобразования, позволяющие взаимодействовать несходным системам.

Другой функцией шлюзов является преобразование протоколов. При получении сообщения IPX/SPX для клиента TCP/IP шлюз преобразует сообщения в протокол TCP/IP.

Точка доступа – представитель активного типа устройств, необходимых для объединения компьютеров в беспроводную сеть. Его аналогом является проводной коммутатор, а в отдельных случаях и маршрутизатор.

Точка доступа (рис. 5.9) в силу особенностей беспроводной среды передачи данных является достаточно интеллектуальным устройством и часто позволяет осуществлять дополнительное управление локальной сетью. Например, в современных точках доступа имеется аппаратная поддержка работы DNS- и DHCP-серверов, что позволяет строить структурированные локальные сети, представляющие собой упрощенный вариант доменной структуры.

Рис. 5.9. Точка доступа

Кроме того, точка доступа одновременно является брандмауэром, способным фильтровать и блокировать пакеты, а также, что самое главное, содержит информацию, необходимую для аутентификации пользователей.

В беспроводной сети большое значение имеет **антенна**, особенно если к ней подключено активное сетевое оборудование (например, точка доступа, концентратор, маршрутизатор и т. д.). Хорошая антенна позволяет сети работать с максимальной отдачей, достигая при этом своих теоретических пределов дальности сигнала и скорости передачи данных.

Антенны бывают *всенаправленные* (рис. 5.10) и *узконаправленные* (рис. 5.11), а также различаются вариантом использования: внутри здания или на открытом воздухе.

Рис. 5.10. Всенаправленная антенна

Рис. 5.11. Узконаправленная антенна

Кроме того, основным показателем возможностей антенны является ее коэффициент усиления сигнала. Например, узконаправленная антенна позволяет достичь большего радиуса сети, что используют, когда необходимо соединить два удаленных сегмента беспроводной

сети. Всенаправленная антенна распространяет сигнал вокруг себя, что дает возможность другим устройствам, установленным рядом, взаимодействовать друг с другом. Использование антенны с большим коэффициентом усиления позволяет увеличить радиус сети и соответственно повысить уровень сигнала, особенно на дальних точках подключения.

Локальная сеть с большим количеством компьютеров редко обходится без **монтажного шкафа**, который позволяет собрать в одном месте все или почти все центральные органы управления сетью. В шкафу обычно располагают большую часть активного оборудования сети (коммутаторы, маршрутизаторы, модемы) и часть пассивного оборудования (кросс-панели, кросс-кабели и т. п.).

В зависимости от размера и варианта исполнения в шкаф можно также устанавливать серверы стоечного типа, блоки бесперебойного питания, KVM-переключатели (для вывода изображения с серверов на один монитор) и т. д.

Существуют разные варианты монтажных шкафов, различающиеся в основном только двумя показателями – типом исполнения (напольный, подвесной) и габаритами. Кроме того, различия могут быть в конструкции шкафа, наличии охлаждающей системы, способе подвода кабелей и др.

Размеры шкафа и вариант его исполнения подбирают исходя из количества компьютеров в сети и количества оборудования, которое планируют установить в шкаф. Если в сети подключено 30–40 компьютеров, то вполне достаточным будет использование подвесного варианта шкафа (рис. 5.12).

Кросс-панель является неотъемлемым атрибутом любой большой локальной сети, которая использует монтажные шкафы. Кросс-панели бывают только определенного размера, который зависит от размеров самого монтажного шкафа.

Рис. 5.12. Монтажный шкаф

Основное предназначение кросс-панели – обеспечение удобного способа монтажа кабеля в контактных площадках разъемов с последующим соединением этих разъемов с портами на активном сетевом оборудовании, установленном в монтажном шкафу.

Внешний вид кросс-панели зависит от количества и типа портов, которые располагаются на ее передней панели, а также от габаритов. Как правило, на кросс-панели не бывает менее 16 портов, что связано со стандартными размерами стоек в монтажном шкафу.

Количество кросс-панелей подбирается в зависимости от количества компьютеров локальной сети и другого оборудования, которому нужно подключение к порту на кросс-панели. Как правило, стандартная кросс-панель содержит от 24 до 48 портов, которые могут располагаться как в один, так и в несколько рядов (рис. 5.13).

Для облегчения монтажа кабеля и создания необходимой проектной документации каждый порт на кросс-панели пронумерован. Кроме того, рядом с портом обычно находится специальный участок, на котором маркером можно сделать любую нужную короткую запись.

Рис. 5.13. Кросс-панель

На задней панели кросс-панели находится система разводки портов, т. е. непосредственно контактные площадки портов, которые используются для зажима в них проводников кабеля или монтажа оптоволоконных жил. Каждый порт снабжается фиксирующим устройством или скобами, позволяющими закрепить кабель, идущий к конкретному порту.

Присутствует также общая система фиксирования, позволяющая зафиксировать сразу все кабели, исключая тем самым возможность потери контакта.

Патч-корд и **кросс-корд** – это кабели небольшой длины с обжатыми коннекторами. Они являются частью сети, построенной с применением кабеля «витая пара».

Патч-корд (рис. 5.14), в отличие от кросс-корда, сделан из более мягкого кабеля и применяется для подключения компьютеров и другого сетевого оборудования к сетевым розеткам или непосредственно к портам на активном оборудовании. Длина кабеля согласно существующим стандартам не должна превышать 5 м, однако на практике часто используют кабель длиной до 10 м.

Рис. 5.14. Патч-корд

Кросс-корд имеет гораздо меньшую длину (как правило, не более 1 м) и используется в монтажном шкафу для соединения портов кросс-панели с портами на активном оборудовании или соединения активного оборудования между собой.

Когда речь идет о кабеле, используемом для создания проводных вариантов сети, то без **коннекторов** он не представляет никакой ценности. Именно коннекторы завершают целостность кабеля и позволяют использовать его по назначению – для передачи данных между отправителем и получателем. С помощью коннекторов кабель подключается к нужным разъемам на оборудовании, как активном, так и пассивном.

Коннектор RJ-45 (рис. 5.15) используется для обжима кабеля «витая пара», который применяется для создания локальных сетей, например, стандарта 100Base-TX. Внешне этот коннектор похож на RJ-11, используемый для обжима двух- или четырехжильного телефонного кабеля, но он шире и содержит в два раза больше контактных групп.

Рис. 5.15. Коннектор RJ-45

Для фиксации коннектора в разъеме используется пластиковый фиксатор. В паре с коннектором RJ-45, как правило, идет специальный защитный колпачок из мягкого материала, например обрезиненного пластика, который надевается на коннектор и часть кабеля, скрывая и защищая тем самым наиболее уязвимое место – место обжима.

Особенностью коннектора является его ограниченный срок службы.

Терминатор (рис. 5.16) представляет собой своего рода заглушку, которая необходима для того, чтобы препятствовать появлению отбитого сигнала.

Рис. 5.16. Терминатор

Терминаторы устанавливаются на обоих концах магистрали, при этом один из них обязательно заземляется. Если терминатор не установить, то сигнал, поступая в «никуда», может привести не только к задержкам неопределенной длительности, но и к выходу сети из строя.

Различные виды **оптических муфт** применяются в оптоволоконных сетях для защиты мест соединений кабелей. С помощью таких муфт можно вывести часть волокон из кабеля и, используя различные патч-корды с соответствующими коннекторами, присоединять к сети активное оборудование.

Тупиковые муфты (рис. 5.17) используют в случаях усиленных нагрузок на сеть или в местах с малоблагоприятными условиями для прокладки линии связи. Эти муфты специально делают устойчивыми к температурным перепадам, повышенной влажности и иным разрушающим факторам. Конструктивно муфту делают так, чтобы можно было легко установить ее и при дальнейшей эксплуатации получать доступ к оптическому кабелю без каких-либо вспомогательных инструментов.

Рис. 5.17. Тупиковая муфта

Розетка RJ-45, как и любая другая розетка, предназначена для обеспечения контакта между носителем и потребителем, в нашем случае – между передающей средой и компьютером или другим сетевым устройством. Подразумевается, что речь идет о локальной сети, использующей один из стандартов на основе кабеля «витая пара».

Розетки применяются при необходимости. Использование сетевых розеток делает кабельную систему более устойчивой к разного рода неприятностям в виде обрывов кабеля, пропадания контактов в соединениях.

Внешний вид сетевой розетки зависит от следующих факторов:

– категории (чем выше категория, тем лучше качество розетки, выше уровень безопасности, лучше способ обжима проводников кабеля);

– типа и способа крепления розетки. Производят розетки с внутренним и внешним способами монтажа. Внутренний способ монтажа подразумевает монтаж розетки в монтажной коробке, для которой в стене делается соответствующее отверстие. Внешний вариант монтажа позволяет крепить розетку прямо на стену с помощью шурупов, встраивать ее в сетевой короб или просто приклеивать к гладкой поверхности с помощью двухстороннего скотча;

– наличия дополнительных портов. Часто на розетке присутствуют дополнительные разъемы, например RJ-45 или RJ-11, что повышает ее универсальность, позволяя использовать одну конструкцию для обслуживания нескольких устройств.

Внешний вид розетки RJ-45 показан на рисунке 5.18.

Рис. 5.18. Розетка RJ-45

5.3. ПЕРЕДАЧА ДАННЫХ В ГВС. АНАЛОГОВАЯ СВЯЗЬ, КОММУТИРУЕМЫЕ ЛИНИИ

Глобальные сети, которые также называют территориальными компьютерными сетями, служат для того, чтобы предоставлять свои сервисы большому количеству конечных абонентов, разбросанных по большой территории – в пределах области, региона, страны, континента или всего земного шара. Ввиду большой протяженности каналов связи построение глобальной сети требует очень больших затрат, в том числе:

– стоимость кабелей и работ по их прокладке;

– затраты на коммутационное оборудование и промежуточную усилительную аппаратуру, обеспечивающую необходимую полосу пропускания канала;

– эксплуатационные затраты на постоянное поддержание в работоспособном состоянии разбросанной по большой территории аппаратуры сети.

Типичными абонентами глобальной компьютерной сети являются локальные предприятия, расположенные в разных городах и странах, которым нужно обмениваться данными между собой. Услугами глобальных сетей пользуются также и отдельные компьютеры. Крупные компьютеры класса мейнфреймов обычно обеспечивают доступ к корпоративным данным, в то время как

персональные компьютеры используются для доступа и к корпоративным и к публичным данным.

Глобальные сети обычно создаются крупными телекоммуникационными компаниями для оказания платных услуг абонентам. Такие сети называют *публичными*, или *общественными*. Существуют также такие понятия, как оператор сети и поставщик услуг сети. **Оператор сети** – это компания, которая поддерживает нормальную работу сети. **Поставщик услуг**, часто называемый также **провайдером**, – та компания, которая оказывает платные услуги абонентам сети. Владелец, оператор, поставщик услуг могут объединяться в одну компанию.

Гораздо реже глобальная сеть полностью создается какой-нибудь крупной корпорацией для своих внутренних нужд. В этом случае сеть называется *частной*. Очень часто встречается и промежуточный вариант – корпоративная сеть пользуется услугами или оборудованием общественной глобальной сети, но дополняет эти услуги или оборудование своими собственными. Наиболее типичным примером является аренда каналов связи, на основе которых создаются собственные территориальные сети.

Кроме вычислительных глобальных сетей существуют и другие виды территориальных сетей передачи информации. В первую очередь это телефонные и телеграфные сети, работающие на протяжении многих десятков лет, а также телексная сеть.

Ввиду большой стоимости глобальных сетей существует долговременная тенденция создания единой глобальной сети, которая может передавать данные любых типов: компьютерные данные, телефонные разговоры, факсы, телеграммы, телевизионное изображение, телетекст (передача данных между двумя терминалами), видеотекст (получение хранящихся в сети данных на свой терминал) и т. д. Пока что каждый тип сети существует

отдельно, и наиболее тесная интеграция достигнута в области использования общих первичных сетей, с помощью которых сегодня создаются постоянные каналы в сетях с коммутацией абонентов. Каждая из технологий (как компьютерных сетей, так и телефонных) старается передавать «чужой» для нее трафик с максимальной эффективностью, а попытки создать интегрированные сети на новом витке развития технологий продолжаются в широкополосной (высокоскоростной) сети с интеграцией услуг.

Сети будут основываться на технологии ATM как универсальном транспорте и поддерживать различные службы верхнего уровня для распространения конечным пользователям сети разнообразной информации – компьютерных данных, аудио- и видеоинформации, а также организации интерактивного взаимодействия пользователей.

Хотя в основе локальных и глобальных вычислительных сетей лежит один и тот же метод – метод коммутации пакетов, глобальные сети имеют достаточно много отличий от локальных сетей. Эти отличия касаются как принципов работы (например, принципы маршрутизации почти во всех типах глобальных сетей, кроме сетей TCP/IP, основаны на предварительном образовании виртуального канала), так и терминологии. Поэтому целесообразно изучение глобальных сетей начать с основных понятий и определений.

В идеале глобальная вычислительная сеть должна передавать данные абонентов любых типов, которые есть на предприятии и нуждаются в удаленном обмене информацией.

Большинство территориальных компьютерных сетей в настоящее время обеспечивает только передачу компьютерных данных, но количество сетей, которые могут передавать остальные типы данных, постоянно растет.

Однако в последнее время функции глобальной сети, относящиеся к верхним уровням стека протоколов, стали играть заметную роль в вычислительных сетях. Это связано, в первую очередь, с популярностью информации, предоставляемой публичной сетью. Список высокоуровневых услуг, которые предоставляет Internet, достаточно широк.

В результате глобальные и локальные сети постепенно сближаются за счет взаимопроникновения технологий разных уровней – от транспортных до прикладных.

Типичный пример структуры глобальной компьютерной сети приведен на рисунке 5.19.

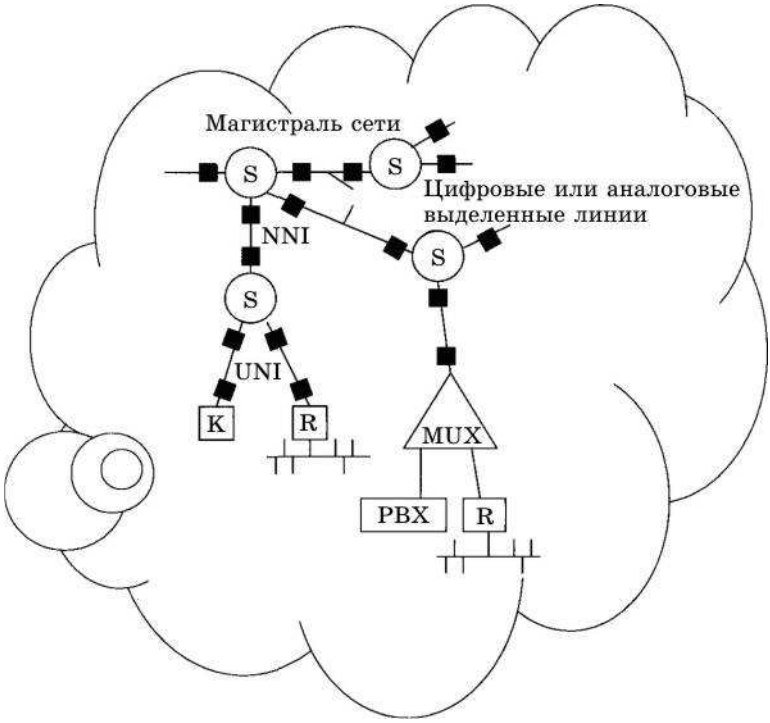

Рис. 5.19. Пример структуры глобальной сети

Сеть строится на основе некоммутируемых (выделенных) каналов связи, которые соединяют коммутаторы глобальной сети между собой. Коммутаторы называют также центрами коммутации пакетов (ЦКП), т. е. они являются коммутаторами пакетов, которые в разных технологиях глобальных сетей могут иметь и другие названия – кадры, ячейки. Как и в технологиях локальных сетей, принципиальной разницы между этими единицами данных нет. Однако в некоторых технологиях есть традиционные названия, которые к тому же часто отражают специфику обработки пакетов.

Коммутаторы устанавливаются в тех географических пунктах, в которых требуется ответвление или слияние потоков данных конечных абонентов либо магистральных каналов, переносящих данные многих абонентов. Естественно, выбор мест расположения коммутаторов определяется многими соображениями, в том числе возможностью обслуживания коммутаторов квалифицированным персоналом, наличием выделенных каналов связи в данном пункте, надежностью сети, определяемой избыточными связями между коммутаторами.

Абоненты сети подключаются к коммутаторам в общем случае также с помощью выделенных анналов связи. Эти каналы связи имеют более низкую пропускную способность, чем магистральные каналы, объединяющие коммутаторы, иначе сеть не справилась бы с потоками данных своих многочисленных пользователей. Для подключения конечных пользователей допускается использование коммутируемых каналов, т. е. каналов телефонных сетей, хотя в таком случае качество транспортных услуг обычно ухудшается. Замена выделенного канала на коммутируемый принципиально ничего не меняет, но вносятся дополнительные задержки, отказы и разрывы канала по вине сети с коммутацией каналов, которая в таком случае становится промежуточным зве-

ном между пользователем и сетью с коммутацией пакетов. Кроме того, в аналоговых телефонных сетях канал обычно имеет низкое качество из-за высокого уровня шумов. Применение коммутируемых каналов на магистральных связях коммутатор-коммутатор возможно, но по изложенным выше причинам нежелательно.

В глобальной сети наличие большого качества абонентов с невысоким средним уровнем трафика весьма полезно – именно в этом случае начинают в наибольшей степени проявляться выгоды метода коммутации пакетов. Если же абонентов мало и каждый из них создает трафик большой интенсивности (по сравнению с возможностями каналов и коммутаторов сети), то равномерное распределение во времени пульсаций трафика становится маловероятным, и для качественного обслуживания абонентов необходимо использовать сеть с низким коэффициентом нагрузки.

Конечные узлы глобальной сети более разнообразны, чем конечные узлы локальной сети.

При передаче данных через глобальную сеть мосты и маршрутизаторы работают в соответствии с той же логикой, что и при соединении локальных сетей. Мосты, которые в этом случае называются удаленными, строят таблицу MAC-адресов на основании проходящего через них трафика и по данным этой таблицы принимают решение – передавать кадры в удаленную сеть или нет. В отличие от своих локальных собратьев удаленные мосты выпускаются и сегодня, привлекая своих интеграторов тем, что их не нужно конфигурировать, а в удаленных офисах, где нет квалифицированного обслуживающего персонала, это свойство оказывается очень полезным. Маршрутизаторы принимают решение на основании номера сети пакета какого-либо протокола сетевого уровня и, если пакет нужно переправить следующему маршрутизатору по глобальной сети, упаковывают его в кадр этой

сети, снабжают соответствующим аппаратным адресом следующего маршрутизатора и отправляют в глобальную сеть.

Мультиплексоры «голос-данные» предназначены для совмещения в рамках одной территориальной сети компьютерного и голосового трафиков. Так как рассматриваемая глобальная сеть передает данные в виде пакетов, мультиплексоры «голос-данные», работающие на сети данного типа, упаковывают голосовую информацию в кадры или пакеты территориальной сети и передают их ближайшему коммутатору точно так же, как и любой конечный узел глобальной сети, т. е. мост или маршрутизатор. Если глобальная сеть поддерживает приоритизацию трафика, то кадрам голосового трафика мультиплексор присваивает наивысший приоритет, чтобы коммутаторы обрабатывали и продвигали их в первую очередь. Приемный узел на другом конце глобальной сети также должен быть мультиплексором «голос-данные», который должен понять, что за тип данных находится в пакете – замеры голоса или пакеты компьютерных данных, и отсортировать эти данные по своим выходам. Голосовые данные направляются офисной АТС, а компьютерные данные поступают через маршрутизатор в локальную сеть. Часто модуль мультиплексора «голос-данные» встраивается в маршрутизатор. Для передачи голоса в наибольшей степени подходят технологии, работающие с предварительным резервированием полосы пропускания для соединения абонентов.

5.4. ПЕРЕДОВЫЕ ТЕХНОЛОГИИ ГВС. ТЕХНОЛОГИЯ АСИНХРОННОЙ ПЕРЕДАЧИ ДАННЫХ (ATM, XDSL)

Передовые технологии глобальных вычислительных сетей:

X.25 – набор протоколов для сетей с коммутацией пакетов;

Freme Relay – усовершенствованная быстрая технология коммутации пакетов переменной длины;

ATM – усовершенствованная технология коммутации пакетов, которая обеспечивает высокоскоростную передачу пакетов фиксированной длины через широкополосные и узкополосные локальные или глобальные сети;

ISDN (цифровая сеть комплексных услуг) – спецификация межсетевой цифровой связи, предназначенной для передачи речи, данных, графики;

FDDI – спецификация, которая описывает высокоскоростную сеть с передачей маркера топологии «кольцо» на основе оптоволокна;

SONET – представитель современных систем, которые реализуют преимущества оптоволоконной технологии;

SMDS – коммутируемая служба, которую предлагают некоторые локальные коммуникационные компании.

Технология асинхронной передачи данных ATM (асинхронный режим передачи) способна передавать речь, данные, факсимильные сообщения, видео в реальном времени, аудиосигналы качества CD, мультимегабитные потоки данных. Это относительно новая технология, требующая специального оборудования и исключительно широкой полосы пропускания.

ATM представляет собой широкополосный метод ретрансляции ячеек, при котором данные передаются ячейками фиксированной длины – по 53 байта (рис. 5.20). Ячейки содержат 48 байтов – собственно передаваемые данные и 5 дополнительных байтов – заголовок ATM. Например, передавая 1000-байтный пакет, ATM разобьет его на 21 кадр и поместит каждый кадр в ячейку. Результат – передача стандартных, единообразных пакетов.

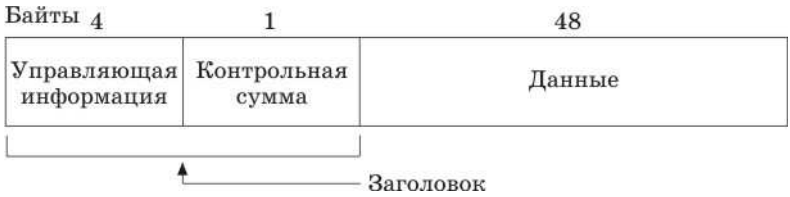

Рис. 5.20. Формат пакета данных ATM

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

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

Технология передачи данных ATM не ограничена конкретным типом среды передачи. Она может использовать существующие среды передачи, разработанные для других коммуникационных систем, в том числе коаксиальный кабель, витую пару, оптоволоконный кабель.

Коммутаторы ATM – это многопортовые устройства, которые могут функционировать как любой из следующих компонентов: концентратор для передачи данных между компьютерами внутри сети, маршрутизатор, который предназначен для высокоскоростной передачи данных в удаленные сети.

Сети ATM предполагают передачу данных при установленном соединении, т. е. сначала устанавливается соединение между источником информации и приемником

и только затем начинается передача пакетов данных, после чего соединение разрывается.

Высокие скорости в ATM обеспечиваются рядом технических решений.

Большое число каналов с временным мультиплексированием можно использовать для параллельной передачи частей одного и того же «объемного» сообщения (статистическое мультиплексирование). При этом цикл синхронизации состоит из отдельных участков, длины участка и ячейки совпадают. Под конкретное сообщение можно выделить N интервалов, совокупность которых называют *виртуальным каналом*. Скорость передачи можно регулировать, изменяя N. Если сеть ATM оказывается перегруженной, то во избежание потери информации и в отличие от коммутации каналов возможна буферизация данных для выравнивания загрузки каналов. Регулирование загрузки (управление потоком) осуществляется периодическим включением (обычно через 32 кадра) RM-ячейки в информационный поток. В эту ячейку промежуточные коммутаторы и конечный узел могут вставлять значения управляющих битов, сигнализирующие о перегрузке или недогрузке канала. RM-ячейка от конечного узла передается в обратном направлении источнику сообщения, который может соответственно изменить режим передачи. В частности, применяется режим занятия всех свободных ресурсов при перегрузке. Таким образом, происходит динамическое перераспределение нагрузки.

Отрицательные квитанции при искажениях сообщений (но не заголовков) возможны только от конечного пункта. Это исключает потери времени в промежуточных пунктах на ожидание подтверждений. Такой способ иногда называют коммутацией кадров (в отличие от коммутации пакетов). Контрольный код (четырехбайтный циклический) по информационной части сообщения имеется только в конце последнего пакета сообщения.

При упрощенной маршрутизации установление соединения выполняется аналогично этой процедуре в TCP/IP. Однако далее номер рассчитанного маршрута помещается в заголовок каждого пакета, и для них не нужно заново определять маршрут по таблицам маршрутизаторов при прохождении через сеть. Такая передача называется *маршрутизацией от источника*. Другими словами, осуществляется передача с установлением соединения (в отличие, например, от IP). При этом клиент направляет серверу запрос в виде специального управляющего кадра. Кадр проходит через промежуточные маршрутизаторы и (или) коммутаторы, в которых соединению (каналу) присваивается номер идентификатора маршрута. Если передача адресована нескольким узлам, то соответствующий номер в коммутаторах присваивается нескольким каналам.

Фиксированная длина пакетов (кадров) упрощает алгоритмы управления и буферизации данных, исключает необходимость инкапсуляции или конвертирования пакетов при смене форматов в промежуточных сетях (если они соответствуют формату ячейки ATM).

Технология DSL (цифровая абонентская линия), предоставляющая доступ к службам цифровой передачи данных по абонентским линиям, является одной из наиболее перспективных. Существует несколько вариантов этой технологии (поскольку их названия отличаются первым словом, весь ряд обозначается аббревиатурой xDSL):

ADSL (асимметричная цифровая абонентская линия) – позволяет передавать и принимать цифровую информацию с высокой скоростью;

SDSL (симметричная цифровая абонентская линия) – предусматривает симметричные, т. е. равные скорости передачи в обоих направлениях;

HDSL (высокоскоростная цифровая абонентская линия) – обеспечивает скорость передачи, соответствую-

щую стандарту DSL (т. е. 1,544 Мбит/с) в обоих направлениях;

VDSL (сверхвысокоскоростная цифровая абонентская линия) – обеспечивает высокую пропускную способность, позволяя достичь скорости передачи данных вплоть до 52 Мбит/с.

? *Контрольные вопросы и задания*

1. Дайте определение термину «модем».
2. Перечислите типы модемов.
3. Опишите основной состав модема.
4. Сравните повторитель и усилитель.
5. Проанализируйте функционирование моста.
6. Объясните, для каких целей служит маршрутизатор.
7. Сравните характеристики узконаправленных и широконаправленных антенн.
8. Поясните отличия патч-корда и кросс-корда.
9. Назовите возможности точки доступа.
10. Перечислите основные передовые технологии.
11. Опишите технологию ATM.
12. Назовите основные варианты технологии DSL.
13. Определите, какую сеть можно создать, имея в наличии:

а) концентратор, витую пару, 8 ПК, пассивные соединители, коннекторы;

б) коммутатор, розетки, соединители, распределительные стойки и полки, маршрутизатор, концентратор, витую пару, 108 ПК.

14. Создайте домашнюю сеть, которая объединяет ПК двух рядом стоящих многоэтажных домов. Подробная информация:

– дома расположены друг напротив друга на расстоянии примерно 80 м;

– в доме *A* пользователи располагаются согласно таблице *A*;

– в доме *B* пользователи располагаются согласно таблице *B*.

Таблица А

Этаж	Подключаемые квартиры	Подключаемые компьютеры	Расстояние от компьютеров до входной двери, м
1	3 смежные	4	12,3; 14; 17,5; 16,6
4	2 напротив	2	13;15
8	2 смежные	2	21; 19
10	4 смежные	4	12; 30,1; 16;17

Таблица В

Этаж	Подключаемые квартиры	Подключаемые компьютеры	Расстояние от компьютеров до входной двери, м
2	1	1	6
4	2 напротив	3	18; 15
5	2 смежные	2	20,5; 19,8

РАЗДЕЛ 6
ЭКСПЛУАТАЦИЯ СЕТЕЙ

6.1. АДМИНИСТРИРОВАНИЕ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ. МОНИТОРИНГ СЕТИ. УПРАВЛЕНИЕ СЕТЬЮ

Корпоративная сеть – сложная система, состоящая из программных, аппаратных и коммуникационных средств, обеспечивающих эффективное распределение вычислительных ресурсов. Основу работы сети составляют сетевые службы.

Базовый набор сетевых служб корпоративной сети:

– службы сетевой инфраструктуры DNS, DHCP, WINS;
– службы файлов и печати;
– службы каталогов;
– службы обмена сообщениями;
– службы доступа к базам данных.

***Администрирование сети*. Сетевое администрирование** – это планирование, установка, настройка, обслуживание корпоративной сети, обеспечение ее надежной, бесперебойной, высокопроизводительной и безопасной работы.

• *Планирование сети*. Несмотря на то что планированием и монтажом больших сетей обычно занимаются специализированные компании-интеграторы, сетевому администратору часто приходится планировать определенные изменения в структуре сети – добавление новых рабочих мест, добавление или удаление сетевых протоколов, добав-

ление или удаление сетевых служб, установку серверов, разбиение сети на сегменты и т. д. Данные работы должны быть тщательно спланированы, чтобы новые устройства, узлы или протоколы включались в сеть или исключались из нее без нарушения целостности сети, без снижения производительности, без нарушения инфраструктуры сетевых протоколов, служб и приложений.

• *Установка и настройка сетевых узлов* (устройств активного сетевого оборудования, персональных компьютеров, серверов, средств коммуникации). Эти работы могут включать замену сетевого адаптера в персональном компьютере с соответствующими настройками, перенос сетевого узла (персонального компьютера, сервера, активного оборудования) в другую подсеть с соответствующими изменениями сетевых параметров узла, добавление или замену сетевого принтера с соответствующей настройкой рабочих мест.

• *Установка и настройка сетевых протоколов*. Данная задача включает выполнение следующих работ: планирование и настройка базовых сетевых протоколов корпоративной сети, тестирование работы сетевых протоколов, определение оптимальных конфигураций протоколов.

• *Установка и настройка сетевых служб*. Корпоративная сеть может содержать большой набор сетевых служб. Основные задачи администрирования сетевых служб:

– установка и настройка служб сетевой инфраструктуры (службы DNS, DHCP, WINS, службы маршрутизации, удаленного доступа и виртуальных частных сетей);

– установка и настройка служб файлов и печати, которые в настоящее время составляют значительную часть всех сетевых служб;

– администрирование служб каталогов, составляющих основу корпоративной системы безопасности и управления доступом к сетевым ресурсам;

– администрирование служб обмена сообщениями (системы электронной почты);

– администрирование служб доступа к базам данных.

• *Поиск неисправностей*. Сетевой администратор должен уметь обнаруживать широкий спектр неисправностей – от поломки сетевого адаптера на рабочей станции пользователя до сбоев отдельных портов коммутаторов и маршрутизаторов, а также неправильные настройки сетевых протоколов и служб.

• *Поиск узких мест сети и повышение эффективности работы сети*. В задачу сетевого администрирования входит анализ работы сети и определение наиболее узких мест, требующих либо замены сетевого оборудования, либо модернизации рабочих мест, либо изменения конфигурации отдельных сегментов сети.

• *Мониторинг сетевых узлов* – включает наблюдение за функционированием сетевых узлов и корректностью выполнения возложенных на данные узлы функций.

• *Мониторинг сетевого трафика* – позволяет обнаружить и ликвидировать различные виды проблем: высокую загруженность отдельных сетевых сегментов, чрезмерную загруженность отдельных сетевых устройств, сбои в работе сетевых адаптеров или портов сетевых устройств, нежелательную активность или атаки злоумышленников (распространение вирусов, атаки хакеров и др.).

• *Обеспечение защиты данных*. Защита данных включает большой набор различных задач: резервное копирование и восстановление данных, разработку и осуществление политики безопасности учетных записей пользователей и сетевых служб (требования к сложности паролей, частота смены паролей), построение защищенных коммуникаций (применение протокола IPSec, построение виртуальных частных сетей, защита беспроводных сетей), планиро-

вание, внедрение и обслуживание инфраструктуры открытых ключей.

Мониторинг сети. Термином **мониторинг сети** называют работу системы, которая выполняет постоянное наблюдение за компьютерной сетью в поисках медленных или неисправных систем и при обнаружении сбоев сообщает о них сетевому администратору с помощью почты, телефона или других средств оповещения. Эти задачи являются подмножеством задач управления сетью.

В то время как система обнаружения вторжений следит за появлением угроз извне, система мониторинга сети выполняет наблюдение за сетью в поисках проблем, вызванных перегруженными и (или) отказавшими серверами, другими устройствами или сетевыми соединениями. Например, для того чтобы определить состояние web-сервера, программа, выполняющая мониторинг, может периодически отправлять запрос HTTP на получение страницы; для почтовых серверов можно отправить тестовое сообщение по SMTP и получить ответ по IMAP или POP3.

Неудавшиеся запросы (например, в том случае, когда соединение не может быть установлено и завершается по тайм-ауту или когда сообщение не было доставлено) обычно вызывают реакцию со стороны системы мониторинга. В качестве реакции может быть отправлен сигнал тревоги системному администратору или автоматически активируется система защиты от сбоев, которая временно (до тех пор, пока проблема не будет решена) выведет проблемный сервер из эксплуатации, и т. д.

Система мониторинга позволяет:

– просканировать сеть;

– найти маршрутизаторы, коммутаторы, рабочие станции, серверы, принтеры и другие сетевые устройства;

– обнаружить запущенные сетевые приложения и сервисы.

Управление сетью. Основные цели управления локальной вычислительной сетью:

– уменьшить число сетевых неполадок за счет правильной организации процесса функционирования сети;

– изолировать возникающие неполадки в работе сети и уменьшить сопутствующие им потери.

Современные локальные вычислительные сети являются динамическими распределенными структурами, объединяющими разнообразные компьютеры, межсетевые шлюзы, мосты, коммутаторы и другое сетевое оборудование, нередко являющееся продукцией различных производителей. Администраторам сети и сетевым интеграторам неизбежно приходится сталкиваться с проблемой объединения несовместимых нестандартных сетей в сеть масштаба организации. Управление такими сетями, решение вопросов контроля и отслеживания трафика – непростая задача. Поддержание работоспособности локальной сети, включающей сотни и даже тысячи рабочих станций, требует большого опыта и глубоких знаний. Наиболее трудными являются вопросы диагностики сети и идентификации неполадок.

Система управления локальной вычислительной сетью:

• управление конфигурацией. В рамках этой категории производится установление и управление параметрами, определяющими состояние локальной сети;

• обработка сбоев. Здесь осуществляются обнаружение, изоляция и исправление неполадок в сети;

• управление учетом. Основные функции – запись и выдача информации об использовании ресурсов локальной вычислительной сети;

• управление производительностью. Здесь производятся анализ и управление скоростью, с которой сеть обрабатывает данные;

• управление защитой. Основные функции – контроль доступа к ресурсам сети и защита информации, циркулирующей в сети.

Средства управления локальной вычислительной сетью предназначены для реализации функций в рамках пяти категорий управления, определенных Международной организацией по стандартизации. Данные средства входят в состав системы управления ЛВС и включают четыре типа продуктов: контрольно-измерительные приборы, сетевые мониторы, сетевые анализаторы и интегрированные системы управления сетями.

Из контрольно-измерительных приборов наиболее распространенными являются рефлектометры, осциллографы, детекторы разрывов, измерители мощности.

6.2. РЕШЕНИЕ СЕТЕВЫХ ПРОБЛЕМ. СПЕЦИАЛЬНЫЕ СРЕДСТВА

Методика решения сетевых проблем предусматривает структурный подход к их устранению. Первый этап – установка приоритетов и сбор информации. Существует множество источников информации по поддержке сетей, которыми пользуются администраторы при решении проблем.

Затем администратор составляет список возможных причин и проверяет каждую из них. После того как причина проблемы найдена, вырабатывается способ ее решения.

Если опрос пользователей не помог выяснить причину проблемы, администратор должен внимательно осмотреть сеть (кабель и оборудование), сегмент за сегментом, так как чаще всего сетевые проблемы связаны с кабелем. Найти неисправность кабеля помогут рефлектометры и *анализаторы протоколов* (сетевые анализаторы). Анализаторы протоколов могут исследовать трафик в реальном времени и предоставить статистику, на основе которой администратор составит впечатление о работе различных сетевых компонентов.

Решение проблем можно упростить, если воспользоваться различными специальными средствами.

Вольтметр (или тестер) – универсальный электроизмерительный прибор (рис. 6.1), с помощью которого можно определить напряжение на резисторе, а также при проверке сетевого кабеля установить, что произошло – разрыв или короткое замыкание.

Рис. 6.1. Вольтметр

Рефлектометр (рис. 6.2) – это устройство для обнаружения обрывов, коротких замыканий и некачественных участков кабеля, которые могут влиять на производительность сети. Устройство посылает по кабелю блокирующие импульсы; если на пути импульса встречается некачественный участок, рефлектометр анализирует отраженный сигнал и выдает результат. Прибор может находить место разрыва с точностью до нескольких десятков сантиметров. Рефлектометры часто используются при установке сети, но также незаменимы и при решении проблем в уже установленных сетях.

Рис. 6.2. Рефлектометр

Расширенные тестеры кабеля работают над физическим уровнем. Они способны отображать информацию о состоянии физического кабеля, а также:

– о количестве кадров;
– об избытке коллизий;
– о последних коллизиях;
– о количестве ошибочных кадров;
– о перегрузках;
– об испускании маяка.

Данные тестеры могут отслеживать весь сетевой трафик, отдельные виды ошибок или трафик конкретного компьютера, информировать о том, какой именно сегмент кабеля или плата сетевого адаптера является причиной проблемы.

Осциллограф – электронный прибор, отображающий на экране форму электрического сигнала (рис. 6.3). Совместно с рефлектометром он позволяет:

– найти короткое замыкание, излом, скручивание или разрыв кабеля;

– увидеть форму передаваемого по кабелю сигнала, на основании которой можно судить о затухании (потере мощности) сигнала.

Рис. 6.3. Осциллограф

Монитор сети – это программно-аппаратное устройство, которое отслеживает весь сетевой трафик или какую-то указанную его часть (рис. 6.4). Он проверяет пакеты и собирает информацию об их типах, ошибках, а также о количестве пакетов, принимаемых и передаваемых каждым компьютером.

Рис. 6.4. Монитор сети

Анализатор протоколов, называемый также сетевым анализатором (рис. 6.5), выполняет анализ сетевого трафика в реальном времени и, кроме того, захват, преобразование, передачу пакетов.

Рис. 6.5. Анализатор протоколов

Многие опытные сетевые администраторы и инженеры поддержки, ответственные за большие сети, во многом полагаются на анализаторы протоколов, используя этот инструмент для интерактивного мониторинга сети. Определяя причину проблемы, анализаторы протоколов исследуют содержимое пакета, собирают статистику о сетевом графике и составляют общую картину состояния кабельной системы, программного обеспечения, файл-серверов, рабочих станций и интерфейсных плат.

В большинство анализаторов протоколов встроены рефлектометры. Анализатор поможет «изнутри» взглянуть на поведение сети и обнаружить:

неисправные компоненты сети;

ошибки настройки или соединения;

узкие места;

колебания трафика;

проблемы, связанные с протоколами;

приложения, которые могут конфликтовать друг с другом;

необычный трафик сервера.

6.3. СТЕК ПРОТОКОЛОВ ДЛЯ INTERNET TCP/IP

Так как большинство операционных систем поддерживают протоколы TCP/IP, они могут использовать этот стек протоколов как средство взаимодействия.

Стек TCP/IP содержит базовые протоколы, прикладные программные интерфейсы, сервисы прикладного уровня, диагностические средства TCP/IP.

Основными функциями протокола IP являются:

1) маршрутизация пакетов;

2) сборка и разборка пакетов (необходима в том случае, когда пакеты формируются в одной сети и переда-

ются через другую сеть, максимальная длина пакета в которой меньше).

Стек TCP/IP был разработан для связи экспериментальной сети ARPAnet с другими сетями как набор общих протоколов для разнородной вычислительной среды. Сегодня этот стек используется для связи компьютеров всемирной информационной сети Internet, а также в огромном количестве корпоративных сетей.

Стек TCP/IP на нижнем уровне поддерживает все популярные стандарты физического и канального уровней: для локальных сетей это Ethernet, Token Ring, FDDI, для глобальных – протоколы работы на аналоговых коммутируемых и выделенных линиях SLIP, PPP, протоколы территориальных сетей X.25 и ISDN.

Основными протоколами стека, давшими ему название, являются протоколы IP и TCP. Эти протоколы в терминологии модели OSI относятся к сетевому и транспортному уровням соответственно: IP обеспечивает продвижение пакета по составной сети, а TCP гарантирует надежность его доставки.

За долгие годы использования в сетях стек TCP/IP вобрал в себя большое количество протоколов прикладного уровня. К ним относятся:

– протокол пересылки файлов FTP;

– протокол эмуляции терминала telnet;

– почтовый протокол SMTP, используемый в электронной почте сети Internet, гипертекстовые сервисы службы WWW и многие другие.

Стремительный рост популярности Internet привел и к изменениям в расстановке сил в мире коммуникационных протоколов – протоколы TCP/IP, на которых построен Internet, стали быстро вытеснять стек IPX/SPX компании Novell. На данный момент стек TCP/IP – это самый распространенный стек транспортных протоколов локальных, корпоративных и территориальных сетей.

Поскольку стек TCP/IP изначально создавался для глобальной сети Internet, он имеет много особенностей, которые обеспечивают ему преимущество перед другими протоколами. Полезное свойство протокола – это его способность фрагментировать пакеты. Действительно, сложная составная сеть часто состоит из сетей, построенных на совершенно разных принципах. В каждой из этих сетей может быть установлена собственная величина максимальной длины единицы передаваемых данных (кадра). В таком случае при переходе из одной сети, имеющей большую максимальную длину, в другую, с меньшей максимальной длиной, может возникнуть необходимость разделения передаваемого кадра на несколько частей. Протокол IP стека TCP/IP эффективно решает эту задачу.

Другая особенность технологии TCP/IP – это гибкая система адресации, позволяющая более просто по сравнению с другими протоколами аналогичного назначения включать в интерсеть (объединенную или составную сеть) сети других технологий. Это свойство также способствует применению стека TCP/IP для построения больших гетерогенных сетей.

В стеке TCP/IP экономно используются возможности широковещательных рассылок. Это свойство просто необходимо при работе на медленных каналах связи, характерных для территориальных сетей.

Для реализации мощных функциональных возможностей протоколов стека TCP/IP требуются большие вычислительные затраты. Гибкая система адресации и отказ от широковещательных рассылок приводят к наличию в IP-сети различных централизованных служб типа DNS, DHCP и т. п. Каждая из этих служб упрощает администрирование сети и конфигурирование оборудования, но требует внимания со стороны администраторов.

Преимущества стека протоколов TCP/IP:

• надежная связь между сетевым оборудованием от различных производителей;

• независимость от сетевой технологии – стек только определяет элемент передачи, дейтаграмму, и описывает способ ее движения по сети;

• всеобщая связанность – стек позволяет любой паре компьютеров, которые его поддерживают, взаимодействовать друг с другом. Каждому компьютеру назначается логический адрес, а каждая передаваемая дейтаграмма содержит логические адреса отправителя и получателя. Промежуточные маршрутизаторы используют адрес получателя для принятия решения о маршрутизации;

• подтверждения – протоколы стека обеспечивают подтверждения правильности прохождения информации при обмене между отправителем и получателем;

• стандартные прикладные протоколы – протоколы стека TCP/IP включают в свой состав средства поддержки основных приложений, таких как электронная почта, передача файлов, удаленный доступ и т. д.

? *Контрольные вопросы и задания*

1. Дайте определение понятию «корпоративная сеть».

2. Перечислите базовый набор сетевых служб корпоративной сети.

3. Назовите основные задачи сетевого администратора.

4. Охарактеризуйте систему мониторинга.

5. Опишите систему управления локальной вычислительной сетью.

6. Перечислите специальные средства для поиска и решения сетевых проблем и поясните, для каких целей используется каждый прибор.

7. Сформулируйте возможности анализатора протоколов.

8. Перечислите основные стандарты, которые поддерживает стек TCP/IP.

9. Прокомментируйте особенности технологии TCP/IP.

10. Объясните, в чем заключаются преимущества стека протоколов TCP/IP.

11. Определите основные параметры, необходимые для протокола TCP/IP.

12. Охарактеризуйте особенности реализации стека TCP/IP.

РАЗДЕЛ 7
ПОДДЕРЖКА СЕТИ

7.1. ПРОГРАММЫ ДЛЯ РАБОТЫ С СЕТЬЮ. ДИНАМИЧЕСКИЕ СИСТЕМЫ ИМЕНОВАНИЯ

Поддержка сети является многоаспектным процессом, включающим мониторинг поведения сети как способ заблаговременного устранения проблем. При планировании сети администратор должен реализовать концепции и процедуры для предупреждения проблем до их возникновения – резервное копирование, унификацию, постоянное совершенствование и ведение документации. Важная часть управления сетью – эталонный график ее поведения, который при сбое сети дает администратору возможность сравнить текущие графики загруженности, найти потенциальные узкие места, проанализировать число ошибок и общую статистику производительности.

Разработано большое количество программ для работы с сетью, ее мониторинга, организации и управления, которые ведут статистику производительности и доступа к ресурсам, а также журналы событий. Рассмотрим некоторые такие программы.

Network Diagnostic Tools – предоставляет большой набор сетевых инструментов (ping, traceroute, dns lookup, finger, echo, whois, port scanner, time и др.), который организован для удобного использования в процессе администрирования сетей.

Lanspider – удобная программа для поиска файлов на компьютерах локальной сети (позволяет искать файл по многочисленным критериям, в том числе по строке текста).

Emco Remote Shutdown – программа для выключения и перезагрузки удаленных машин, на которых установлена система windows/nt/2000/xp. Перед выключением программа принудительно закрывает все работающие приложения.

Pixcript – для удобного конфигурирования. При помощи этой программы можно создать сценарии конфигурирования, которые выполнят всю работу за администратора.

Netobserve – программа анализа сетевой работы компьютеров локальной сети. Позволяет отслеживать процесс обмена чат-сообщениями, статистику www сайтов, обнаруживать программы, работающие на удаленных компьютерах, анализировать работу удаленных принтеров, а также работу удаленных web-камер. Все лог-файлы шифруются, и к ним предоставляется доступ через web-браузер.

Max Infrastructure Management Suite – приложение, которое предоставляет своим пользователям все функции, необходимые для обслуживания локальных сетей (позволяет определять работоспособность аппаратного обеспечения сетей, программного обеспечения, работоспособность баз данных, серверов).

Lan Netbrowse – позволяет собирать информацию об адресах mac, ip, ipx, именах компьютеров, о расширенных ресурсах и т. д.

Remote Shutdown – программа для удаленного выключения / перезагрузки компьютеров в локальной сети. Позволяет создавать уведомление о выключении / перезагрузке компьютера пользователя и устанавливать вре-

мя, за которое будет показано это сообщения. Также дает пользователям возможность отменить операцию.

My Sanity – позволяет управлять в очень удобной форме многочисленными аккаунтами пользователей (системный администратор может назначать каждому пользователю или группе пользователей права доступа и определять уровень их безопасности), а также работой сетевых устройств, принтеров и другого оборудования.

2Morrow Visual Server Monitor – программа для контроля в реальном времени над работоспособностью серверов на удаленных машинах (результаты выводятся в графическом виде).

Total Network Inventory – программа для инвентаризации сети и учета компьютеров (предназначена для офисов, малых и больших корпоративных сетей). Опрашивает все компьютеры в сети и предоставляет полную информацию об операционной системе, ее обновлениях, аппаратном обеспечении, установленном программном обеспечении, о запущенных процессах и т. д. Эта информация заносится в централизованную базу данных.

Total Network Monitor – программа для постоянного наблюдения за работой локальной сети отдельных компьютеров, сетевых и системных служб (администратор может в любой момент проверить работу той или иной службы, сервера или файловой системы).

Active Directory (активные директории) – позволяет администратору использовать групповые политики (наборы правил, по которым производится настройка рабочей среды) для обеспечения единообразия настройки пользовательской рабочей среды, разворачивать программное обеспечение на множестве компьютеров через групповые политики сети. Active Directory – избыточная поддержка нескольких стандартных систем именований. В качестве собственной системы имен в AD применяется DNS;

в то же время она может использовать LDAP или HTTP для обмена информацией с приложениями или иными каталогами.

В Active Directory объединены лучшие возможности X.500 и сервиса обнаружения DNS (DNS – сервис, наиболее часто используемый для преобразования имени в IP-адрес как в Internet, так и в интрасетях). Active Directory использует DNS в качестве своего поискового сервиса. Имя домена в AD – не что иное, как полностью определенное имя DNS.

Традиционно DNS был присущ один недостаток – статичность базы, что вело к необходимости обновлять данные и тиражировать изменения на другие серверы DNS вручную. В Windows NT 4.0 было реализовано решение, объединяющее сервис DNS с сервисом WINS и позволявшее динамически обновлять базу имен. Кроме того, в состав операционной системы был включен графический инструмент для администрирования DNS, что позволяло пользователям легко освоить эту «науку».

DNS + WINS работала следующим образом: при поступлении от DNS-клиента запроса на разрешение имени (например, mydesktop.mycorp.ru) разрешение имени хоста выполнялось на сервере WINS, к которому обращался сервер DNS и которому возвращался разрешенный IP-адрес. Такая конфигурация делала возможным использование DHCP для динамического назначения адресов. Хотя интеграция DNS с WINS и была временным решением, она частично облегчила работу администраторам до принятия стандарта на динамический DNS3.

В динамическом сервере DNS обновлением и тиражированием базы занимается непосредственно сервер. Серверы, на которых установлена служба каталогов Active Directory, используют динамический DNS для публикации самих себя в базе DNS.

Форма именований, принятая в каталоге, влияет как на пользователей, так и на приложения. В различных стандартах используются различные форматы имен. Многие из них поддерживаются в Active Directory, что позволяет пользователям, например, обращаться к объектам привычным образом. Перечислим некоторые из поддерживаемых систем именований.

RFC822. Этот стандарт именований хорошо знаком пользователям Internet (по форме имя@домен при отправке или получении сообщений по электронной почте).

HTTP URL. Как упоминалось ранее, к службе каталогов Active Directory можно обратиться по протоколу HTTP. Для этого необходимо указать имя URL, формат которого также хорошо знаком пользователям Internet: http://имя-домена/путь-к-странице. При этом имя домена – это имя сервера, на котором установлена служба каталога, а путь к странице – путь в иерархичной структуре каталога к интересующему объекту.

LDAP URL и имена X.500. В Active Directory поддерживается доступ и по протоколу LDAP. То, что имена LDAP сложнее по сравнению с именами Internet, не так важно – ведь обычно LDAP используется приложениями. В рамках LDAP действуют соглашения об именовании X.500, называемые *атрибутированным именованием*. Имя при этом состоит из URL сервера, на котором располагается каталог, и далее – атрибутированного имени объекта;

Имена UNC. В Active Directory поддерживается также и соглашение об универсальном именовании, которое традиционно используется в сетях Windows NT для ссылок на совместно используемые ресурсы: тома, принтеры и файлы.

В каталоге LDAP пространство имен может быть либо смежным, либо раздельным. В первом случае имя дочернего домена всегда содержит имя родительского домена.

Например, если домен с именем DC=Finance, DC=MyCorp, DC=Ru – дочерний для домена DC=MyCorp, DC=Ru, то это пространство смежных имен. Имя родительского домена всегда может быть восстановлено при отбрасывании первой части дочернего имени. В пространстве раздельных имен родительский и дочерний домены не связаны друг с другом непосредственно. Например, домен DC=Finance, DC=Ru – дочерний для домена DC=MyCorp, DC=Ru, его имя не содержит имени родительского домена. Смежные имена или раздельные – важно при поиске. В случае применения смежных имен на контроллере домена всегда создаются ссылки на дочерние домены. При использовании раздельных имен поиск останавливается и ссылки не создаются. Одновременное использование смежных и раздельных имен делает механизм поиска в древовидной структуре сложным для понимания. Поэтому в Active Directory вводятся понятия *дерево* и *лес*.

Дерево характеризуется:

– иерархией доменов;

– пространством смежных имен;

– доверительными отношениями Kerberos между доменами;

– использованием общей схемы;

– принадлежностью к общему глобальному каталогу.

Лес характеризуется:

– одним или несколькими наборами деревьев;

– раздельными пространствами имен между этими деревьями;

– доверительными отношениями Kerberos между доменами;

– использованием общей схемы;

– принадлежностью к общему глобальному каталогу.

Active Directory использует тиражирование типа мульти-мастер. Как уже упоминалось, в этой службе ка-

талогов более не существует различий между контроллерами доменов – они все равноправны. Изменения, внесенные в каталог на одном контроллере, тиражируются на остальные. Но такой подход проще существовавшей в предыдущих версиях модели с одним главным и несколькими резервными контроллерами домена, он требует принятия специальных мер по синхронизации тиражируемой информации. Тиражирование Active Directory основано не на временных интервалах, а на последовательных номерах обновлений USN. В каждом контроллере домена имеется таблица, где записаны как свой собственный номер USN, так и USN партнеров по тиражированию. При тиражировании происходит сравнение последнего известного USN партнера с тем, который сообщается. И если сообщенный номер больше записанного, запрашиваются все изменения у партнера по тиражированию (такой тип тиражирования носит название *запрашиваемый*). После обновления данных USN на контроллере домена становится равным значению, полученному от партнера. Если данные одного и того же объекта изменились сразу на нескольких контроллерах домена, то обновление выполняется следующим образом.

У каждого свойства свой номер версии. С помощью этого номера определяется «наиболее актуальное», т. е. имеющее наибольший номер версии свойство. Это не всегда верное решение, однако оно позволяет согласовывать версии без дополнительных переговоров с партнером по тиражированию и гарантирует идентичность данных на всех контроллерах доменов. Если свойства имеют одинаковый номер версии, то проверяется временная отметка, создаваемая вместе с номером версии при модификации свойств. При этом предполагается, что все контроллеры домена синхронизованы по времени. Предпочтение отдается версии, созданной позднее. Если и номер версии,

и временные отметки совпадают, то выполняется сравнение в двоичном виде, причем предпочтение получает то свойство, которое в двоичном виде занимает больший объем. Если размеры одинаковы, то считается, что обе версии идентичны и в расчет не принимается ни одна из них

Узел с Active Directory состоит из одной или нескольких подсетей IP. Администратор может определять эти подсети, а также добавлять к ним новые. При этом он исходит из следующих посылок:

• оптимизация графика тиражирования между узлами по медленным линиям;

• создание клиентам наилучших условий для быстрого обнаружения ближайших к ним контроллеров.

Тиражирование внутри узла и между узлами осуществляется по различным топологиям. Внутри узла контроллер домена задерживает оповещение о сделанных изменениях на некоторый устанавливаемый промежуток времени (по умолчанию равный 10 минутам).

Концепция поиска ближайшего ресурса или контроллера домена позволяет сократить трафик в низкоскоростных частях глобальных сетей. Для поиска ближайших ресурсов или контроллеров домена клиенты могут использовать информацию об узле. Начиная вход в сеть, клиент получает от контроллера домена имя узла, к которому принадлежит, имя узла, к которому относится контроллер домена, а также информацию о том, является ли данный контроллер домена ближайшим к клиенту. Если это не ближайший контроллер, то клиент может обратиться к контроллеру домена в собственном узле и в дальнейшем работать с ним как с ближайшим контроллером. Так как данная информация сохраняется в реестре, клиент может ее использовать при следующем входе в сеть. Если пользователь перемещается со своей рабочей станцией в новое место, то при входе в сеть

станция обращается к прежнему контроллеру домена (в этом случае он уже не является ближайшим) и сообщает клиенту информацию о ближайшем узле. Эта информация может быть использована клиентом для доступа к DNS и определения адреса ближайшего контроллера домена.

7.2. ГЛОБАЛЬНЫЕ СЛУЖБЫ КАТАЛОГОВ. ПРИНЦИП ОРГАНИЗАЦИИ DNS. СЛУЖБА ПЕРЕДАЧИ ФАЙЛОВ FTP

Глобальный каталог представляет собой репозиторий распределенных данных, который хранит информацию о каждом объекте, а также облегчает поиск в лесу Active Directory. Глобальный каталог хранится на контроллерах домена, назначенных в качестве серверов глобального каталога, и распространяется посредством репликации с множеством равноправных участников. Глобальный каталог позволяет пользователям и приложениям находить объекты в любом домене текущего леса посредством поиска атрибутов, включенных в глобальный каталог, которые идентифицируются в схеме в качестве частного набора атрибутов Таким образом, при отсутствии сервера глобального каталога контроллер домена, принимающий поисковые запросы объектов в других доменах, пересылает поисковые запросы на контроллер в домене с искомым объектом. Глобальный каталог автоматически конфигурируется на первом контроллере домена, который устанавливается в лесу.

Как и доменные службы Active Directory, серверы глобального каталога не могут функционировать без DNS. Службы DNS предоставляют данные, необходимые компьютерам в сети для локализации контроллеров домена Active Directory и для предоставления IP-адресов серверов глобального каталога клиентам сервера глобального каталога.

DNS – это схема именования. Внешне она похожа на структуру каталогов на диске, т. е. имеет структуру дерева, называемого *пространством доменных имен*, в котором каждый домен (узел дерева) определяет группу компьютеров, образующих часть сети и управляемых как единое целое в соответствии с общими правилами и процедурами.

Пространство доменных имен состоит:

из *корневого домена* – представляет корень пространства имен и обозначается концевой точкой (обычно эта точка опускается и заменяется пустым символом (null));

доменов верхнего уровня – расположены непосредственно под корнем и указывают тип организации, а также назначаются для каждой страны. Имена этих доменов должны следовать международному стандарту ISO 3166, за что отвечает InterNIC. Для обозначения стран используются трехбуквенные и двухбуквенные аббревиатуры, а для различных типов организаций, классифицированных по выполняемым функциям, – следующие аббревиатуры:

com – коммерческая организация;

edu – образовательное учреждение;

gov – правительственное учреждение;

mil – военная организация;

net – центр поддержки сетей;

org – некоммерческие организации;

int – международная организация;

доменов второго уровня – располагаются за доменами верхнего уровня и идентифицируют конкретные организации. За поддержку имен доменов второго уровня и соблюдение их уникальности в Internet отвечает InterNIC;

поддоменов – принадлежат конкретной организации и располагаются за доменами второго уровня. За создание и поддержку своих поддоменов отвечают сами организации.

Каждый домен имеет уникальное имя, а каждый из поддоменов – уникальное имя внутри своего домена. Имя домена идентифицирует его положение в пространстве доменных имен по отношению к родительскому домену, причем точки в имени отделяют части, соответствующие узлам домена и называемые *суффиксами домена*. Однако, если полное имя файла формируется из пути к этому файлу от корневого каталога с добавлением в конце собственно имени файла, то хост-имя формируется из цепочки доменов в обратном порядке, т. е. от хоста к корню. Получаемое таким образом уникальное хост-имя, отражающее положение хоста в иерархии, составляется из имен поддоменов, в которые он входит, и называется *полным доменным именем*. Имя домена, не чувствительное к регистру букв, может содержать до 63 символов, а полное доменное имя может достигать глубины 127 уровней, пока общая длина вместе с точками не достигнет 254 символов. Но на практике регистраторы доменных имен используют более строгие ограничения.

Организации, не соединенные с Internet, могут использовать произвольные имена доменов верхнего и второго уровня. Но обычно даже такие организации придерживаются спецификации InterNIC, чтобы впоследствии – при подключении к Internet – не пришлось переименовывать домены.

Хост-имена могут иметь различные формы. Самые распространенные из них – это уже упомянутое доменное имя и *понятное имя*. Понятное имя является псевдонимом IP-адреса, произвольно назначенного отдельным пользователем. Оно, как и доменное имя, может быть длиной до 255 знаков и включать алфавитно-цифровые символы, а также дефисы и точки. Каждый вправе создать любые нужные записи, присвоив часто используемым ресурсам понятные имена, которые нетрудно запо-

минать. Однако понятные имена неэффективны при наличии большого количества записей.

К адресам хост-компьютеров в сети предъявляются специальные требования. Адрес должен иметь формат, с одной стороны, позволяющий просто выполнять его синтаксическую автоматическую обработку; с другой стороны, он должен иметь семантическую окраску, т. е. нести информацию об адресуемом объекте. Поэтому адреса хост-компьютеров в сети Internet могут иметь двойную кодировку:

– обязательную кодировку, удобную для работы системы телекоммуникации в сети: дружественный компьютеру цифровой IP-адрес (IP, Internet Protocol);

– необязательную кодировку, удобную для абонента сети: дружественный пользователю DNS-адрес (DNS, Domain Name System).

IP-адрес (Internet Protocol Address) – уникальный идентификатор (адрес) устройства (компьютера), подключенного к локальной сети или Internet. Это основной тип адресов, на основании которых сетевой уровень протокола IP передает пакеты между сетями. IP-адрес назначается администратором во время конфигурирования компьютеров и маршрутизаторов и состоит из двух частей: номера сети и номера узла. В случае изолированной сети ее адрес может быть выбран администратором из специально зарезервированных для таких сетей блоков адресов (192.168.0.0/16, 172.16.0.0/12 или 10.0.0.0/8). Если же сеть должна работать как составная часть Internet, то адрес сети выдается провайдером либо региональным Internet-регистратором. Региональные регистраторы получают номера автономных систем, после чего выдают номера автономных систем и блоки адресов меньшего размера локальным Internet-регистраторам, являющимся крупными провайдерами.

Цифровой IP-адрес версии v.4 представляет собой 32-разрядное двоичное число. Для удобства он разделяется на четыре блока по 8 битов, которые можно записать в десятичном виде. Адрес содержит полную информацию, необходимую для идентификации компьютера.

Удобной формой записи IP-адреса является запись в виде четырех десятичных чисел (от 0 до 255), разделенных точками, например 192.168.0.1. (или 128.10.2.30 – десятичная форма представления адреса,

а 10000000 00001010 00000010 00011110 – двоичная форма представления этого же адреса).

Номер узла в протоколе IP назначается независимо от локального адреса узла. Маршрутизатор по определению входит сразу в несколько сетей. Поэтому каждый порт маршрутизатора имеет собственный IP-адрес. Конечный узел также может входить в несколько IP-сетей. В этом случае компьютер должен иметь несколько IP-адресов, по числу сетевых связей. Таким образом, IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение.

Какая часть адреса относится к номеру сети, а какая – к номеру узла, определяется значениями первых битов адреса.

Классовая маршрутизация повсеместно вытеснена бесклассовой маршрутизацией, при которой количество адресов в сети определяется только и исключительно маской подсети.

В протоколе IP существует несколько соглашений об особой интерпретации IP-адресов:

• если весь IP-адрес состоит только из двоичных нулей, то он обозначает адрес того узла, который сгенерировал этот пакет;

• если в поле номера сети стоят только нули, то по умолчанию считается, что узел назначения принадлежит той же самой сети, что и узел, который отправил пакет;

• если все двоичные разряды IP-адреса равны единице, то пакет с таким адресом назначения должен рассылаться всем узлам, находящимся в той же сети, что и источник этого пакета;

• если в поле номера узла назначения стоят только единицы, то пакет, имеющий такой адрес, рассылается всем узлам сети с заданным номером сети.

IP-адрес называют динамическим, если он назначается автоматически при подключении устройства к сети и используется в течение ограниченного промежутка времени, как правило, до завершения сеанса подключения.

Ввиду огромного количества подключенных к сети компьютеров и различных организаций ощущается ограниченность 32-разрядных IP-адресов, поэтому ведется разработка модернизированного протокола IP-адресации, имеющего целью:

– повышение пропускной способности сети;

– создание лучше масштабируемой и адаптируемой схемы адресации;

– обеспечение гарантий качества транспортных услуг;

– обеспечение защиты информации, передаваемой в сети.

Основой этого протокола являются 128-битовые адреса, обеспечивающие более 1000 адресов на каждого жителя Земли. Внедрение этой адресации (IP-адресация υ.6) снимет проблему дефицита цифровых адресов.

Однако главной целью разработки нового протокола является не столько расширение разрядности адреса, сколько увеличение уровней иерархии в адресе, отражающей теперь пять идентификаторов: два старших – для провайдеров сети (идентификаторы провайдера и его реестра) и три – для абонентов (абонента, его сети и узла сети).

Доменный адрес состоит из нескольких отделяемых друг от друга точкой буквенно-цифровых доменов (*domain* –

область). Этот адрес построен на основе иерархической классификации: каждый домен, кроме крайнего левого, определяет целую группу компьютеров, выделенных по какому-либо признаку; при этом домен группы, находящийся слева, является подгруппой правого домена. Примером могут служить географические двухбуквенные домены некоторых стран:

by – Республика Беларусь;
ca – Канада;
ch – Швейцария;
cz – Чехия;
de – Германия;
es – Испания;
fr – Франция;
jp – Япония;
lt – Литва;
pl – Польша;
ru – Россия;
ua – Украина.

Доменный адрес может иметь произвольную длину. В отличие от цифрового адреса он читается в обратном порядке: вначале указывается домен нижнего уровня – имя хост-компьютера, затем домены – имена подсетей и сетей, в которой он находится, и наконец домен верхнего уровня – чаще всего идентификатор географического региона (страны).

Итак, доменный адрес хост-компьютера включает несколько уровней доменов. Каждый уровень отделяется точкой. Слева от домена верхнего уровня располагаются другие имена. Все, находящиеся слева, – поддомен для общего домена.

Для пользователей сети Internet почтовыми адресами могут быть просто их имена, зарегистрированные в службе электронной почты и не отражающие такой длинной иерархии.

Преобразование (разрешение) доменного адреса в соответствующий цифровой IP-адрес выполняют специальные серверы DNS – серверы имен. Поэтому пользователю нет необходимости знать цифровые адреса.

Для работы в сети Internet достаточно знать только доменный адрес компьютера или пользователя, с которым требуется установить связь.

Более эффективно использовать для адресации не просто доменный адрес, а *унифицированный указатель ресурса* – URL, который дополнительно к доменному адресу содержит указания на используемую технологию доступа к ресурсам и спецификацию ресурса внутри файловой структуры компьютера.

Протокол FTP – сетевой протокол, предназначенный для передачи файлов в компьютерных сетях. По своему функциональному назначению он совпадает с файловым сервером. Отличие состоит в способе доступа пользователя к информационной базе сервера. В этом случае пользователь «входит» в машину, на которой расположен сервер, выясняет, какие файлы имеются, и осуществляет передачу нужного ему файла на свою машину в рамках текущего сеанса связи.

Протокол FTP позволяет подключаться к серверам FTP (это доступ к сотням файловых библиотек, начиная от программного обеспечения и заканчивая документами), просматривать содержимое каталогов и загружать файлы с сервера или на сервер. Кроме того, возможен режим передачи файлов между серверами.

FTP является одним из старейших прикладных протоколов и широко используется для распространения программного обеспечения и доступа к удаленным хостам. FTP предназначен для решения задач разделения доступа к файлам на удаленных хостах, прямого или косвенного использования ресурсов удаленных компьютеров, обеспечения независимости клиента от файловых

систем удаленных хостов, эффективной и надежной передачи данных. Обмен данными в FTP происходит по TCP-каналу. Обмен построен на технологии «клиент-сервер». FTP не может использоваться для передачи конфиденциальных данных, поскольку не обеспечивает защиты передаваемой информации и передает между сервером и клиентом открытый текст. FTP-сервер может потребовать от FTP-клиента аутентификации, при которой логин и пароль также передаются открытым текстом. На многих FTP-серверах существует каталог, открытый на запись и предназначенный для закачки файлов на сервер. Это позволяет пользователям наполнять сервер данными.

Технология FTP была разработана в рамках проекта ARPA и предназначена для обмена большими объемами информации между машинами с различной архитектурой. Главным в проекте было обеспечение надежной передачи, поэтому с современной точки зрения FTP кажется перегруженным излишними редко используемыми возможностями. Стержень технологии составляет FTP-протокол.

Алгоритм работы протокола FTP:

• сервер FTP использует в качестве управляющего соединения на TCP порт 21, который всегда находится в состоянии ожидания соединения со стороны пользователя FTP;

• после того как устанавливается управляющее соединение модуля «Интерпретатор протокола пользователя» с модулем сервера «Интерпретатор протокола сервера», пользователь (клиент) может отправлять на сервер команды. FTP-команды определяют параметры соединения передачи данных: роль участников соединения (активный или пассивный), порт соединения, тип передачи, тип передаваемых данных, структуру данных и управля-

ющие директивы, обозначающие действия, которые пользователь хочет совершить (например, сохранить, считать, добавить или удалить данные или файл и другие);

• после того как согласованы все параметры канала передачи данных, один из участников соединения (пассивный) становится в режим ожидания открытия соединения на заданный для передачи данных порт. Затем активный модуль открывает соединение и начинает передачу данных;

• после окончания передачи данных соединение между «Программой передачи данных сервера» и «Программой передачи данных пользователя» закрывается, но управляющее соединение «Интерпретатора протокола сервера» и «Интерпретатора протокола пользователя» остается открытым. Пользователь, не закрывая сессии FTP, может еще раз открыть канал передачи данных.

Как правило, сервер FTP ответственен за открытие и закрытие канала передачи данных. Сервер FTP должен самостоятельно закрыть канал передачи данных в следующих случаях:

– сервер закончил передачу данных в формате, который требует закрытия соединения;

– сервер получил от пользователя команду прервать соединение;

– пользователь изменил параметры порта передачи данных;

– было закрыто управляющее соединение;

– возникли ошибки, при которых невозможно возобновить передачу данных.

Основные недостатки FTP-серверов:

1) FTP-серверы представляют собой потенциальную «дыру» в системе безопасности сети, поэтому, если не планируется организация архивов, библиотек, т. е. хранилищ данных, доступных для широкого доступа, лучше не запускать FTP-сервер вообще;

2) FTP-серверы уязвимы в той или иной степени, но различия в реализации и конфигурации приводят в одних случаях к отказу от обслуживания, а в других – к полному контролю над хостом, причем из-за особенностей протокола FTP могут быть поражены как серверы, так и клиенты.

Одной из проблем FTP-серверов является отсутствие проверки подлинности источника пакетов: при установке соединения сервер прослушивает один из TCP портов, сообщает его номер клиенту, после чего клиент открывает указанный порт и начинает передачу данных – это пассивный режим. При активном режиме TCP порт назначает клиент, а сервер открывает соединение с порта 20 на порт, назначенный клиентом. Поскольку в процессе сеанса подлинность абонента не проверяется, то возможна атака следующего вида: на открытый порт периодически посылаются запросы на TCP соединение. Как только соединение установлено, происходит подмена клиента. Уязвимость к данной атаке демонстрируют все ftpd-серверы.

Основные недостатки FTP с точки зрения клиента – возможность перехвата данных, недостаточная стандартизованность и плохая совместимость с брандмауэрами.

? *Контрольные вопросы и задания*

1. Приведите примеры программ для администрирования сети.
2. Охарактеризуйте основные программы администрирования.
3. Опишите назначение Active Directory.
4. Назовите характеристики дерева и леса.
5. Охарактеризуйте основное тиражирование Active Directory.
6. Перечислите основные системы именования Active Directory.
7. Объясните принцип организации DNS.

8. Укажите, из чего состоит пространство доменных имен.
9. Приведите основные трехбуквенные аббревиатуры.
10. Опишите основные характеристики домена.
11. Сравните хост-имя и доменное имя.
12. Поясните, что представляет собой IP-адрес.
13. Укажите отличия FTP-сервера и файлового сервера.

СПИСОК АНГЛИЙСКИХ ТЕРМИНОВ

Термин	Расшифровка	Описание
AD	Active Directory	Избыточная поддержка нескольких стандартных систем именований
ADSL	Asymmetric Digital Subscriber Line	Асимметричная цифровая абонентская линия
AMR	Adaptive Multi Rate	Адаптивное кодирование с переменной скоростью
ArcNet	Attached Resource Computer NETwork	Технология локальных вычислительных сетей, назначение которой аналогично назначению Ethernet или Token ring, являлась первой технологией для создания сетей микрокомпьютеров
ARPAnet	Advanced Research Projects Agency Network	Первая в мире сеть, перешедшая на маршрутизацию пакетов данных
ATM	Asynchronous Transfer Mode	Усовершенствованная технология коммутации пакетов, которая обеспечивает высокоскоростную передачу пакетов фиксированной длины через широкополосные и узкополосные локальные или глобальные сети
CDDI	Copper Distributed Data Interface	Распределенный интерфейс передачи данных по кабельным линиям, распределенный интерфейс передачи данных по медным кабелям
COM	Component Object Model	Объектная модель компонентов
CRC	Cyclic Redundancy Check	Алгоритм вычисления контрольной суммы, предназначенный для проверки целостности данных

Термин	Расшифровка	Описание
CSMA/CA	Carrier Sense Multiple Access With Collision Avoidance или Carrier Sensing Multiple Access With Collision Avoidance	Множественный доступ с контролем несущей и избеганием коллизий или многостанционный доступ с контролем несущей и предотвращением конфликтов
CSMA/CD	Carrier Sense Multiple Access with Collision Detection	Множественный доступ с контролем несущей и обнаружением коллизий
DHCP	Dynamic Host Configuration Protocol	Протокол динамической конфигурации узла
Digital DECnet		Набор сетевых протоколов, созданный Digital Equipment Corporation
DLL		Выполняемый модуль, содержащий программный код или ресурсы, используемые другими прикладными программами
DNS	Domain Name System	Система доменных имен
DOCSIS	Data Over Cable Service Interface Specifications	Стандарт передачи данных по коаксиальному (телевизионному) кабелю
DSL	Digital Subscriber Line	Цифровая абонентская линия
DTE	Data Terminal Equipment	Конец инструмента, который преобразует пользовательскую информацию в сигналы или преобразует полученные сигналы
Ethernet		Пакетная технология передачи данных преимущественно локальных компьютерных сетей
FDDI	Fiber Distributed Data Interface	Распределенный интерфейс передачи данных по волоконно-оптическим каналам
FM		Обозначение частотной модуляции
Freme Relay		Усовершенствованная быстрая технология коммутации пакетов переменной длины

Термин	Расшифровка	Описание
FTP	File Transfer Protocol	Протокол передачи файлов, предназначенный для передачи файлов по TCP-сетям (например, Internet)
HDSL	High-Rate Digital Subscriber Line	Высокоскоростная цифровая абонентская линия
HTTP	HyperText Transfer Protoco	Протокол передачи гипертекста — протокол прикладного уровня передачи данных
IBM	System Network Architecture	Собственная сеть архитектуры, созданной в 1974 г.
IEEE 802.X		Стандарт Института инженеров электротехники и электроники, описывающий процесс инкапсуляции данных, передаваемых между запрашивающими устройствами (клиентами), системами, проверяющими подлинность (коммутаторами, точками беспроводного доступа), и серверами проверки подлинности
IMAP	Internet Message Access Protocol	Протокол прикладного уровня для доступа к электронной почте
Internet		Всемирная система объединенных компьютерных сетей, построенная на базе протокола IP и маршрутизации IP-пакетов
ISA	Industry Standard Architecture	8- или 16-разрядная шина ввода/вывода IBM PS-совместимых компьютеров
ISDN	Integrated Services Digital Network	Цифровая сеть комплексных услуг – спецификация межсетевой цифровой связи, предназначенной для передачи речи, данных, графики
LAN	Local Area Network	Компьютерная сеть, покрывающая обычно относительно небольшую территорию или небольшую группу зданий
LDAP	Lightweight Directory Access Protocol	«Облегченный протокол доступа к каталогам» — протокол прикладного уровня для доступа к службе каталогов X.500

Термин	Расшифровка	Описание
LLC	Logical Link Control	Подуровень управления логической связью в компьютерных сетях
MAN	Metropolitan Area Network	Компьютерная сеть, которая объединяет компьютеры в пределах города, представляет собой сеть, по размерам меньшую, чем WAN, но большую, чем LAN
Novell NetWare		Сетевая операционная система и набор операционных систем, которые используются в этой системе для взаимодействия с компьютерами-клиентами, подключенными к сети
NVRAM	Non Volatile Random Access Memory	Энергонезависимая электрически перепрограммируемая память, в которой хранятся настройки модема. Пользователь может изменять установки, например используя набор AT-команд
OSI	Open Systems Interconnection Basic Reference Model	Базовая эталонная модель взаимодействия открытых систем
PCI	Peripheral Component Interconnect	Взаимосвязь периферийных компонентов – шина ввода/вывода для подключения периферийных устройств к материнской плате компьютера
PCMCIA	Personal Computer Memory Card International Association	Спецификация на модули расширения, разработанная ассоциацией PCMCIA
PLC	Programmable Logic Controller	Программируемый контроллер – электронная составляющая промышленного контроллера, специализированного (компьютеризированного) устройства, используемого для автоматизации технологических процессов
POP3	Post Office Protocol Version 3	Протокол почтового отделения, версия 3 – стандартный Internet-протокол прикладного уровня,

Термин	Расшифровка	Описание
		используемый клиентами электронной почты для извлечения электронного сообщения с удаленного сервера по TCP/IP-соединению
RAM	Random Access Memory	Оперативная память модема, используется для буферизации принимаемых и передаваемых данных, работы алгоритмов сжатия и прочего
ROM	Read-Only Memory	Энергонезависимая память, в которой хранится микропрограмма управления модемом
SDSL	Symmetric Digital Subscriber Line	Симметричная цифровая абонентская линия
SMDS	Switched Multi-megabit Data Services	Коммутируемая служба, которую предлагают некоторые локальные коммуникационные компании
SMTP	Simple Mail Transfer Protocol	Простой почтовый протокол
SNA	Systems Network Architecture	Системная сетевая архитектура, разработанная компанией IBM в 1974 г. Общее описание структуры, форматов, протоколов, используемых для передачи информации между программами IBM и оборудованием, создавалось для объединения в глобальные сети мейнфреймов IBM
SONET		Представитель современных систем, которые реализуют преимущества оптоволоконной технологии – синхронная оптическая сеть
Token Bus		Механизм организации сетей под названием «маркерная шина»
Token Ring		Механизм организации сетей под названием «маркерное кольцо»
TCP/IP	Transmission Control Protocol/ Internet Protocol	Протокол управления передачей — набор сетевых протоколов разных уровней модели сетевого взаимодействия DOD, используемых в сетях
VDSL	Very-high bit rate Digital Subscriber Line	Сверхвысокоскоростная цифровая абонентская линия

Термин	Расшифровка	Описание
WAN	Wide Area Network	Компьютерная сеть, охватывающая большие территории и включающая большое число компьютеров
Web-страницы		Документ или информационный ресурс Всемирной паутины, доступ к которому осуществляется с помощью web-браузера
WINS	Windows Internet Name Service	Служба имен Windows Internet – служба сопоставления NetBIOS-имен компьютеров с IP-адресами узлов
WWW	World Wide Web	Распределенная система, предоставляющая доступ к связанным между собой документам, расположенным на различных компьютерах, подключенных к Internet
X.25		Набор протоколов для сетей с коммутацией пакетов

ЛИТЕРАТУРА

Айвенс, К. Компьютерные сети. Хитрости / К. Айвенс. Санкт-Петербург : Питер, 2006.

Архитектура компьютерных систем и сетей : учеб. пособие / Т.П. Барановская [и др.] ; под ред. В.И. Лойко. М. : Финансы и статистика, 2003.

Бормотов, С.В. Системное администрирование на 100 % / С.В. Бормотов. СПб. : Питер, 2006. + 1 эл. опт. диск (CD).

Бройдо, В.Л. Вычислительные системы, сети и телекоммуникации / В.Л. Бройдо. СПб. : Питер, 2003.

Ватаманюк, А.И. Создание, обслуживание и администрирование сетей на 100 % / А.И. Ватаманюк. СПб. : Питер, 2010.

Галатенко, В.А. Основы информационной безопасности: курс лекций : учеб. пособие / В.А. Галатенко ; под ред. академика РАН В.Б. Бетелина. 3-е изд. М. : ИНТУИТ. РУ «Интернет-университет информационных технологий», 2006.

Гук, М.Ю. Аппаратные средства локальных сетей. Энциклопедия / М.Ю. Гук. СПб. : Питер, 2004.

Гультяев, А.К. Виртуальные машины: несколько компьютеров в одном / А.К. Гультяев. СПб. : Питер. 2006. + 1 эл. опт. диск (CD).

Иванов, В.Б. Компьютерные коммуникации : учеб. пособие / В.Б. Иванов. СПб. : Питер 2002.

Камер, Э. Дуглас. Компьютерные сети и Internet / Дуглас Э. Камер. М. : Издательский дом «Вильямс», 2002.

Крупич, А.А. Телекоммуникационные системы и компьютерные сети. Курс лекций / А.А. Крупич, О.А. Сосновский. Минск : БГЭУ, 2012.

Кузин, А.В. Компьютерные сети : учеб. пособие / А.В. Кузин, В.М. Демин. М. : ФОРУМ : ИНФРА-М, 2005.

Кульгин, М.В. Компьютерные сети. Практика построения. Для профессионалов / М.В. Кульгин. 2-е изд. СПб. : Питер, 2003.

Максимов, Н.В. Компьютерные сети : учеб. пособие / Н.В. Максимов, И.И. Попова. М. : ФОРУМ : ИНФРА-М, 2005.

Нанс, Б. Компьютерные сети / Б. Нанс ; пер. с англ. Ш.С. Зейналова ; под ред. А.В. Голдецкого, В.Е. Кошелева. М. : Восточная Книжная Компания, 1996.

Новиков, Ю.В. Основы локальных сетей: курс лекций : учеб. пособие / Ю.В. Новиков, С.В. Кондратенко. М. : ИНТУИТ.РУ «Интернет-университет информационных технологий», 2005.

Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы : учеб. / В.Г. Олифер, Н.А. Олифер. 4-е изд. СПб. : Питер, 2010.

Олифер, В.Г. Основы сетей передачи данных. Курс лекций : учеб. пособие / В.Г. Олифер, Н.А. Олифер. 2-е изд., испр. М. : ИНТУИТ.РУ «Интернет-университет информационных технологий», 2005.

Пасько, В.П. Энциклопедия ПК. Аппаратура. Программы. Интернет / В.П. Пасько. Киев : Издательская группа BHV ; СПб. : Питер, 2004.

Поляк-Брагинский, А.В. Администрирование сети на примерах / А.В. Поляк-Брагинский. СПб. : БХВ-Петербург, 2005.

Пятибратов, А.П. Вычислительные системы, сети и телекоммуникации : учеб. / А.П. Пятибратов, Л.П. Гудыно, А.А. Кириченко ; под ред. А.П. Пятибратова. 2-е изд., перераб. и доп. М. : Финансы и статистика, 2004.

Столлингс, В. Современные компьютерные сети / В. Столлингс. 2-е изд. СПб. : Питер, 2003.

Таненбаум, Э. Компьютерные сети / Э. Таненбаум. 4-е изд. СПб. : Питер, 2010.

Шиндер, Д.Л. Основы компьютерных сетей / Д.Л. Шиндер. М. : Издательский дом «Вильямс», 2002.

ОГЛАВЛЕНИЕ