Содержание

Глава 1. Определение локальных сетей и их топология

Содержание первой главы:

1.1. Место и роль локальных сетей

Передача информации между компьютерами существует с момента возникновения вычислительной техники. Она позволяет организовать совместную работу отдельных компьютеров, решать одну задачу с помощью нескольких компьютеров, специализировать каждый из компьютеров на выполнении какой-то одной функции, совместно использовать ресурсы и решать множество других проблем. Способов и средств обмена информацией за последнее время предложено множество: от простейшего переноса файлов с помощью дискеты до всемирной компьютерной сети Internet, способной связать все компьютеры мира. Какое же место во всей этой иерархии отводится локальным сетям?

Чаще всего термин «локальные сети» (LAN, Local Area Network) понимают буквально, то есть под локальными понимаются такие сети, которые имеют небольшие, локальные размеры, соединяют близко расположенные компьютеры. Однако достаточно посмотреть на характеристики некоторых локальных сетей, чтобы понять, что такое определение не слишком точно. Например, некоторые локальные сети легко обеспечивает связь на расстоянии нескольких километров или даже десятков километров. Это уже размеры не комнаты, не здания, не близко расположенных зданий, а, может быть, целого города. С другой стороны, по глобальной сети (WAN, Wide Area Network или GAN, Global Area Network) вполне могут связываться компьютеры, находящиеся на соседних столах в одной комнате, но ее почему-то никто не называет локальной сетью. Близко расположенные компьютеры могут также связываться с помощью кабеля, соединяющего разъемы внешних интерфейсов (RS232-C, Centronics) или даже без кабеля по инфракрасному каналу. Но такая связь также не называется локальной сетью.

Неверно и определение локальной сети как малой сети, которая связывает небольшое количество компьютеров. Действительно, в реальности наиболее часто локальная сеть связывает от двух до нескольких десятков компьютеров. Но предельные возможности некоторых локальных сетей гораздо выше: максимальное число абонентов может достигать тысячи. Называть такую сеть малой, наверное, неправильно.

Некоторые авторы определяют локальную сеть как «систему для непосредственного соединения многих компьютеров». При этом подразумевается, что информация передается от компьютера к компьютеру без посредников и по единой среде передачи. Однако говорить о единой среде передачи в современной локальной сети не приходится. Например, в пределах одной сети могут использоваться как электрические кабели различных типов, так и оптоволоконные кабели. Определение передачи «без посредников» также не слишком четко, ведь в современных локальных сетях используются самые разнообразные концентраторы, коммутаторы, маршрутизаторы, мосты, которые порой производят довольно сложную обработку передаваемой информации. Не совсем понятно, считать их посредниками или нет.

Наверное, наиболее точно было бы определить как локальную такую сеть, которая позволяет пользователям не замечать связи. Компьютеры, связанные локальной сетью, объединяются, по сути, в один виртуальный компьютер, ресурсы которого могут быть доступны всем пользователям, причем этот доступ не менее удобен, чем к ресурсам, входящим непосредственно в каждый отдельный компьютер. Под удобством в первую очередь понимается в данном случае высокая реальная скорость доступа, при которой обмен информацией между приложениями осуществляется незаметно для пользователя. При таком определении ни медленные глобальные сети, ни медленная связь через последовательный или параллельный порты не подпадают под понятие локальной сети.

Из такого определения сразу же следует, что скорость передачи по локальной сети должна обязательно расти по мере роста быстродействия наиболее распространенных компьютеров. Именно это мы и наблюдаем: если еще сравнительно недавно вполне приемлемой считалась скорость обмена в 1-10 Мбит/с, то сейчас среднескоростной считается сеть, работающая на скорости 100 Мбит/с и активно разрабатываются средства для скорости 1000 Мбит/с и даже больше. При меньших скоростях передачи связь станет узким местом, будет чрезмерно замедлять работу объединенного сетью виртуального компьютера.

Таким образом, главное отличие локальной сети от любой другой — высокая скорость обмена. Но это не единственное отличие, не менее важны и другие факторы.

Например, принципиально необходим низкий уровень ошибок передачи. Ведь даже очень быстро переданная, но искаженная ошибками информация бессмысленна — ее придется передавать еще раз. Поэтому локальные сети обязательно используют специально прокладываемые качественные линии связи.

Принципиальное значение имеет и такая характеристика сети, как возможность работы с большими нагрузками, то есть с большой интенсивностью обмена (или, как еще говорят, с большим трафиком). Если механизм управления обменом, используемый в сети, не слишком эффективен, то компьютеры могут чрезмерно долго ждать своей очереди на передачу, и даже если передача будет производиться затем на высочайшей скорости и полностью безошибочно, то для пользователя сети это все равно обернется неприемлемой задержкой доступа ко всем сетевым ресурсам.

Любой механизм управления обменом может гарантированно работать только тогда, когда заранее известно, сколько компьютеров (абонентов, узлов) может быть подключено к сети. При включении непредусмотренно большого числа абонентов забуксует вследствие перегрузки любой механизм. Наконец, сетью в истинном смысле этого слова можно назвать только такую систему передачи данных, которая позволяет объединять хотя бы до нескольких десятков компьютеров, но никак не два, как в случае связи через стандартные порты.

Таким образом, можно сформулировать следующие отличительные признаки локальной сети:

- высокая скорость передачи, большая пропускная способность;
- низкий уровень ошибок передачи (или, что то же самое, высококачественные каналы связи). Допустимая вероятность ошибок передачи данных должна быть порядка 10"7 — 10~8;
- эффективный, быстродействующий механизм управления обменом;
- ограниченное, точно определенное число компьютеров, подключаемых к сети.

При таком определении понятно, что глобальные сети отличаются от локальных тем, что рассчитаны на неограниченное число абонентов и используют, как правило, не слишком качественные каналы связи и сравнительно низкую скорость передачи, а механизм управления обменом в них в принципе не может быть гарантированно быстрым. В глобальных сетях гораздо важнее не качество связи, а сам факт ее существования.

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

Правда, сейчас уже нельзя провести четкую и однозначную 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 выданном 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. Кстати, именно задача передачи изображений, особенно полноцветных динамических изображений, предъявляет самые высокие требования к быстродействию сети. Чаще всего локальные сети используются для разделения (то есть 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. Абонентами (узлами) сети могут быть не только компьютеры, но и другие устройства, например принтеры, плоттеры, сканеры. Локальные сети дают возможность организовать систему параллельных вычислений на всех компьютерах сети, что позволяет многократно ускорить решение сложных математических задач. С их помощью можно также управлять работой сложной технологической системы или исследовательской установки с нескольких компьютеров одновременно.

Однако локальные сети имеют и некоторые недостатки, о которых всегда следует помнить. Помимо дополнительных материальных затрат на покупку оборудования и сетевого программного обеспечения, на прокладку соединительных кабелей и обучение персонала, необходимо также иметь специалиста, который будет заниматься контролем за работой сети, модернизацией сети, управлением доступом к ресурсам, устранением возможных неисправностей — то есть администратора сети. Сети ограничивают возможности перемещения компьютеров, так как при этом может понадобиться перекладка соединительных кабелей. Кроме того, сети представляют собой прекрасную среду для распространения компьютерных вирусов,

поэтому вопросам защиты придется уделять гораздо больше внимания, чем в случае автономного использования компьютеров. Так что ничто не дается даром.

Здесь же упомянем о таких важнейших понятиях теории сетей, как сервер и клиент.

Сервером называется абонент (узел) сети, который предоставляет свои ресурсы другим абонентам, но сам не использует ресурсы других абонентов, то есть служит только сети. Серверов в сети может быть несколько, и совсем не обязательно сервер — это самый мощный компьютер. Выделенный сервер — это сервер, занимающийся только сетевыми задачами. Невыделенный сервер может заниматься помимо обслуживания сети и другими задачами. Специфический тип сервера — это сетевой принтер.

Клиентом называется абонент сети, который только использует сетевые ресурсы, но сам свои ресурсы в сеть не отдает, то есть сеть его обслуживает. Компьютер-клиент также часто называют рабочей станцией. 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 то приложение, которое только отдает ресурс в сеть, является сервером, а то приложение, которое только пользуется сетевыми ресурсами, является клиентом.

1.2. Топология локальных сетей

Под топологией (компоновкой, конфигурацией, структурой) компьютерной сети обычно понимается 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 не слишком важна, так как каждый сеанс связи может производиться по своему собственному пути.

Топология определяет требования к оборудованию, тип используемого кабеля, возможные и наиболее удобные методы управления обменом, надежность работы, возможности расширения сети. И хотя выбирать топологию пользователю сети приходится нечасто, знать об особенностях основных топологий, их достоинствах и недостатках, наверное, надо всем.

Существует три основных топологии сети:

- шина (bus), при которой все компьютеры параллельно подключаются к одной линии связи и информация от каждого компьютера одновременно передается всем остальным компьютерам (рис. 1.1);
- звезда (star), при которой к одному центральному компьютеру присоединяются остальные периферийные компьютеры, причем каждый из них использует свою отдельную линию связи (рис. 1.2);
- кольцо (ring), при которой каждый компьютер передает информацию всегда только одному компьютеру, следующему в цепочке, а получает информацию только от предыдущего в цепочке компьютера, и эта цепочка замкнута в «кольцо» (рис. 1.3).
-

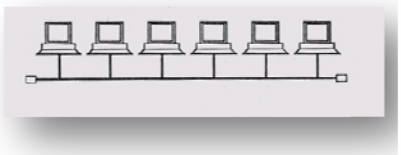


Рис. 1.1
Сетевая топология «шина»

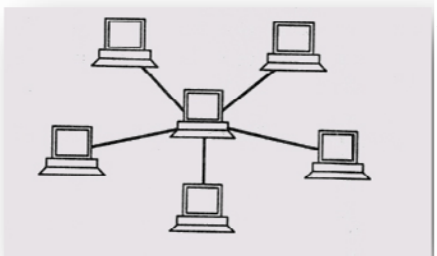


Рис. 1.2
Сетевая топология «звезда»

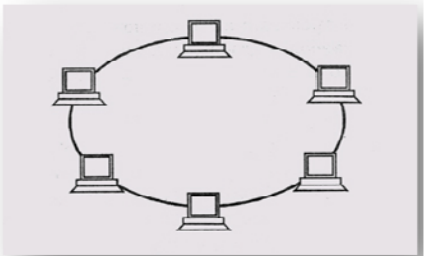


Рис. 1.3
Сетевая топология «кольцо»

На практике нередко используют и комбинации базовых топологий, но большинство сетей ориентированы именно на эти три. Рассмотрим теперь кратко особенности перечисленных сетевых топологий.

1.2.1. Топология «шина»

Топология «шина» (или, как ее еще называют, «общая шина») самой своей структурой предполагает идентичность сетевого оборудования компьютеров, а также равноправие всех абонентов. При таком соединении компьютеры могут передавать только по очереди, так как линия связи единственная. В

противном случае передаваемая информация будет искажаться в результате наложения (конфликта, коллизии). Таким образом, в шине реализуется режим полудуплексного (half duplex) обмена (в обоих направлениях, но по очереди, а не одновременно).

В топологии «шина» отсутствует центральный абонент, через которого передается вся информация, что увеличивает ее надежность (ведь при отказе любого центра перестает функционировать вся управляемая этим центром 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. Правда, надо учесть, что к каждому компьютеру (кроме двух крайних) подходит два кабеля, что не всегда удобно.

Так как разрешение возможных конфликтов в данном случае ложится на сетевое оборудование каждого отдельного абонента, аппаратура сетевого адаптера при топологии «шина» получается сложнее, чем при других топологиях. Однако из-за широкого распространения сетей с топологией «шина» (Ethernet, Arcnet) стоимость сетевого оборудования получается не слишком высокой.

Шине не страшны отказы отдельных компьютеров, так как все остальные компьютеры сети могут нормально продолжать обмен. Может показаться, что шине не страшен и обрыв кабеля, поскольку в этом случае мы получим две вполне работоспособные шины. Однако из-за особенностей распространения электрических сигналов по длинным линиям связи необходимо предусматривать включение на концах шины специальных согласующих устройств — терминаторов, показанных на рис. 1.1 в виде прямоугольников. Без включения терминаторов сигнал отражается от конца линии и искажается так, что связь по сети становится невозможной. Так что при разрыве или повреждении кабеля (например, мышами, которые почему-то очень любят грызть кабели сети) нарушается согласование линии связи, и прекращается обмен даже между теми компьютерами, которые остались соединенными между собой. Подробнее о согласовании будет рассказано в специальном разделе книги. Короткое замыкание в любой точке кабеля шины выводит из строя всю сеть. Любой отказ сетевого оборудования в шине очень трудно локализовать, так как все адаптеры включены параллельно, и понять, какой из них вышел из строя, не так-то просто.

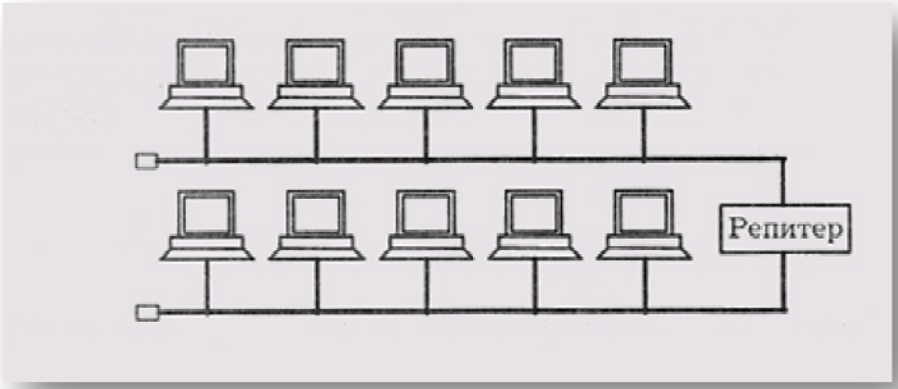


Рис. 1.4
Соединение сегментов сети типа «шина» с помощью репитера

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, кроме того, 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 (каждый из которых представляет собой шину), соединенных между собой с помощью специальных восстановителей сигналов — репитеров, или повторителей (на рис. 1.4 показано соединение двух сегментов).

Однако такое наращивание длины сети не может продолжаться бесконечно, так как существуют еще и ограничения, связанные с конечной скоростью распространения сигналов по линиям связи.

1.2.2. Топология «звезда»

«Звезда» — это топология с явно выделенным центром, к которому подключаются все остальные абоненты. Весь обмен информацией идет исключительно через центральный компьютер, на который таким образом ложится очень большая нагрузка, поэтому ничем другим, кроме сети, он заниматься не может. Понятно, что сетевое оборудование центрального абонента должно быть существенно более сложным, чем оборудование периферийных абонентов. О равноправии абонентов в данном случае говорить не

приходится. Как правило, именно центральный компьютер является самым мощным, и именно на него возлагаются все функции по управлению обменом. Никакие конфликты в сети с топологией «звезда» в принципе невозможны, так как управление полностью централизовано, конфликтовать нечему.

Если говорить об устойчивости звезды к отказам компьютеров, то выход из строя периферийного компьютера никак не отражается на функционировании оставшейся части сети, зато любой отказ центрального компьютера делает сеть полностью неработоспособной. Поэтому должны приниматься специальные меры по повышению надежности центрального компьютера и его сетевой аппаратуры. Обрыв любого 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 только в одном направлении. Таким образом, на каждой линии связи имеется только один приемник и один передатчик. Все это существенно упрощает сетевое оборудование по сравнению с шиной и избавляет от необходимости применения дополнительных внешних терминаторов. Проблема затухания сигналов в линии связи также решается в «звезде» проще, чем в «шине», ведь каждый приемник всегда получает сигнал одного уровня.

Серьезный недостаток топологии «звезда» состоит в жестком ограничении количества абонентов. Обычно центральный абонент может обслуживать не более 8-16 периферийных абонентов. Если в этих пределах подключение новых абонентов довольно просто, то при их превышении оно просто невозможно. Правда, иногда в звезде предусматривается возможность наращивания, то есть подключение вместо одного из периферийных абонентов еще одного центрального абонента (в результате получается топология из нескольких соединенных между собой звезд).

Звезда, показанная на рис. 1.2, носит название активной, или истинной, звезды. Существует также топология, называемая пассивной звездой, которая только внешне похожа на звезду (рис. 1.5). В настоящее время она распространена гораздо больше, чем активная звезда. Достаточно сказать, что она используется в самой популярной на сегодняшний день сети Ethernet.

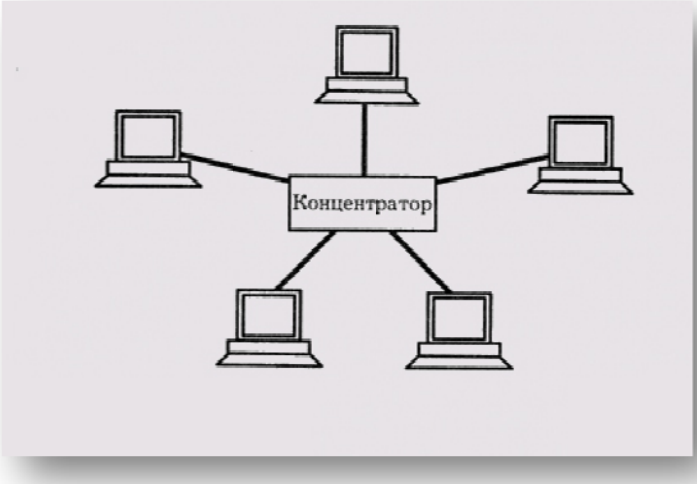


Рис. 1.5
Топология «пассивная звезда»

В центре сети с данной топологией помещается не компьютер, а концентратор, или хаб (hub), выполняющий ту же функцию, что и репитер. Он восстанавливает приходящие сигналы и пересылает их в другие линии связи. Хотя схема прокладки кабелей подобна истинной или активной звезде, фактически мы имеем дело с шинной топологией, так как информация от каждого компьютера одновременно передается ко всем остальным компьютерам, а центрального абонента не существует. Естественно, пассивная звезда получается дороже обычной шины, так как в этом случае обязательно требуется еще и концентратор. Однако она предоставляет целый ряд дополнительных возможностей, связанных с преимуществами звезды. Именно поэтому в последнее время пассивная звезда все больше вытесняет истинную шину, 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 сети путем простого отключения от центра тех или иных абонентов (что невозможно,

например, в случае шины), а также ограничивать доступ посторонних лиц к жизненно важным для сети точкам подключения. К каждому периферийному абоненту в случае звезды может подходить как один кабель (по которому идет передача в обоих направлениях), так и два кабеля (каждый из них передает в одном направлении), причем вторая ситуация встречается чаще.

Общим недостатком для всех топологий типа «звезда» является значительно больший, чем при других топологиях, расход кабеля. Например, если компьютеры расположены в одну линию (как на рис. 1.1), то при выборе топологии «звезда» понадобится в несколько раз больше кабеля, чем при топологии «шина». Это может существенно повлиять на стоимость всей сети в целом.

1.2.3. Топология «кольцо»

«Кольцо» — это топология, в которой каждый компьютер соединен линиями связи только с двумя другими: от одного он только получает информацию, а другому только передает. На каждой линии связи, как и в случае звезды, работает только один передатчик и один приемник. Это позволяет отказаться от применения внешних терминаторов. Важная особенность кольца состоит в том, что каждый компьютер ретранслирует (восстанавливает) приходящий к нему сигнал, то есть выступает в роли репитера, поэтому затухание сигнала во всем кольце не имеет никакого значения, важно только затухание между соседними компьютерами кольца. Четко выделенного центра в данном случае нет, все компьютеры могут быть одинаковыми. Однако довольно часто в кольце выделяется специальный абонент, который управляет обменом или контролирует обмен. Понятно, что наличие такого управляющего абонента снижает надежность сети, так как выход его из строя сразу же парализует весь обмен.

Строго говоря, компьютеры в кольце не являются полностью равноправными (в отличие, например, от шинной топологии). Одни из них обязательно получают 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 этих методах право на следующую передачу (или, как еще говорят, на захват сети) переходит последовательно к следующему по кругу компьютеру.

Подключение новых абонентов в «кольцо» обычно совершенно безболезненно, хотя и требует обязательной остановки работы всей сети на время подключения. Как и в случае топологии «шина», максимальное количество абонентов в кольце может быть довольно велико (до тысячи и больше). Кольцевая топология обычно является самой устойчивой к перегрузкам, она обеспечивает уверенную работу с самыми большими потоками передаваемой по сети информации, так как в ней, как правило, нет конфликтов (в отличие от шины), а также отсутствует центральный абонент (в отличие от звезды).

Так как сигнал в кольце проходит через все компьютеры сети, выход из строя хотя бы одного из них (или же его сетевого оборудования) нарушает работу всей сети в целом. Точно так же любой обрыв или короткое замыкание в любом из кабелей кольца делает работу всей сети невозможной. Кольцо наиболее уязвимо к повреждениям кабеля, поэтому в этой топологии обычно предусматривают прокладку двух (или более) параллельных линий связи, одна из которых находится в резерве.

В то же время крупное преимущество кольца состоит в том, что ретрансляция сигналов каждым абонентом позволяет существенно увеличить размеры всей сети в целом (порой до нескольких десятков километров). Кольцо в этом отношении существенно превосходит любые другие топологии.

Недостатком кольца (по сравнению со звездой) можно считать то, что к каждому компьютеру сети необходимо подвести два кабеля.

Иногда топология «кольцо» выполняется на основе двух кольцевых линий связи, передающих информацию в противоположных направлениях. Цель подобного решения — увеличение (в идеале — вдвое) скорости передачи информации. К тому же при повреждении одного из кабелей сеть может работать с другим кабелем (правда, предельная скорость уменьшится).

1.2.4. Другие топологии

Кроме трех рассмотренных основных, базовых топологий нередко применяется также сетевая топология «дерево» (tree), которую можно рассматривать как комбинацию нескольких звезд. Как и в случае звезды, дерево может быть активным, или истинным (рис. 1.6), и пассивным (рис. 1.7). При активном дереве в центрах объединения нескольких линий связи находятся центральные компьютеры, а при пассивном — концентраторы (хабы).

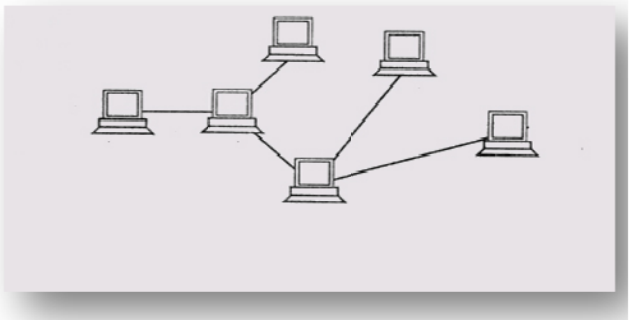


Рис. 1.6
Топология «активное дерево»

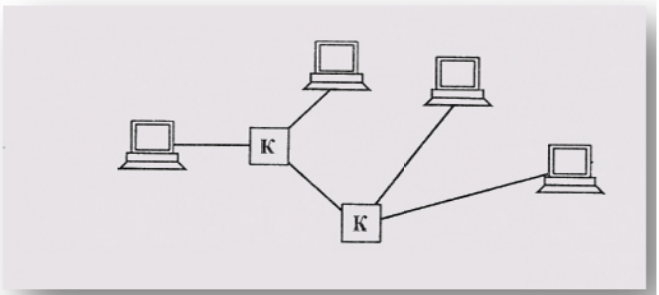


Рис. 1.7
Топология «пассивное дерево». К — концентраторы

Применяются довольно часто и комбинированные топологии, среди которых наибольшее распространение получили звездно-шинная (рис. 1.8) и звездно-кольцевая (рис. 1.9).

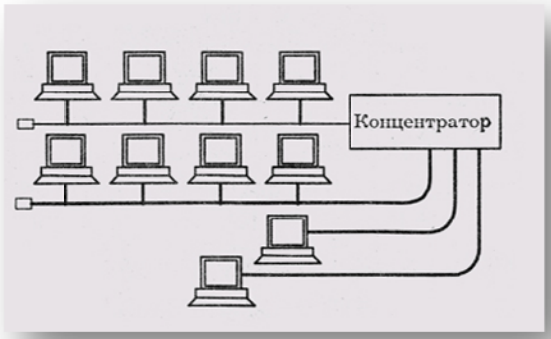


Рис. 1.8
Пример звездно-шинной топологии

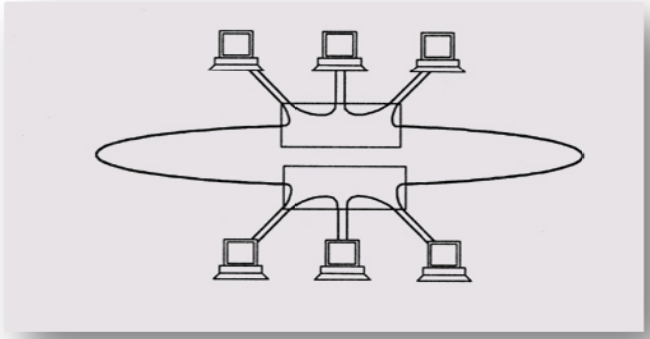


Рис. 1.9
Пример звездно-кольцевой топологии

В звездно-шинной (star-bus) топологии используется комбинация шины и пассивной звезды. В этом случае к концентратору подключаются как отдельные компьютеры, так и целые шинные сегменты, то есть на самом деле реализуется физическая топология «шина», включающая все компьютеры сети. В данной топологии может использоваться и несколько концентраторов, соединенных между собой и образующих так называемую магистральную, опорную шину. К каждому из концентраторов при этом подключаются отдельные компьютеры или шинные сегменты. Таким образом, пользователь получает возможность гибко комбинировать преимущества шинной и звездной топологий, а также легко изменять количество компьютеров, подключенных к сети.

В случае звездно-кольцевой (star-ring) топологии в кольцо объединяются не сами компьютеры, а специальные концентраторы (изображенные на рис. 1.9 в виде прямоугольников), к которым в свою очередь подключаются компьютеры с помощью звездообразных двойных линий связи. В действительности все компьютеры сети включаются в замкнутое кольцо, так как внутри концентраторов все линии связи образуют замкнутый контур (как показано на рис. 1.9). Данная топология позволяет комбинировать преимущества звездной и кольцевой топологий. Например, концентраторы позволяют собрать в одно место все точки подключения кабелей сети.

1.2.5. Многозначность понятия топологии

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

Более того, физическое расположение компьютеров, соединяемых сетью, вообще довольно слабо влияет на выбор топологии. Любые компьютеры, как бы они ни были расположены, всегда можно соединить с помощью любой заранее выбранной топологии (рис. 1.10).

В случае, когда соединяемые компьютеры расположены по контуру круга, они вполне могут соединяться звездой или шиной. Когда компьютеры расположены вокруг некоего центра, они вполне могут

соединяться между собой шиной или кольцом. Наконец, когда компьютеры расположены в одну линию, они могут соединяться звездой или кольцом. Другое дело, какова будет требуемая для этого суммарная длина кабеля.

Когда в литературе упоминается о топологии сети, то могут подразумевать четыре совершенно разных понятия, относящихся к различным уровням сетевой архитектуры.

Физическая топология (то есть схема расположения компьютеров и прокладки кабелей). В этом смысле, например, пассивная звезда ничем не отличается от активной звезды, поэтому ее нередко называют просто «звездой».

Логическая топология (то есть структура связей, характер распространения сигналов по сети). Это, наверное, наиболее правильное определение топологии.

Топология управления обменом (то есть принцип и последовательность передачи права на захват сети между отдельными компьютерами).

Информационная топология (то есть направление потоков информации, передаваемой по сети).

Например, сеть с физической и логической топологией «шина» может в качестве метода управления использовать эстафетную передачу права захвата сети (то есть быть в этом смысле кольцом) и одновременно передавать всю информацию через один выделенный компьютер (быть в этом смысле звездой). Сеть с логической топологией «шина» может иметь физическую топологию «звезда» (пассивная) или «дерево» (пассивное).

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

Заканчивая обзор особенностей топологий локальных сетей, необходимо отметить, что топология все-таки не является основным фактором при выборе типа сети. Гораздо важнее, например, уровень стандартизации сети, скорость обмена, количество абонентов, стоимость оборудования, выбранное программное обеспечение. Но, с другой стороны, некоторые сети позволяют использовать разные топологии на разных уровнях. Этот выбор уже целиком ложится на пользователя, который должен учитывать все перечисленные в данном разделе соображения.

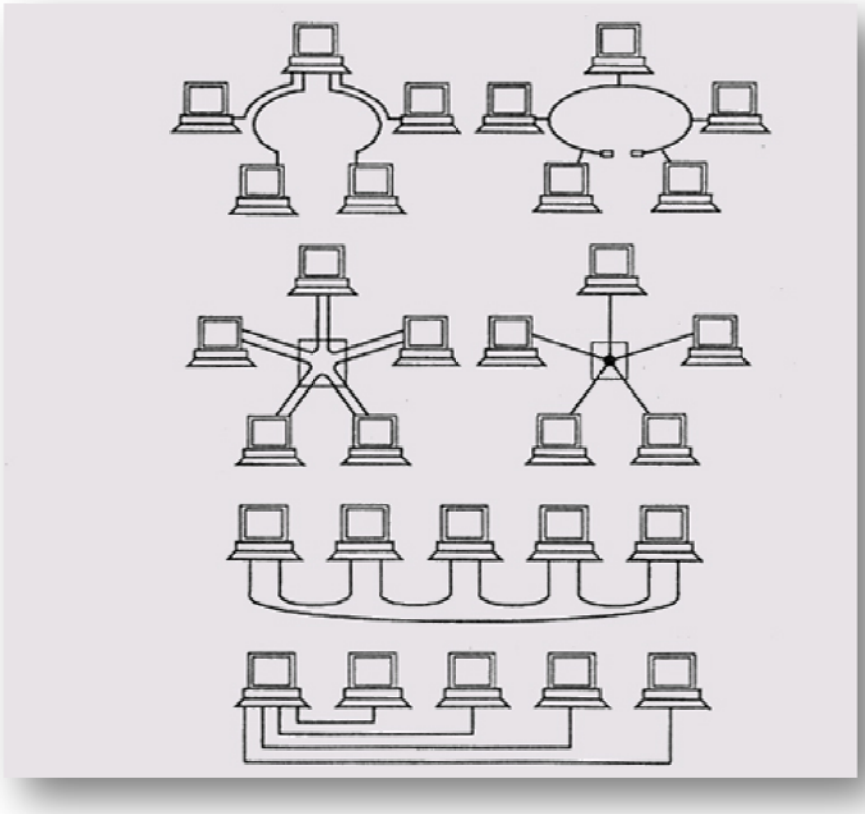


Рис. 1.10
Примеры использования разных топологий

Глава 2. Среды передачи информации

Содержание второй главы:

2.1. Коаксиальные кабели

Коаксиальный кабель представляет собой электрический кабель, состоящий из центрального провода и металлической оплетки, разделенных между собой слоем диэлектрика (внутренней изоляции) и помещенных в общую внешнюю оболочку (рис. 2.2).

Рис. 2.2
Коаксиальный кабель

Коаксиальный кабель до недавнего времени был распространен наиболее широко, что связано с его высокой помехозащищенностью (благодаря металлической оплетке), а также более высокими, чем в случае витой пары, допустимыми скоростями передачи данных (до 500 Мбит/с) и большими допустимыми расстояниями передачи (до километра и выше). К нему труднее механически подключиться для несанкционированного прослушивания сети, он также дает заметно меньше электромагнитных . излучений вовне. Однако монтаж и ремонт коаксиального кабеля существенно сложнее, чем витой пары, а стоимость его выше (он дороже примерно в 1,5-3 раза по сравнению с кабелем на основе витых пар). Сложнее и установка разъемов на концах кабеля. Поэтому его сейчас применяют реже, чем витую пару.

Основное применение коаксиальный кабель находит в сетях с топологией типа «шина». При этом на концах кабеля обязательно должны устанавливаться терминаторы для предотвращения внутренних отражений сигнала, причем один (и только один!) из терминаторов должен быть заземлен. Без заземления металлическая оплетка не защищает сеть от внешних электромагнитных помех и не снижает излучение передаваемой по сети информации во внешнюю среду. Но при заземлении оплетки в двух или более точках из строя может выйти не только сетевое оборудование, но и компьютеры, подключенные к сети (подробнее об этом — в специальном разделе этой главы). Терминаторы должны быть обязательно согласованы с кабелем, то есть их сопротивление должно быть равно волново му сопротивлению кабеля. Например, если используется 50-омный кабель, для него подходят только 50-омные терминаторы.

Реже коаксиальные кабели применяются в сетях с топологией «звезда» и «пассивная звезда» (например, в сети Arcnet). В этом случае проблема согласования существенно упрощается, так как внешних терминаторов на свободных концах не требуется.

Волновое сопротивление кабеля указывается в сопроводительной документации. Чаще всего в локальных сетях применяются 50-омные (например, RG-58, RG-11) и 93-омные кабели (например, RG-62). 75-омные кабели, распространенные в телевизионной технике, в локальных сетях не используются. Вообще, марок коаксиального кабеля значительно меньше, чем кабелей на основе витых пар. Он не считается особо перспективным. Не случайно в сети Fast Ethernet не предусмотрено применение коаксиальных кабелей. Однако во многих случаях классическая шинная топология (а не пассивная звезда) очень удобна. Как уже отмечалось, она не требует применения дополнительных устройств — концентраторов.

Существует два основных типа коаксиального кабеля:

тонкий (thin) кабель, имеющий диаметр около 0,5 см, более гибкий;

толстый (thick) кабель, имеющий диаметр около 1 см, значительно более жесткий. Он представляет собой классический вариант коаксиального кабеля, который уже почти полностью вытеснен более современным тонким кабелем.

Тонкий кабель используется для передачи на меньшие расстояния, чем толстый, так как в нем сигнал затухает сильнее. Зато с тонким кабелем гораздо удобнее работать: его можно оперативно проложить к каждому компьютеру, а толстый требует жесткой фиксации на стене помещения. Подключение к тонкому кабелю (с помощью разъемов BNC байонетного типа) проще и не требует дополнительного оборудования, а для подключения к толстому кабелю надо использовать специальные довольно дорогие устройства, прокалывающие его оболочки и устанавливающие контакт как с центральной жилой, так и с экраном. Толстый кабель примерно вдвое дороже, чем тонкий. Поэтому тонкий кабель применяется гораздо чаще.

Как и в случае витых пар, важным параметром коаксиального кабеля является тип его внешней оболочки. Точно так же в данном случае применяются как non-plenum (PVC), так и plenum кабели. Естественно, теф-лоновый кабель дороже поливинилхлоридного. Обычно тип оболочки можно отличить по ее окраске (например, для кабеля PVC фирма Belden использует желтый цвет, а для тефлонового — оранжевый).

Типичные величины задержки распространения сигнала в коаксиальном кабеле составляют для тонкого кабеля около 5 нс/м, а для толстого — около 4,5 нс/м.

Существуют варианты коаксиального кабеля с двойным экраном (один экран расположен внутри другого и отделен от него дополнительным слоем изоляции). Такие кабели имеют лучшую помехозащищенность и защиту от прослушивания, но они немного дороже обычных.

В настоящее время считается, что коаксиальный кабель устарел, в большинстве случаев его вполне может заменить витая пара или оптоволоконный кабель. Новые стандарты на кабельные системы уже не включают его в перечень типов кабелей.

2.2. Оптоволоконные кабели

Оптоволоконный (он же волоконно-оптический) кабель — это принципиально иной тип кабеля по сравнению с рассмотренными двумя типами электрического или медного кабеля. Информация по нему передается не электрическим сигналом, а световым. Главный его элемент — это прозрачное стекловолокно, по которому свет проходит на огромные расстояния (до десятков километров) с незначительным ослаблением.

Структура оптоволоконного кабеля очень проста и похожа на структуру коаксиального электрического кабеля (рис. 2.3), только вместо центрального медного провода здесь используется тонкое (диаметром порядка 1-10 мкм) стекловолокно, а вместо внутренней изоляции — стеклянная или пластиковая оболочка, не позволяющая свету выходить за пределы стекловолокна. В данном случае мы имеем дело с режимом так называемого полного внутреннего отражения света от границы двух веществ с разными коэффициентами преломления (у стеклянной оболочки коэффициент преломления значительно ниже, чем у центрального волокна). Металлическая оплетка кабеля обычно отсутствует, так как экранирование от внешних электромагнитных помех здесь не требуется, однако иногда ее все-таки применяют для механической защиты от окружающей среды (такой кабель иногда называют броневым, он может объединять под одной оболочкой несколько оптоволоконных кабелей).

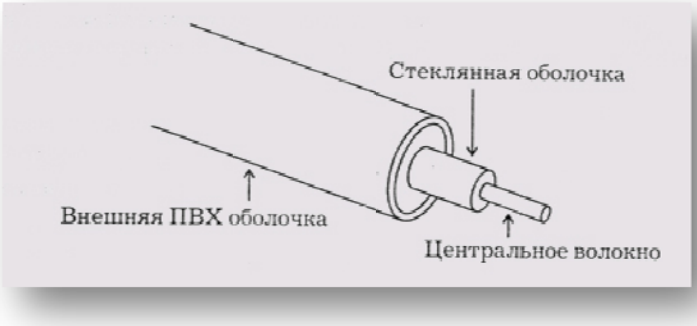


Рис. 2.3
Структура оптоволоконного кабеля

Оптоволоконный кабель обладает исключительными характеристиками по помехозащищенности и секретности передаваемой информации. Никакие внешние электромагнитные помехи в принципе не способны исказить световой сигнал, а сам этот сигнал принципиально не порождает внешних электромагнитных излучений. Подключиться к этому типу кабеля для несанкционированного прослушивания сети практически невозможно, так как это требует нарушения целостности кабеля. Теоретически возможная

полоса пропускания такого кабеля достигает величины 1012 Гц, что несравнимо выше, чем у любых электрических кабелей. Стоимость оптоволоконного кабеля постоянно снижается и сейчас примерно равна стоимости тонкого коаксиального кабеля. Однако в данном случае необходимо применение специальных оптических приемников и передатчиков, преобразующих световые сигналы в электрические и обратно, что порой существенно увеличивает стоимость сети в целом.

Типичная величина затухания сигнала в оптоволоконных кабелях на частотах, используемых в локальных сетях, составляет около 5 дБ/км, что примерно соответствует показателям электрических кабелей на низких частотах. Но в случае оптоволоконного кабеля при росте частоты передаваемого сигнала затухание увеличивается очень незначительно, и на больших частотах (особенно свыше 200 МГц) его преимущества перед электрическим кабелем неоспоримы, он просто не имеет конкурентов.

Однако оптоволоконный кабель имеет и некоторые недостатки.

Самый главный из них — высокая сложность монтажа (при установке разъемов необходима микронная точность, от точности скола стекловолокна и степени его полировки сильно зависит затухание в разъеме). Для установки разъемов применяют сварку или склеивание с помощью специального геля, имеющего такой же коэффициент преломления света, что и стекловолокно. В любом случае для этого нужна высокая квалификация персонала и специальные инструменты. Поэтому чаще всего оптоволоконный кабель продается в виде заранее нарезанных кусков разной длины, на обоих концах которых уже установлены разъемы нужного типа.

Хотя оптоволоконные кабели и допускают разветвление сигналов (для этого выпускаются специальные разветвители на 2-8 каналов), как правило, их используют для передачи данных только в одном направлении, между одним передатчиком и одним приемником. Ведь любое разветвление неизбежно сильно ослабляет световой сигнал, и если разветвлений будет много, то свет может просто не дойти до конца сети.

Оптоволоконный кабель менее прочен, чем электрический, и менее гибкий (типичная величина допустимого радиуса изгиба составляет около 10—20 см). Чувствителен он и к ионизирующим излучениям, из-за которых снижается прозрачность стекловолокна, то есть увеличивается затухание сигнала. Чувствителен он также к резким перепадам температуры, в результате которых стекловолокно может треснуть. В настоящее времы выпускаются оптические кабели из радиационно стойкого стекла (стоят они, естественно, дороже).

Оптоволоконные кабели чувствительны также к механическим воздействиям (удары, ультразвук) — так называемый микрофонный эффект. Для его уменьшения используют мягкие звукопоглощающие оболочки.

Применяют оптоволоконный кабель только в сетях с топологией «звезда» и «кольцо». Никаких проблем согласования и заземления в данном случае не существует. Кабель обеспечивает идеальную гальваническую развязку компьютеров сети. В будущем этот тип кабеля, вероятно, вытеснит электрические кабели всех типов или, во всяком случае, сильно потеснит их. Запасы меди на планете истощаются, а сырья для производства стекла более чем достаточно.

Существуют два различных типа оптоволоконных кабелей:

- многомодовый, или мультимодовый, кабель, более дешевый, но менее качественный;
- одномодовый кабель, более дорогой, но имеющий лучшие характеристики.

Основные различия между этими типами связаны с разным режимам прохождения световых лучей в кабеле.

В одномодовом кабеле практически все лучи проходят один и тот же путь, в результате чего все они достигают приемника одновременно, и форма сигнала практически не искажается. Одномодовый кабель имеет диаметр центрального волокна около 1,3 мкм и передает свет только с такой же длиной волны (1,3 мкм). Дисперсия и потери сигнала при этом очень незначительны, что позволяет передавать сигналы на значительно большее расстояние, чем в случае применения многомодового кабеля. Для одномо-дового кабеля применяются лазерные приемопередатчики, использующие свет исключительно с требуемой длиной волны. Такие приемопередатчики пока еще сравнительно дороги и не слишком долговечны. Однако в перспективе одномодовый кабель должен стать основным благодаря своим прекрасным характеристикам.

В многомодовом кабеле траектории световых лучей имеют заметный разброс, в результате чего форма сигнала на приемном конце кабеля искажается. Центральное волокно имеет диаметр 62,5 мкм, а диаметр внешней оболочки — 125 мкм (это иногда обозначается как 62,5/125). Для передачи используется обычный (не лазерный) светодиод, что снижает стоимость и увеличивает срок службы приемопередатчиков по сравнению с одномодовым кабелем. Длина волны света в многомодовом кабеле равна 0,85 мкм. Допустимая длина кабеля достигает 2-5 км. В настоящее время многомодовый кабель — основной тип оптоволоконного кабеля, так как он дешевле и доступнее.

Задержка распространения сигнала в оптоволоконном кабеле не сильно отличается от задержки в электрических кабелях. Типичная величина задержки для наиболее распространенных кабелей составляет около 4-5 нс/м.

2.3. Бескабельные каналы связи

Кроме кабельных, в компьютерных сетях иногда используются также бескабельные каналы. Их главное преимущество состоит в том, что не ребуется никакой прокладки проводов (не надо делать отверстий в стемах, не надо закреплять кабель в трубах и желобах, прокладывать его .од фальшполами, над подвесными потолками или в вентиляционных laxrax, не надо искать и устранять повреждения кабеля). К тому же компьютеры сети можно в этом случае легко перемещать в пределах комнаты или здания, так как они ни к чему не привязаны.

Радиоканал использует передачу информации по радиоволнам, поэтому я может обеспечить связь на многие десятки, сотни и даже тысячи километров. Скорость передачи может достигать десятков мегабит в секунду здесь многое зависит от выбранной длины волны и способа кодирования). Однако в локальных сетях радиоканал не получил широкого распространения из-за довольно высокой стоимости передающих и приемных устройств, низкой помехозащищенности, полного отсутствия секретности передаваемой информации и низкой надежности связи. А вот для глобальных сетей радиоканал часто является единственно возможным решением, так как позволяет с помощью спутников-ретрансляторов сравнительно просто обеспечить связь со всем миром. Используют радиоканал , и для связи двух и более локальных сетей, находящихся далеко друг от друга, в единую сеть.

Существует несколько стандартных типов радиопередачи информации. Остановимся на двух из них.

Передача в узком спектре (или одночастотная передача) рассчитана на охват площади до 46 500 м2. Радиосигнал в данном случае не проникает через металлические и железобетонные преграды, поэтому даже в пределах одного здания могут быть серьезные проблемы со связью. Связь в данном случае относительно медленная (около 4,8 Мбит/с).

Передача в рассеянном спектре для преодоления недостатков одночастотной передачи предполагает использование некоторой полосы частот, разделенной на каналы. Все абоненты сети через определенный временной интервал синхронно переходят на следующий канал. Для повышения секретности используется специальное кодирование информации. Скорость передачи при этом невысока — не более 2 Мбит/с, расстояние между абонентами — не более 3,2 км на открытом пространстве и не более 120 м внутри здания.

Кроме указанных типов, существуют и другие радиоканалы, например сотовые сети, строящиеся по тем же принципам, что и сотовые телефонные сети (они используют равномерно распределенные по площади ретрансляторы), а также микроволновые сети, применяющие узконаправленную передачу между наземными объектами или между спутником и наземной станцией.

Инфракрасный канал также не требует соединительных проводов, так как использует для связи инфракрасное излучение (подобно пульту дистанционного управления домашнего телевизора). Главное его преимущество по сравнению с радиоканалом — нечувствительность к электромагнитным помехам, что позволяет применять его, например, в производственных условиях. Правда, в данном случае требуется довольно высокая мощность передачи, чтобы не влияли никакие другие источники теплового (инфракрасного) излучения. Плохо работает инфракрасная связь и в условиях сильной запыленности воздуха.

Предельные скорости передачи информации по инфракрасному каналу не превышают 5-10 Мбит/с. Секретность передаваемой информации, как /чае радиоканала, также не достигается. Как и в случае радиоканала требуются сравнительно дорогие приемники и передатчики. Все это приводит к тому, что применяют инфракрасные каналы довольно редко.

Инфракрасные каналы делятся на две группы:

Каналы прямой видимости, в которых связь осуществляется на лучах, идущих непосредственно от передатчика к приемнику. При этом связь возможна только при отсутствии препятствий между компьютерами сети. Протяженность канала прямой видимости может достигать нескольких километров.

Каналы на рассеянном излучении, которые работают на сигналах, отраженных от стен, потолка, пола и других препятствий. Препятствия в данном случае не страшны, но связь может осуществляться только в пределах одного помещения.

Если говорить о возможных топологиях, то наиболее естественно все беспроводные каналы связи подходят для топологии типа «шина», в которой яация передается одновременно всем абонентам. Но в принципе при организации узконаправленной передачи можно реализовать любые TOPI (кольцо, звезда, комбинированные топологии) как на радиоканале, так и на инфракрасном канале.

2.4. Согласование, экранирование пьваническая развязка линий связи

Как уже отмечалось, любые электрические линии связи требуют принятия специальных мер, без которых невозможна не только безошибочная передача данных, но и любое функционирование сети. Оптоволоконные решают все подобные проблемы автоматически.

Согласование электрических линий связи применяется для обеспечения нормального прохождения сигнала по длинной линии без отражений и искажений. Принцип согласования очень прост: на концах кабеля необходимо установить согласующие резисторы (терминаторы) с сопротив-равным волновому сопротивлению используемого кабеля.

Волновое сопротивление — это параметр данного типа кабеля, зависящий его устройства (сечения, количества и формы проводников, тол-материала изоляции и т.д.). Величина волнового сопротивления обязательно указывается в документации на кабель и составляет обычно от 50-100 Ом для коаксиального кабеля до 100-150 Ом для витой пары или плоского многопроводного кабеля. Точное значение волнового сопротивления легко можно измерить с помощью генератора импульсов и осциллографа по отсутствию искажения формы передаваемого по кабелю импульса. Обычно требуется, чтобы отклонение величины согласующего резистора не превышало 5~10% в ту или другую сторону.

Если согласующее сопротивление RH меньше волнового сопротивления кабеля RB, то фронт передаваемого прямоугольного импульса на приемном конце будет затянут, если же RH больше RB, то на фронте будет колебательный процесс (рис. 2.4).

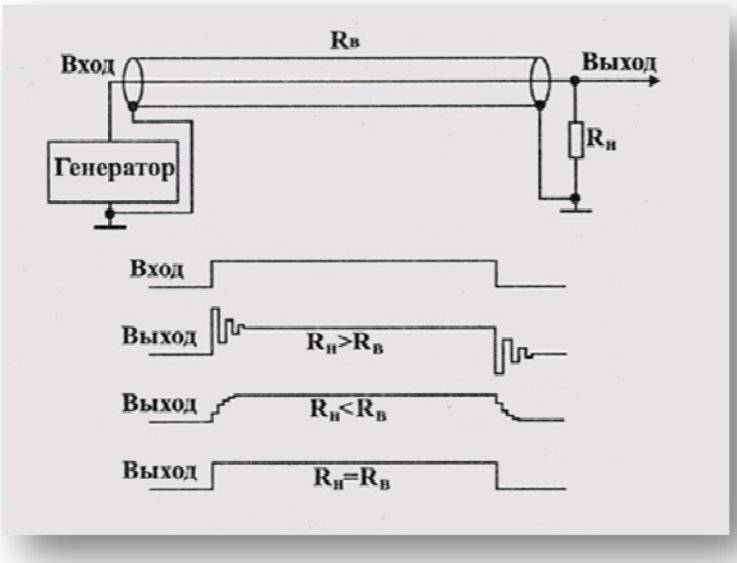


Рис. 2.4
Передача сигналов по электрическому кабелю

Надо сказать, что сетевые адаптеры, их приемники и передатчики специально рассчитываются на работу с данным типом кабеля с известным волновым сопротивлением. Поэтому даже при идеально согласованном на концах кабеле, волновое сопротивление которого существенно отличается от стандартного, сеть, скорее всего, работать не будет или будет работать со сбоями.

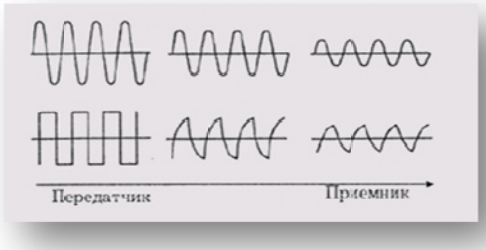


Рис. 2.5
Затухание сигналов в электрическом кабеле

Рис. 2.6
Трапецевидный и колоколообразный импульсы

Здесь же стоит упомянуть о том, что сигналы с пологими фронтами передаются по длинному электрическому кабелю лучше, чем сигналы с крутыми фронтами, то есть их форма меньше искажается (рис. 2.5). Это связано с разницей величин затухания для разных частот (высокие частоты затухают сильнее).

Меньше всего искажается форма синусоидального сигнала, такой сигнал просто уменьшается по амплитуде. Поэтому для улучшения качества передачи нередко используются трапецевидные или колоколообразные импульсы (рис. 2.6), близкие по форме к полуволне синуса, для чего искусственно затягиваются или сглаживаются фронты изначальных прямоугольных сигналов.

Экранирование электрических линий связи применяется для снижения влияния на кабель внешних электромагнитных полей. Экран представляет собой медную или алюминиевую оболочку (плетеную или из фольги), в которую заключаются провода кабеля. Для того чтобы экранирование работало, экран обязательно должен быть заземлен — в этом случае наведенные на него токи стекают на землю. Экран заметно увеличивает стоимость кабеля, но в то же время повышает его механическую прочность.

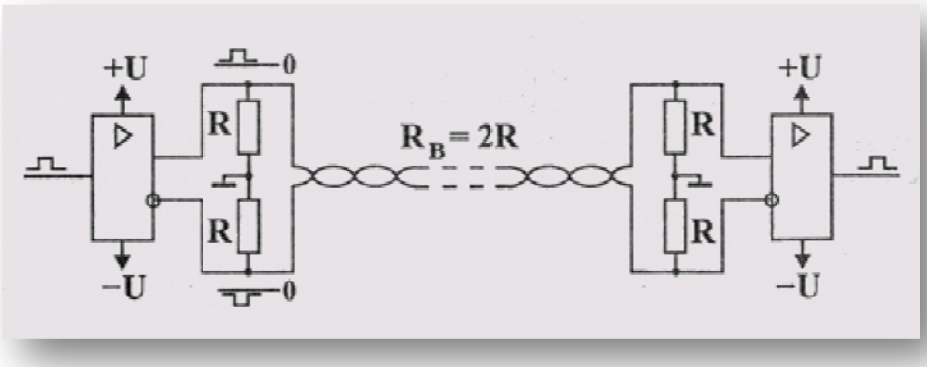


Рис. 2.7
Дифференциальная передача сигналов по витой паре

Снизить влияние наведенных помех можно и без экрана, если использовать дифференциальную передачу сигнала (рис. 2.7). В этом случае передача идет по двум проводам, оба они являются сигнальными. Передатчик формирует противофазные сигналы, а приемник реагирует на разность сигналов на обоих проводах. Условием согласования является равенство сопротивлений согласующих резисторов половине волнового сопротивления кабеля. Если оба провода имеют одинаковую длину и проложены рядом (в одном кабеле), то помехи действуют на оба провода примерно одинаково, и разностный сигнал между проводами практически не искажается. Именно такая дифференциальная передача применяется обычно в кабелях из витых пар. Но экранирование и в этом случае существенно улучшает помехоустойчивость.

Гальваническая развязка компьютеров от сети при использовании электрического кабеля совершенно необходима. Дело в том, что по электрическим кабелям (как по сигнальным проводам, так и по экрану) могут идти не только информационные сигналы, но и так называемый выравнивающий ток, возникающий вследствие неидеальности заземления компьютеров.

Когда компьютер не заземлен, на его корпусе образуется наведенный потенциал около 110В переменного тока (половина питающего напряжения). Его можно ощутить на себе, если одной рукой взяться за корпус компьютера, а другой за батарею центрального отопления или за какой-нибудь заземленный прибор.

При автономной работе компьютера (например, дома) отсутствие заземления, как правило, не оказывает серьезного влияния на его работу. Правда, иногда может увеличиться количество сбоев в работе компьютера. Но при соединении нескольких территориально разнесенных компьютеров электрическим кабелем заземление становится серьезной проблемой. Если один из соединяемых компьютеров заземлен, а другой не заземлен, то возможен даже полный выход из строя одного из них или обоих.

Поэтому компьютеры крайне желательно заземлять. В случае использования трехконтактной вилки и розетки, в которых есть нулевой провод, это получается автоматически. При двухконтактной вилке и розетке необходимо принимать специальные меры, организовывать заземление отдельным проводом большого сечения. Стоит также отметить, что в случае трехфазной сети желательно обеспечить питание всех компьютеров от одной фазы.

Но проблема осложняется еще и тем, что « земля », к которой присоединяются компьютеры, обычно далека от идеала. В идеале заземляющие провода компьютеров должны сходиться в одной точке, соединенной короткой массивной шиной с зарытым в землю массивным проводником. Такая ситуация возможна только тогда, когда компьютеры не слишком разнесены, а заземление действительно сделано грамотно. Обычно же заземляющая шина имеет значительную длину, в результате чего стекающие по ней токи создают значительную разность потенциалов между ее отдельными точками. Особенно велика эта разность потенциалов в случае подключения к шине мощных и высокочастотных потребителей энергии.

Поэтому даже присоединенные к одной и той же шине, но в разных точках,-компьютеры имеют на своих корпусах разные потенциалы (рис. 2.8). В результате по электрическому кабелю, соединяющему компьютеры, течет выравнивающий ток (переменный с высокочастотными составляющими).

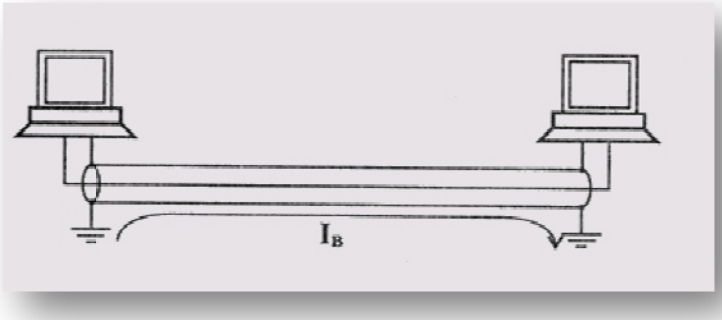


Рис. 2.8
Выравнивающий ток при отсутствии гальванической развязки

Ситуация ухудшается, когда компьютеры подключаются к разным шинам заземления. Выравнивающий ток может достигать в этом случае величины в несколько ампер. Понятно, что подобные токи смертельно опасны для малосигнальных узлов компьютера. В любом случае выравнивающий ток существенно влияет на передаваемый сигнал, порой полностью забивая его. Даже тогда, когда сигналы передаются без участия экрана (например, по двум проводам, заключенным в экран), выравнивающий ток, вследствие индуктивного действия, мешает передаче информации. Именно поэтому экран всегда должен быть заземлен только в од-ной-единственной точке.

Грамотное соединение компьютеров электрическим кабелем обязательно должно включать (рис. 2.9):

- оконечное согласование кабеля;
- гальваническую развязку компьютеров от сети (обычно трансформаторная гальваническая развязка входит в состав каждого сетевого адаптера);
- заземление каждого компьютера;
- заземление экрана (если, конечно, он есть) в одной-единственной точке.

Не стоит пренебрегать ни одним из этих требований. Например, гальваническая развязка сетевых адаптеров часто рассчитывается на допустимое напряжение изоляции всего лишь 100 В, что при отсутствии заземления одного из компьютеров может легко привести к выходу из строя его адаптера.

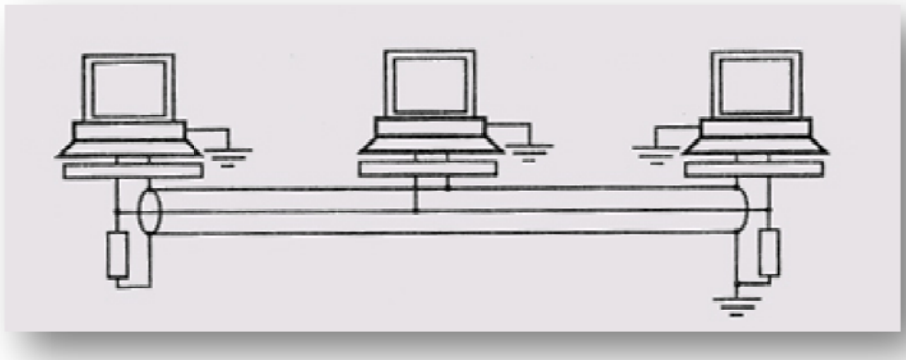


Рис. 2.9
Правильное соединение компьютеров сети
(гальваническая развязка условно показана в виде прямоугольника)

Отметим, что для присоединения коаксиального кабеля обычно применяются разъемы в металлическом корпусе. Этот корпус не должен соединяться ни с корпусом компьютера, ни с «землей» (на плате адаптера он установлен с пластиковой изоляцией от крепежной планки). Заземление экрана кабеля сети лучше производить не через корпус компьютера, а отдельным специальным проводом, что обеспечивает лучшую надежность. Пластмассовые корпуса разъемов RJ-45 для кабелей с неэкранированными витыми парами снимают эту проблему.

При заземлении экрана в одной точке он становится штыревой антенной с заземленным основанием и может усиливать ВЧ-помехи на нескольких частотах, кратных его длине. Для уменьшения этого «антенного» эффекта используют многоточечное заземление по высокой частоте, т.е. в одной точке экран соединяется с «землей» накоротко, а в остальных точках -через высоковольтные керамические

конденсаторы. В простейшем случае на одном конце кабеля экран соединяется с землей непосредственно, на другом конце — через емкость.

2.5. Кодирование информации в локальных сетях

Кодирование передаваемой по сети информации имеет самое непосредственное отношение к соотношению максимально допустимой скорости передачи и пропускной способности используемой среды передачи. Например, при разных кодах предельная скорость передачи по одному и тому же кабелю может отличаться в два раза. От выбранного кода прямо зависят также сложность сетевой аппаратуры и надежность передачи информации.

Некоторые коды, используемые в локальных сетях, показаны на рис. 2.10. Рассмотрим их преимущества и недостатки.

Код NRZ (Non Return to Zero — без возврата к нулю) — это простейший код, представляющий собой практически обычный цифровой сигнал (правда, возможно преобразование на обратную полярность или изменение уровней, соответствующих нулю и единице). К несомненным достоинствам кода NRZ относятся его очень простая реализация (исходный сигнал не надо ни кодировать на передающем конце, ни декодировать на приемном конце), а также минимальная среди других кодов пропускная способность линии связи, требуемая при данной скорости передачи. Пример: наиболее частое изменение сигнала в сети будет при непрерывном чередовании единиц и нулей, то есть при последовательности 10101010] 0..., поэтому при скорости передачи, равной 10 Мбит/с (длительность одного бита 100 не), частота изменения сигнала и соответственно.требуемая пропускная способность линии составит 1 / 200нс = 5 МГц (рис. 2.11).

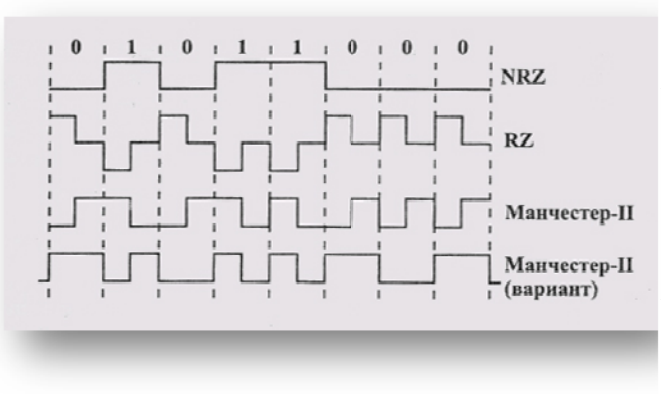


Рис. 2.10
Наиболее распространенные коды передачи информации

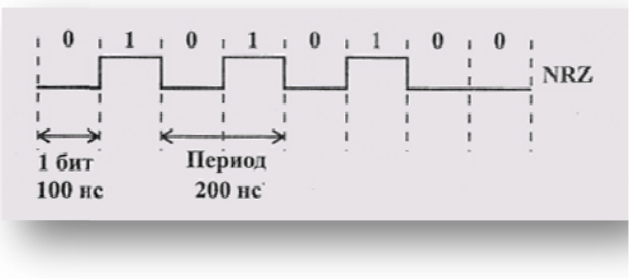


Рис. 2.11
Скорость передачи и требуемая пропускная способность при коде NRZ

Самый большой недостаток кода NRZ — это возможность потери синхронизации приемником при приеме слишком длинных блоков (пакетов) информации. Приемник может привязывать момент начала приема только к первому (стартовому) биту пакета, а в течение приема пакета он вынужден пользоваться только собственным внутренним тактовым генератором. Если часы приемника расходятся с часами передатчика в ту или другую сторону, то временной сдвиг к концу приема пакета может превысить длительность одного бита или даже нескольких бит. В результате произойдет потеря переданных данных. Так, при длине пакета в 10000 бит допустимое расхождение часов составит не более 0,01% даже при идеальной передаче формы сигнала по кабелю.

Чтобы избежать потери синхронизации, можно было бы ввести вторую линию связи для синхросигнала (рис. 2.12). Но при этом требуемое количество кабеля увеличивается в два раза, количество приемников и передатчиков также увеличивается в два раза. При большой длине сети и большом количестве абонентов это оказывается невыгодным.

Поэтому код NRZ используется только для передачи короткими пакетами (обычно до 1 Кбита). Для синхронизации начала приема пакета используется стартовый служебный бит, чей уровень отличается от пассивного состояния линии связи (например, пассивное состояние линии при отсутствии передачи — 0, стартовый бит — 1). Наиболее известное применение кода NRZ — стандарт RS232-C, последовательный порт персонального компьютера. Передача информации в нем ведется байтами (8 бит), сопровождаемыми стартовым и стоповым битами.

Код RZ (Return to Zero — с возвратом к нулю) — этот трехуровневый код получил такое название потому, что после значащего уровня сигнала в первой половине передаваемого бита информации следует возврат к некоему «нулевому» уровню (например, к нулевому потенциалу). Переход к нему происходит в середине каждого бита. Логическому нулю, таким образом, соответствует положительный импульс, логической единице -отрицательный (или наоборот) в первой половине битового интервала.

Особенностью кода RZ является то, что в центре бита всегда есть переход (положительный или отрицательный), следовательно, из этого кода приемник может выделить синхроимпульс (строб). В данном случае возможна временная привязка не только к началу пакета, как в случае кода NRZ, но и к каждому отдельному биту, поэтому потери синхронизации не произойдет при любой длине пакета. Такие коды, несущие в себе строб, получили название самосинхронизирующихся.

Недостаток кода RZ состоит в том, что для него требуется вдвое большая полоса пропускания канала при той же скорости передачи по сравнению с NRZ (так как здесь на один бит приходится два изменения уровня напряжения). Например, для скорости передачи информации 10 Мбит/с требуется пропускная способность линии связи 10 МГц, а не 5 МГц, как при коде NRZ.

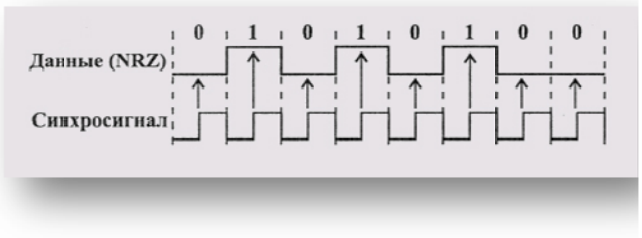


Рис. 2.12
Передача в коде NRZ с синхросигналом

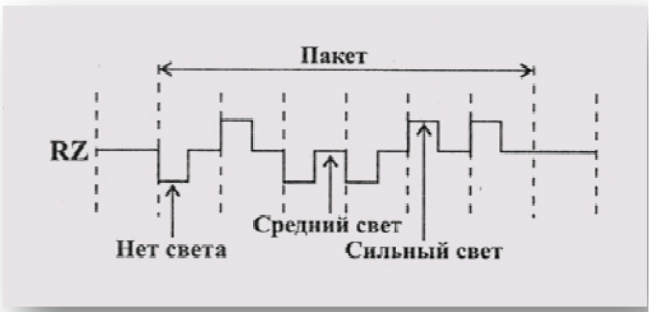


Рис. 2.13
Использование кода RZ в оптоволоконных сетях

Код RZ применяется не только в сетях на основе электрического кабеля, но и в оптоволоконных сетях. Поскольку в них не существует положительных и отрицательных уровней сигнала, используется три уровня: отсутствие света, «средний» свет, «сильный» свет. Это очень удобно: даже когда нет передачи информации, свет все равно присутствует, что позволяет легко определить целостность оптоволоконной линии связи без дополнительных мер (рис. 2.13).

Код Манчестер-П, или манчестерский код, получил наибольшее распространение в локальных сетях. Он также относится к самосинхронизирующимся кодам, но в отличие от кода RZ имеет не три, а всего только два уровня, что способствует его лучшей помехозащищенности. Логическому нулю соответствует положительный переход в центре бита (то есть первая половина битового интервала — низкий уровень, вторая половина — высокий), а логической единице соответствует отрицательный переход в центре бита (или наоборот).

Обязательное наличие перехода в центре бита позволяет приемнику кода Манчестер-П легко выделить из пришедшего сигнала синхросигнал, что дает возможность передавать информацию сколь угодно большими пакетами без потерь из-за рассинхронизации. Допустимое расхождение часов приемника и передатчика может достигать величины 25%. Как и в случае кода RZ, пропускная способность линии требуется в два раза выше, чем при использовании простейшего кода NRZ. Например, для скорости передачи 10 Мбит/с требуется полоса пропускания 10 МГц. Код Манчес-тер-П используется как в электрических кабелях, так и в оптоволоконных кабелях (в последнем случае один уровень соответствует отсутствию света, а другой — наличию света).

Большое достоинство манчестерского кода — отсутствие постоянной составляющей в сигнале (половину времени сигнал положительный, другую половину — отрицательный). Это дает возможность применять для гальванической развязки импульсные трансформаторы. При этом не требуется дополнительного источника питания для линии связи (как в случае использования оптронной развязки), резко уменьшается влияние низкочастотных помех, которые не проходят через трансформатор, легко решается проблема согласования. Если же один из уровней сигнала в манчестерском коде нулевой (как, например, в сети Ethernet), то величина постоянной составляющей в течение передачи будет равна примерно половине амплитуды сигнала. Это позволяет легко фиксировать столкновения пакетов в сети (конфликт, коллизию) по отклонению величины постоянной составляющей за установленные пределы.

Частотный спектр сигнала при манчестерском кодировании включает в себя только две частоты: при скорости передачи 10 Мбит/с это 10 МГц (соответствует передаваемой цепочке из одних нулей или из одних единиц) и 5 МГц (соответствует последовательности из чередующихся нулей и единиц: 1010101010 ...), поэтому с помощью простейших полосовых фильтров можно легко отфильтровать все другие частоты (помехи, наводки, шумы).

Так же как и в случае кода RZ, при манчестерском кодировании очень просто определить, идет передача или нет, то есть детектировать занятость сети или, как еще говорят, обнаруживать несущую частоту. Для этого достаточно контролировать, происходит ли изменение сигнала в течение битового интервала. Обнаружение несущей частоты необходимо, например, для определения момента начала и конца

принимаемого пакета, а также для предотвращения начала передачи в случае занятости сети (когда передает какой-то другой абонент).

Стандартный манчестерский код имеет несколько вариантов, один из которых показан на рис. 2.10. Данный код, в отличие от классического, не зависит от перемены мест двух проводов кабеля. Особенно это удобно в случае, когда для связи используется витая пара, провода которой легко перепутать. Именно этот код используется в одной из самых известных сетей Token-Ring фирмы IBM.

Принцип данного кода прост: в начале каждого битового интервала сигнал меняет уровень на противоположный предыдущему, а в середине единичных (и только единичных) битовых интервалов уровень изменяется еще раз. Таким образом, в начале битового интервала всегда есть переход, который используется для самосинхронизации. Как и в случае классического кода Манчестер-П, в частотном спектре при этом присутствует две частоты. При скорости 10 Мбит/с это частоты 10 МГц (при последовательности одних единиц: 11111111...) и 5 МГц (при последовательности одних нулей: 00000000...).

Здесь же стоит упомянуть о том, что часто совершенно неправомерно считается, что скорость передачи в бодах равняется скорости передачи в битах в секунду. Это верно только в случае кода NRZ. Скорость в бодах характеризует не количество передаваемых бит в секунду, а количество изменений уровня сигнала в секунду. При использовании кодов RZ или Манчестер-П требуемая скорость в бодах оказывается вдвое выше, чем при коде NRZ, поэтому логичнее измерять скорость передачи по сети не в бодах, а в битах в секунду (бит/с, Кбит/с, Мбит/с).

Все разрабатываемые в последнее время коды призваны найти компромисс между требуемой при заданной скорости передачи полосой пропускания кабеля и возможностью самосинхронизации. Разработчики стремятся сохранить самосинхронизацию, но не ценой двукратного увеличения полосы пропускания.

Чаще всего для этого в поток передаваемых битов добавляют биты синхронизации, например, один бит синхронизации на 4, 5 или 6 информационных битов или два бита синхронизации на 8 информационных битов. Правда, в действительности все обстоит несколько сложнее: кодирование не сводится к простой вставке в передаваемые данные дополнительных битов. Группы информационных битов преобразуются в передаваемые по сети группы с количеством битов на один или два больше. Приемник, естественно, осуществляет обратное преобразование, восстанавливает исходные информационные биты. Довольно просто осуществляется в этом случае и обнаружение несущей частоты (то есть детектирование передачи).

Так, в сети FDDI (скорость передачи 100 Мбит/с) применяется код 4B/5B, который 4 информационных бита преобразует в 5 передаваемых битов. При этом синхронизация приемника осуществляется один раз на 4 бита, а не в каждом бите, как в случае кода Манчестер-П. Требуемая полоса пропускания увеличивается по сравнению с кодом NRZ не в два раза, а только в 1,25 раза (то есть составляет не 100 МГц, а всего лишь 62,5 МГц). По тому же принципу строятся и другие коды, например 5B/6B, исполь зуемый в стандартной сети lOOVG-AnyLAN, или 8B/10B, используемый в сети Gigabit Ethernet.

В сегменте 100BASE-T4 сети Fast Ethernet применен несколько иной подход. Там используется код 8B/6T, предусматривающий параллельную передачу трех трехуровневых сигналов по трем витым парам. Это позволяет достичь скорости передачи 100 Мбит/с на дешевых кабелях с витыми парами категории 3, имеющих полосу пропускания всего лишь!6 МГц (см. табл. 2.1). Правда, это требует большего расхода кабеля и увеличения количества приемников и передатчиков. К тому же принципиально важно, чтобы все провода были одной длины, чтобы задержки сигнала в них не различались на заметную величину.

Подробнее эти коды будут рассмотрены в разделах книги, посвященных конкретным типам существующих сетей.

Все упомянутые коды предусматривают непосредственную передачу в сеть цифровых двух- или трехуровневых прямоугольных импульсов. Однако иногда в сетях используется и другой путь — модуляция информационными импульсами высокочастотного аналогового сигнала. Такое аналоговое кодирование позволяет при переходе на широкополосную передачу существенно увеличить пропускную способность канала связи. К тому же, как уже отмечалось, при прохождении по каналу связи аналогового сигнала (синусоидального) не искажается форма сигнала, а только уменьшается его амплитуда, а в случае цифрового сигнала еще и искажается форма сигнала (см. рис. 2.5).

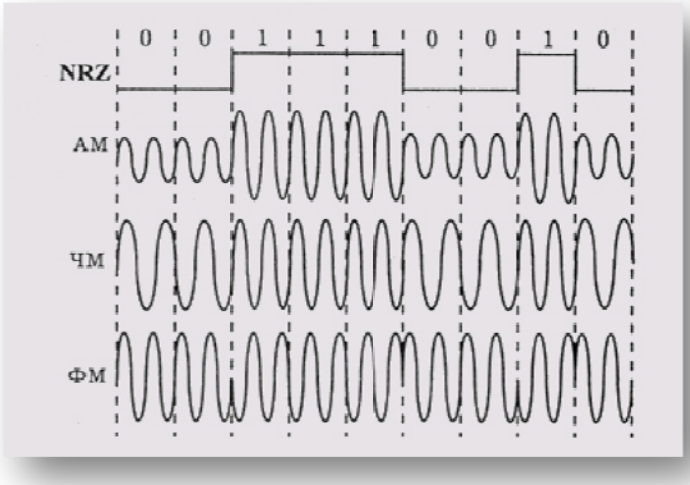


Рис. 2.14
Аналоговое кодирование цифровой информации

К самым простым видам аналогового кодирования относятся следующие (рис. 2.14):

- амплитудная модуляция (АМ), при которой логической единице соответствует наличие сигнала, а логическому нулю -его отсутствие (или сигнал меньшей амплитуды). Частота сигнала остается постоянной;
- частотная модуляция (ЧМ), при которой логической единице соответствует сигнал более высокой частоты, а логическому нулю — сигнал более низкой частоты (или наоборот). Амплитуда сигнала остается постоянной;
- фазовая модуляция (ФМ), при которой смене логического нуля на логическую единицу и логической единицы на логический нуль соответствует резкое изменение фазы синусоидального сигнала одной и той же частоты и амплитуды.

Чаще всего аналоговое кодирование используется при передаче информации по каналу с узкой полосой пропускания, например по телефонным линиям в глобальных сетях. В локальных сетях оно применяется редко из-за высокой сложности и стоимости как кодирующего, так и декодирующего оборудования.

Глава 3. Пакеты, протоколы и методы управления обменом

Содержание третьей главы:

3.1. Назначение пакетов и их структура

Информация в локальных сетях, как правило, передается отдельными порциями, кусками, называемыми в различных источниках пакетами, кадрами или блоками. Использование пакетов связано с тем, что в сети, как правило, одновременно может происходить несколько сеансов связи (во всяком случае, при топологиях «шина» и «кольцо»), то есть в течение одного и того же интервала времени могут идти два или больше процессов передачи данных между различными парами абонентов. Пакеты как раз и позволяют разделить во времени сеть между передающими информацию абонентами.

Если бы вся требуемая информация передавалась сразу, непрерывно, без разделения на пакеты, то это привело бы к монопольному захвату сети одним из абонентов на довольно продолжительное время. Все остальные абоненты вынуждены были бы ждать окончания передачи всей информации, что в ряде случаев могло бы потребовать десятков секунд и даже минут (например, при копировании содержимого целого жесткого диска). Чтобы уравнять в правах всех абонентов, а также примерно уравнять время доступа к сети и интегральную скорость передачи информации для всех абонентов, как раз и используются пакеты (кадры). Длина пакета зависит от типа сети, но обычно она составляет от нескольких десятков байт до нескольких килобайт.

Важно также и то, что при передаче больших массивов информации становится довольно высокой вероятность ошибки из-за помех и сбоев. Например, при характерной для локальных сетей величине вероятности одиночной ошибки в 10~8 пакет длиной 10 Кбит будет искажен с вероятностью 10~4, а массив длиной 10 Мбит — с вероятностью 10"1. К тому же обнаружить ошибку в массиве из нескольких мегабайт намного сложнее, чем в пакете из нескольких килобайт. При обнаружении ошибки придется повторить передачу всего массива, что гораздо сложнее, чем повторно передать небольшой пакет. Но при повторной передаче большого массива снова высока вероятность ошибки, и процесс этот при слишком большом массиве может повторяться до бесконечности.

С другой стороны, пакеты имеют преимущества и перед побайтовой (8 бит) или пословной (16 бит или 32 бита) передачей информации, так как увеличивается полезная загрузка сети за счет уменьшения требуемого количества служебной информации. Это же относится и к маленьким пакетам длиной в несколько байт. Ведь каждый передаваемый по сети пакет обязательно содержит в себе биты, относящиеся непосредственно к обмену по сети (стартовые биты, биты адресации, биты типа и номера пакета и т.д.). При маленьких пакетах доля этой служебной информации будет непозволительно высокой, что приведет к снижению интегральной (средней) скорости обмена информацией между абонентами сети.

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

Структура пакета определяется прежде всего аппаратурными особенностями данной сети, выбранной топологией и типом среды передачи информации, а также существенно зависит от используемого протокола (порядка обмена информацией). Строго говоря, в каждой сети структура пакета индивидуальна. Но существуют некоторые общие принципы формирования пакета, определяемые характерными особенностями обмена информацией по любым локальным сетям.

Чаще всего пакет содержит в себе следующие основные поля или части (рис. 3.1).

Стартовая комбинация, или преамбула, которая обеспечивает настройку аппаратуры адаптера или другого сетевого устройства на прием и обработку пакета. Это поле может отсутствовать или сводиться к одному-единственному стартовому биту.

Сетевой адрес (идентификатор) принимающего абонента, то есть 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.

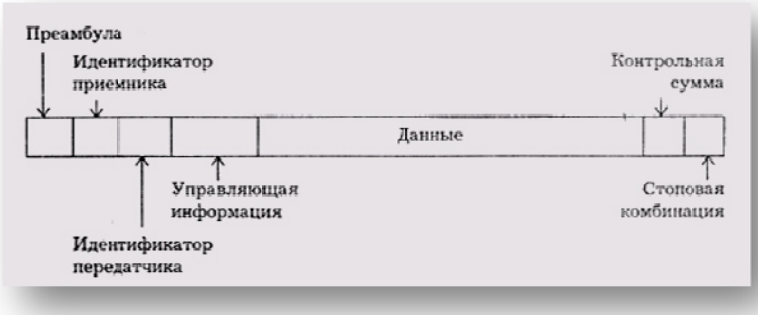


Рис. 3.1
Типичная структура пакета

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

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

Данные — та информация, ради передачи которой используется данный пакет. Правда, существуют специальные управляющие пакеты, которые не имеют поля данных. Их можно рассматривать как сетевые команды. Пакеты, включающие поле данных, называются информационными пакетами. Управляющие пакеты могут выполнять функцию начала сеанса связи, 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.

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

Нередко в структуре пакета выделяют всего три поля:

- Начальное управляющее поле пакета (или заголовок пакета), то есть поле, включающее в себя стартовую комбинацию, сетевые адреса приемника и передатчика, а также служебную информацию.
- Поле данных пакета.
- Конечное управляющее поле пакета (или заключение, трейлер), включающее в себя контрольную сумму и стоповую комбинацию, а также, возможно, служебную информацию.

Помимо термина «пакет» в литературе также используется термин «кадр». Иногда под этими терминами имеется в виду одно и то же, но иногда подразумевается, что кадр вложен в пакет. В этом случае все перечисленные поля кадра, кроме преамбулы и стоповой комбинации, относятся к кадру. В пакет может также входить признак начала кадра (в конце преамбулы). Такая терминология принята, например, в сети Ethernet. Но надо всегда помнить, что физически по сети передается все-таки не кадр, а пакет (если, конечно, различать два эти понятия), и именно передача пакета, а не передача кадра, соответствует занятости 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. Пример простейшего протокола показан на рис. 3.2. В данном случае сеанс связи начинается с запроса готовности приемника принять данные. В случае, когда приемник готов, он посылает в ответ управляющий пакет «Готовность». Если приемник не готов, он отказывается от сеанса другим управляющим пакетом. Затем начинается собственно передача данных. При этом на каждый полученный пакет данных приемник отвечает пакетом подтверждения. В случае, когда пакет передан с ошибками, приемник запрашивает повторную передачу. Заканчивается сеанс управляющим пакетом, 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).

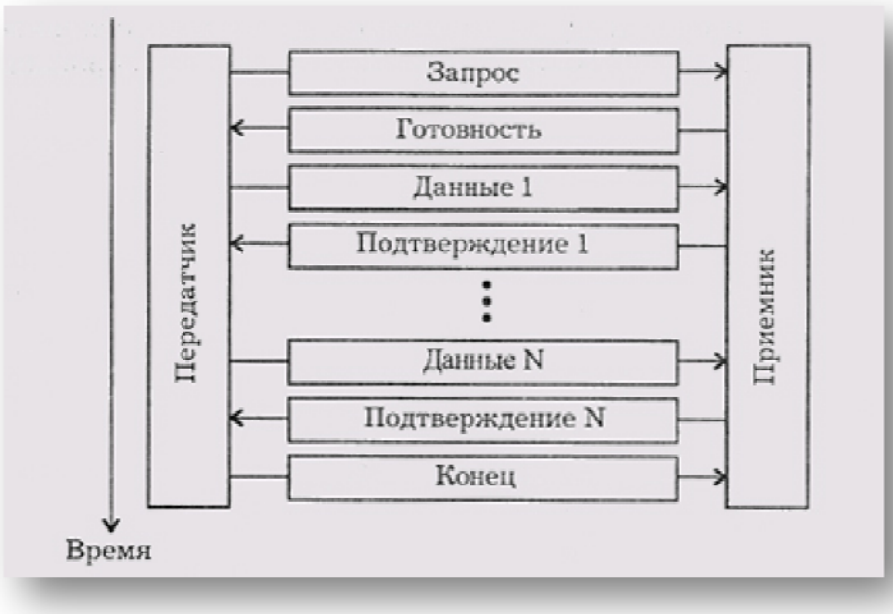


Рис. 3.2
Пример обмена пакетами при сеансе связи

При реальном обмене по сети используются многоуровневые протоколы, каждый из которых предполагает свою структуру кадра (свою адресацию, свою управляющую информацию, свой формат данных и т.д.). Ведь протоколы высоких уровней имеют дело с такими понятиями, как файл-сервер или приложение, запрашивающее данные у другого приложения, и вполне могут не иметь представления ни о типе аппаратуры сети, ни о методе управления обменом. Все кадры более высоких уровней последовательно вкладываются в передаваемый пакет, точнее, в поле данных передаваемого пакета (рис. 3.3). Каждый следующий вкладываемый кадр может содержать свою собственную служебную информацию, располагающуюся как до данных (заголовок), так и после данных (трейлер), причем ее назначение может быть самым различным. Естественно, доля вспомогательной информации в пакетах при этом возрастает с каждым следующим уровнем, что снижает эффективную скорость передачи данных. Поэтому для увеличения этой скорости лучше, чтобы протоколы обмена были как можно проще, и чтобы уровней этих протоколов было как можно меньше. Иначе никакая скорость передачи битов не поможет, и быстрая сеть может передавать, к примеру, какой-нибудь файл дольше, чем медленная сеть, которая пользуется более простым протоколом.

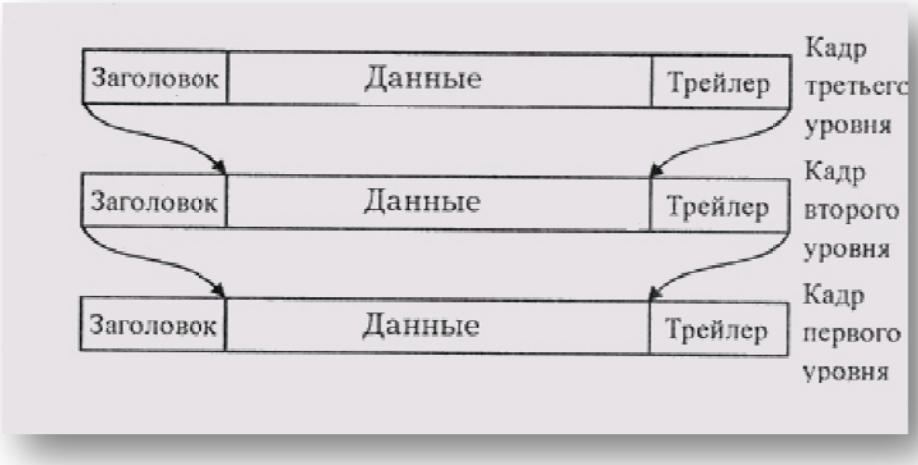


Рис. 3.3
Многоуровневая система вложения кадров

3.2. Адресация пакетов

Каждый абонент (узел) локальной сети должен иметь свой уникальный адрес (он же идентификатор, MAC-адрес), чтобы ему можно было адресовать пакеты. Существуют две основные системы присвоения адресов абонентам сети (точнее, сетевым адаптерам этих абонентов).

Первая система элементарно проста. Она сводится к тому, что при установке сети каждому абоненту присваивается свой адрес (программно или с помощью переключателей на плате адаптера). При этом требуемое количество разрядов адреса определяется из простого уравнения:

2n>Nmax,

- где п — количество разрядов адреса, а Nmax — максимально возможное количество абонентов в сети. Например, восьми разрядов адреса достаточно для сети из 255 абонентов. Один адрес (обычно 1111....11) отводится для широковещательной передачи, то есть используется для пакетов, адресованных всем абонентам одновременно. Именно этот подход использо
- ван в такой известной сети, как Arcnet. Достоинства данного подхода -простота и малый объем служебной информации в пакете, а также простота аппаратуры адаптера, распознающей адрес пакета. Недостаток -трудоемкость задания адресов и возможность ошибки (например, двум абонентам сети может быть присвоен один и тот же адрес).

Второй подход к адресации был разработан международной организацией IEEE, занимающейся стандартизацией сетей. Именно он используется в большинстве сетей и рекомендован для всех новых разработок. Идея 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 не будет абонентов с одинаковыми адресами. Был выбран 48-битный формат адреса, что соответствует примерно 280 триллионам различных адресов. Понятно, что столько сетевых.адаптеров никогда не будет выпущено.

Чтобы распределить возможные диапазоны адресов между многочисленными изготовителями сетевых адаптеров, была предложена следующая структура адреса:

Младшие 24 разряда кода адреса называются OUA (Organizationally Unique Address) — организационно уникальный адрес. Именно их присваивает производитель сетевого адаптера. Всего возможно свыше 16 миллионов комбинаций.

Следующие 22 разряда кода называются OUI (Organizationally Unique Identifier) — организационно уникальный идентификатор. IEEE присваивает один или несколько ОШ каждому производителю сетевых адаптеров. Это позволяет исключить совпадения адресов адаптеров от разных производителей. Всего возможно свыше 4 миллионов разных OUI. Вместе OUA и OUI называются UAA (Universally Administered Address) — универсально управляемый адрес или IEEE-адрес.

Два старших разряда адреса являются управляющими и определяют тип адреса, способ интерпретации остальных 46 разрядов. Старший бит I/G (Individual/Group) определяет, индивидуальный это адрес или групповой. Если он установлен в 0, то мы имеем дело с индивидуальным адресом, если установлен в 1, то с групповым (многопунктовым или функциональным) адресом. Пакеты с групповым адресом получают все имеющие его сетевые адаптеры, причем групповой адрес определяется всеми 46 младшими разрядами. Второй управляющий бит U/L (Universal/Local) называется флажком универсального/местного управления и определяет, как был присвоен адрес данному сетевому адаптеру. Обычно он установлен в 0. Установка бита U/L в 1 означает, что адрес задан не производителем сетевого адаптера, а организацией, использующей данную сеть. Это довольно редкая ситуация.

Для широковещательной передачи используется специально выделенный сетевой адрес, все 48 битов которого установлены в единицу. Его принимают все абоненты сети независимо от их индивидуальных и групповых адресов.

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

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

3.3. Методы управления обменом

Сеть всегда объединяет несколько абонентов, каждый из которых имеет право передавать свои пакеты. Но по одному кабелю не может одновременно передаваться два пакета, иначе возможен конфликт (коллизия), что приведет к искажению и потере обоих пакетов. Значит, надо каким-то образом установить

очередность доступа к сети (захвата сети) всеми абонентами, желающими передавать. Это относится прежде всего к сетям с топологиями «шина» и «кольцо». Точно так же при топологии «звезда» необходимо установить очередность передачи пакетов периферийными абонентами, иначе центральный абонент просто не сможет справиться с их обработкой.

Поэтому в любой сети применяется тот или иной метод управления обменом (он же метод доступа, он же метод арбитража), разрешающий или предотвращающий конфликты между абонентами. От эффективности выбранного метода зависит очень многое: скорость обмена информацией между компьютерами, нагрузочная способность сети, время реакции сети на внешние события и т.д. Метод управления — это один из важнейших параметров сети. Тип метода управления обменом во многом определяется особенностями топологии сети, но в то же время он и не привязан жестко к топологии.

Методы управления обменом делятся на две группы:

Централизованные методы, при которых все управление сосредоточенно в одном месте. Недостатки таких методов: неустойчивость к отказам центра, малая гибкость управления. Достоинство — отсутствие конфликтов.

Децентрализованные методы, при которых отсутствует центр управления. Главные достоинства таких методов: высокая устойчивость к отказам и большая гибкость. Однако возможны конфликты, которые надо разрешать.

Существует и другое деление методов управления обменом, относящееся, главным образом, к децентрализованным методам:

- Детерминированные методы определяют четкие правила, по которым чередуются захватывающие сеть абоненты. Абоненты имеют ту или иную систему приоритетов, причем приоритеты эти различны для всех абонентов. При этом, как правило, конфликты полностью исключены (или маловероятны), но некоторые абоненты могут дожидаться своей очереди слишком долго. К детерминированным методам относится, например, маркерный доступ, при котором право передачи передается по эстафете от абонента к абоненту.
- Случайные методы подразумевают случайное чередование передающих абонентов. В этом случае возможность конфликтов подразумевается, но предлагаются способы их разрешения. Случайные методы работают хуже, чем детерминированные, при больших информационных потоках в сети (при большом трафике сети) и не гарантируют абоненту величину времени доступа (это интервал между возникновением желания передавать и получением возможности передать свой пакет). Пример случайного метода — CSMA/CD.

Рассмотрим три наиболее типичных метода управления обменом, характерных для трех основных топологий.

3.3.1. Управление обменом в сети с топологией «звезда»

Для топологии «звезда» наиболее органично подходит централизованный метод управления, причем в данном случае не слишком важно, что находится в центре звезды: компьютер (центральный абонент), как на рис. 1.2, или же специальный концентратор, управляющий обменом, но сам не участвующий в нем (рис. 1.5). Именно эта вторая ситуация реализована в сети 100VGAnyLAN.

Самый простой централизованный метод состоит в следующем.

Абоненты, желающие передать свой пакет (или, как еще говорят, имеющие заявки на передачу), посылают центру свои запросы. Центр же предоставляет им право передачи пакета в порядке очередности, например, по их физическому расположению по часовой стрелке. После окончания передачи пакета каким-то абонентом право передавать получит следующий по порядку (по часовой стрелке) абонент, имеющий заявку на передачу (рис. 3.5).

В этом случае говорят, что абоненты имеют географические приоритеты (по их физическому расположению). В каждый конкретный момент наивысшим приоритетом обладает следующий по порядку абонент, но в пределах полного цикла опроса ни один из абонентов не имеет никаких преимуществ перед другими. Никому не придется ждать своей очереди слишком долго. Максимальная величина времени доступа для любого абонента в этом случае будет равна суммарному времени передачи пакетов всех абонентов сети, кроме данного. Для топологии, показанной на рис. 3.5, она составит четыре длительности пакета. Никаких столкновений пакетов при данном методе быть не может в принципе, так как все решения о доступе принимаются в одном месте.

Возможен и другой принцип реализации централизованного управления.

В этом случае центр посылает запросы (управляющие пакеты) по очереди всем периферийным абонентам. Тот периферийный абонент, который хочет передавать (первый из опрошенных) посылает ответ (или же сразу начинает передачу). В дальнейшем сеанс обмена проводится именно с ним. После окончания

этого сеанса центральный абонент продолжает опрос периферийных абонентов по кругу. Если же хочет передать центральный абонент, он передает без всякой очереди тому, кому хочет.

Как в первом, так и во втором случае никаких конфликтов быть не может (все решения принимает единый центр, которому не с кем конфликтовать). Если все абоненты очень активны и заявки на передачу поступают интенсивно, то все они будут передавать строго по очереди. Но центр должен быть исключительно надежен, иначе будет парализован весь обмен. Механизм управления не слишком гибок, так как центр работает по жестко заданному алгоритму. К тому же скорость управления невысока. Ведь даже в случае, когда все время передает только один абонент, ему все равно приходится ждать после каждого переданного пакета, пока центр опросит всех остальных абонентов.

3.3.2. Управление обменом в сети с топологией «шина»

Рис. 3.5
Централизованный метод управления обменом в сети с топологией «звезда»

В принципе при топологии «шина» возможно точно такое же централизованное управление, как и в случае звезды. При этом один из абонентов («центральный») посылает всем остальным («периферийным») запросы, выясняя, кто из них хочет передать, затем разрешает передачу одному из абонентов. После окончания передачи передававший абонент сообщает «центру», что он закончил передачу, и «центр» снова начинает опрос (рис. 3.6).

Все преимущества и недостатки такого управления — те же самые, что и в случае звезды. Единственное отличие состоит в том, что центр здесь не пересылает информацию от одного абонента к другому, как в топологии «активная звезда», а только управляет обменом.

Однако гораздо чаще в шине используется децентрализованное случайное управление, так как все сетевые адаптеры всех абонентов в данном случае одинаковы. При выборе децентрализованного управления все абоненты также имеют равные права доступа к сети, то есть особенности топологии совпадают с особенностями метода управления. Решение о том, когда можно передавать свой пакет, принимается каждым абонентом на месте, исходя только из анализа состояния сети. В данном случае существует конкуренция между абонентами за захват сети и, следовательно, возможны конфликты между ними и искажения передаваемых данных из-за наложения пакетов.

Рис. 3.6
Централизованное управление в сети с топологией «шина»

Существует множество алгоритмов доступа или, как еще говорят, сценариев доступа, порой очень сложных. Их выбор зависит от скорости передачи в сети, от длины шины, загруженности сети (интенсивности

обмена или трафика сети), от используемого кода передачи. Отметим, что иногда для управления доступом к шине используется дополнительная линия связи, что упрощает аппаратуру контроллеров и методы доступа, но обычно заметно увеличивает стоимость сети в целом за счет удвоения длины кабеля и количества приемопередатчиков. Поэтому данное решение не получило широкого распространения.

Суть всех случайных методов управления обменом довольно проста. Пока сеть занята, то есть по ней идет передача пакета, абонент, желающий передавать, ждет освобождения сети. Ведь в противном случае неминуемо исказятся и пропадут оба пакета. После освобождения сети абонент, желающий передавать, начинает свою передачу. Если одновременно с ним начали передачу еще несколько абонентов, то возникает коллизия (конфликт, столкновение пакетов). Конфликт этот детектируется всеми абонентами, передача прекращается, и через некоторое время предпринимается повторная попытка передачи. При этом не исключены повторные коллизии и новые попытки передать свой пакет. И так продолжается до тех пор, пока пакет не будет передан без коллизий.

Существует несколько разновидностей случайных методов управления обменом. В некоторых из них не все передающие абоненты распознают коллизию, а только те, которые имеют меньшие приоритеты. Абонент с максимальным приоритетом из всех, начавших передачу, закончит передачу своего пакета без ошибок. В некоторых случайных методах управления обменом каждый абонент начинает свою передачу после освобождения сети не сразу, а выдержав свою, строго индивидуальную задержку. Максимальным приоритетом будет обладать абонент с минимальной задержкой. Но хотя в обоих случаях имеется система приоритетов, методы все-таки относятся к случайным, так как исход конкуренции невозможно предсказать.

Чаще всего система приоритетов отсутствует полностью, и после обнаружения коллизии абоненты выбирают задержку до следующей попытки передачи по случайному закону. Именно так работает стандартный метод управления обменом CSM A/CD (Carrier Sense Multiple Access with Collision Detection), используемый в самой популярной сети Ethernet. Его главное достоинство в том, что все абоненты полностью равноправны, и ни один из них не может надолго заблокировать обмен другому (как в случае наличия приоритетов). Подробнее метод CSMA/CD будет рассмотрен в специальной главе.

Понятно, что все подобные методы будут хорошо работать только при не слишком большой интенсивности обмена по сети. Считается, что приемлемое качество связи обеспечивается только при нагрузке не выше 30-40% (то есть сеть занята не более 30-40% всего времени). При большей нагрузке становятся слишком частыми повторные столкновения, и наступает так называемый коллапс, или крах сети, представляющий собой резкое падение ее производительности. Недостаток всех подобных методов еще и в том, что они не гарантируют величину времени доступа к сети, которая зависит не только от выбора задержки между попытками передачи, но и от общей загруженности сети. Поэтому, например, в сетях, выполняющих задачи управления оборудованием (на производстве, в научных лабораториях), где требуется быстрая реакция на внешние события, сети со случайными методами управления используются довольно редко.

При любом случайном методе управления обменом возникает вопрос о том, какой должна быть минимальная длительность пакета, чтобы коллизию обнаружили все начавшие передавать абоненты. Ведь сигнал по любой физической среде распространяется не мгновенно, и при больших размерах сети (как еще говорят, при большом диаметре сети) задержка распространения может составлять десятки и сотни микросекунд, и информацию об одновременно происходящих событиях разные абоненты получают не одновременно. Чтобы ответить на этот вопрос, обратимся к рис. 3.7.

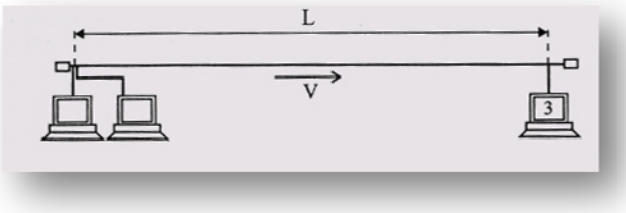


Рис. 3.7
Расчет минимальной длительности пакета

Пусть L — полная длина сети, V — скорость распространения сигнала в используемом кабеле. Допустим, абонент 1 закончил свою передачу, а абоненты 2 и 3 захотели передавать во время передачи абонента 1. После освобождения сети абонент 3 узнает об этом событии и .начинает свою передачу через временной интервал прохождения сигнала по всей длине сети, то есть через время L/V, а абонент 2 начнет передавать сразу после освобождения сети. Пакет от абонента 3 дойдет до абонента 2 еще через временной интервал L/V после начала передачи абонентом 3 (обратный путь сигнала). К этому моменту передача пакета абонентом 2 ни в коем случае не должна еще закончиться, иначе абонент 2 так и не узнает о столкновении пакетов (о коллизии).

Поэтому получается, что минимально допустимая длительность пакета в сети должна составлять 2L/V, то есть должна равняться удвоенному времени распространения сигнала по полной длине сети (или по пути наибольшей длины в сети). Это время называется двойным или круговым временем задержки сигнала в сети, или PDV (Path Delay Value). Отметим, что этот же временной интервал можно рассматривать как универсальную меру одновременности любых событий в сети.

Отдельно стоит остановиться на том, как сетевые адаптеры распознают коллизию, то есть столкновение пакетов. Ведь простое сравнение передаваемой абонентом информации с той, которая реально присутствует в сети, возможно только в случае самого простого кода NRZ, используемого довольно редко. При применении кода Манчестер-П, который обычно подразумевается в случае метода управления обменом CSMA/CD, требуется принципиально другой подход.

Как уже отмечалось, сигнал в коде Манчестер-П всегда имеет постоянную составляющую, равную половине размаха сигнала (если один из двух уровней сигнала нулевой). Однако в случае столкновения двух и более пакетов (коллизии) это правило выполняться не будет. Постоянная составляющая суммарного сигнала в сети будет обязательно больше или меньше половины размаха (рис. 3.8). Ведь пакеты всегда отличаются друг от друга и к тому же сдвинуты друг относительно друга во времени. Именно по выходу уровня постоянной составляющей за установленные пределы и определяет каждый сетевой адаптер наличие коллизии в сети.

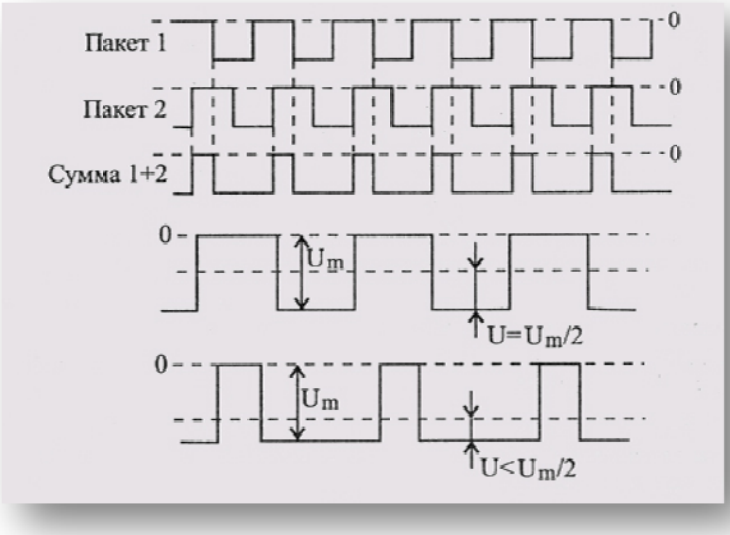


Рис. 3.8
Определение факта коллизии при использовании кода Манчестер-II

3.3.3. Управление обменом в сети с топологией кольцо

Кольцевая топология имеет свои особенности при выборе метода управления обменом. В этом случае важно то, что любой пакет, посланный по кольцу, последовательно пройдя всех абонентов, через некоторое время возвратится в ту же точку, к тому же абоненту (так как топология замкнутая), то есть нет одновременного распространения сигнала в две стороны, как в топологии «шина». Отметим, что сети с топологией «кольцо» бывают однонаправленными и двунаправленными. Мы будем здесь рассматривать только однонаправленные, как более распространенные.

(СМ-свободный маркер, ЗМ— занятый маркер, МП— занятый маркер с подтверждением, ПД— пакет данных)

В принципе, в сети с топологией «кольцо» можно использовать различные централизованные методы управления (как в звезде), можно применять также методы случайного доступа (как в шине), но чаще выбирают все-таки специфические методы управления, в наибольшей степени соответствующие именно особенностям кольца. Наиболее популярны в этом случае маркерные (эстафетные) методы управления, то есть те, которые используют маркер (эстафету) — небольшой управляющий пакет специального вида. Именно эстафетная передача маркера по кольцу позволяет передавать право на захват сети от одного абонента к другому. Маркерные методы относятся к децентрализованным и детерминированным методам управления обменом в сети. В них нет явно выраженного центра, но существует четкая система приоритетов, и потому не бывает конфликтов.

Рассмотрим работу маркерного метода управления в сети с топологией кольцо (рис. 3.9).

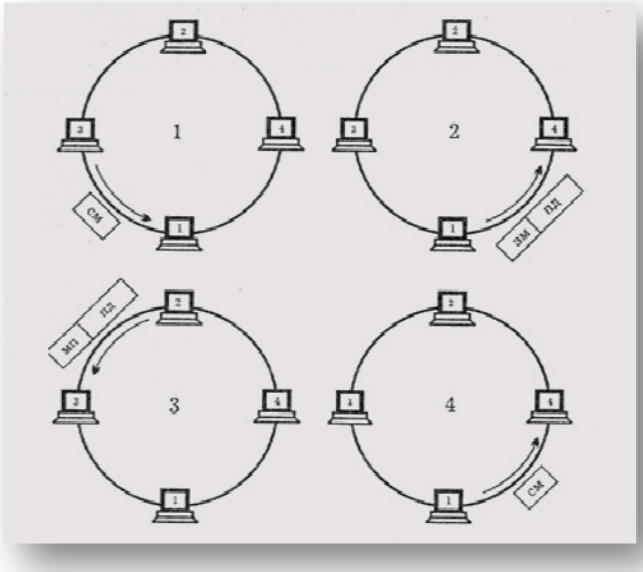


Рис. 3.9
Маркерный метод управления обменом

По кольцу непрерывно ходит специальный пакет, маркер, предоставляющий абонентам право передавать свой пакет. Алгоритм действий абонентов включает в себя следующее:

Абонент 1, желающий передать свой пакет, должен дождаться прихода к нему свободного маркера. Затем он присоединяет к маркеру свой пакет, помечает маркер как занятый и отправляет эту посылку следующему по кольцу абоненту.

Все остальные абоненты (2, 3, 4), получив маркер с присоединенным пакетом, проверяют, им ли адресован пакет. Если пакет адресован не им, то они передают полученную посылку (маркер + пакет) дальше по кольцу.

Если какой-то абонент (в нашем случае это будет абонент 3) распознает пакет как адресованный ему, то он принимает этот пакет, устанавливает в маркере бит подтверждения приема и передает посылку (маркер + пакет) дальше по кольцу.

Передававший абонент 1 получает свою посылку, прошедшую по всему кольцу, обратно, помечает маркер как свободный, удаляет из сети свой пакет и посылает свободный маркер дальше по кольцу. Абонент, желающий передавать, ждет этого маркера, и все повторяется снова.

Приоритет при данном методе управления получается географический, то есть право передачи после освобождения сети переходит к следующе- „ му по направлению кольца абоненту от последнего передававшего абонента. Но эта система приоритетов работает только при большой интенсивности обмена. При малой интенсивности обмена все абоненты равноправны, и время доступа к сети каждого из них определяется только положением маркера в момент возникновения заявки на передачу.

В чем-то рассматриваемый метод похож на метод опроса (централизованный), хотя явно выделенного центра здесь не существует. Однако некоторый центр обычно все-таки должен присутствовать: один из абонентов (или специальное устройство) должен следить, чтобы маркер не потерялся в процессе прохождения по кольцу (например, из-за действия помех или сбоя в работе какого-то абонента). В противном случае механизм доступа работать не будет. Следовательно, надежность управления в данном случае снижается (выход центра из строя приводит к полной дезорганизации обмена), поэтому обычно применяются специальные средства для повышения надежности, восстановления центра контроля за маркером.

Основное преимущество данного метода перед CSMA/CD состоит в том, что здесь гарантирована величина времени доступа. Его величина составит (N — 1) t , где N — полное число абонентов в сети, tnK — время прохождения пакета по кольцу. Вообще маркерный метод управления обменом гораздо эффективнее случайных методов при большой интенсивности обмена в сети (при загруженности более 30-40%). Он позволяет сети работать с большей нагрузкой, которая теоретически может приближаться к 100%.

Метод маркерного доступа может использоваться не только в кольце (например, в сети IBM Token Ring или FDDI), но и в шине (например, сеть Arcnet-BUS), и в пассивной звезде (например, сеть Arcnet-STAR). В этих случаях реализуется не физическое, а логическое кольцо, то есть все абоненты последовательно передают друг другу маркер, и эта цепочка передачи маркеров замкнута в кольцо. При этом совмещаются достоинства физической топологии «шина» и маркерного метода управления.

Глава 4. Уровни сетевой архитектуры

Содержание Четвёртой главы:

4.1. Эталонная модель OSI

При связи компьютеров по сети производится множество операций, обеспечивающих передачу данных от компьютера к компьютеру. Пользователю, работающему с каким-то приложением, в общем-то безразлично, что и как при этом происходит. Для него просто существует доступ к другому приложению или компьютерному ресурсу, расположенному на другом компьютере сети. В действительности же вся передаваемая информация проходит много этапов обработки. Прежде всего она разбивается на блоки, каждый из которых снабжается управляющей информацией. Полученные блоки оформляются в виде сетевых пакетов, эти пакеты кодируются, передаются с помощью электрических или световых сигналов по сети в соответствии с выбранным методом доступа, затем из принятых пакетов вновь восстанавливаются заключенные в них блоки данных, блоки соединяются в данные, которые и становятся доступны другому приложению. Это, конечно, очень упрощенное описание происходящих процессов. Часть из указанных процедур реализуется только программно, другая — аппаратно, а какие-то операции могут выполняться как программами, так и аппаратурой.

Упорядочить все выполняемые процедуры, разделить их на уровни и подуровни, взаимодействующие между собой, как раз и призваны модели сетей. Эти модели позволяют правильно организовать взаимодействие как абонентам внутри одной сети, так и самым разным сетям на различных уровнях. Наибольшее распространение получила в настоящее время так называемая эталонная модель обмена информацией открытой системы OSI (Open System Interchange). Под термином «открытая система» в данном случае понимается незамкнутая в себе система, имеющая возможность взаимодействия с какими-то другими системами (в отличие от закрытой системы).

Модель OSI была предложена Международной организацией стандартов ISO (International Standards Organization) в 1984 году. С тех пор ее используют (более или менее строго) все производители сетевых продуктов. Как и любая универсальная модель, модель OSI довольно громоздка, избыточна и не слишком гибка, поэтому реальные сетевые средства, предлагаемые различными фирмами, не обязательно придерживаются принятого разделения функций. Однако знакомство с моделью OSI позволяет лучше понять, что же происходит в сети.

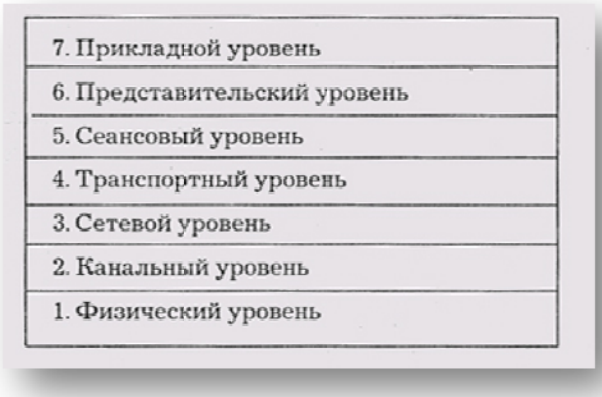


Рис. 4.1
Семь уровней модели OSI

Все сетевые функции в модели разделены на 7 уровней (рис. 4.1). При этом вышестоящие уровни выполняют более сложные, глобальные задачи, для чего используют в своих целях нижестоящие уровни, а также управляют ими. Цель нижестоящего уровня — предоставление услуг вышестоящему уровню, причем вышестоящему уровню не важны детали выполнения этих услуг. Нижестоящие уровни выполняют более

простые, более конкретные функции. В идеале каждый уровень взаимодействует только с теми, которые находятся рядом с ним (выше него и ниже него). Верхний уровень соответствует прикладной задаче, работающему в данный момент приложению, нижний — непосредственной передаче сигналов по каналу связи.

Функции, входящие в показанные на рис 4.1 уровни, реализуются каждым абонентом сети. При этом каждый уровень на одном абоненте работает так, как будто он имеет прямую связь с соответствующим уровнем другого абонента, то есть между одноименными уровнями абонентов сети существует виртуальная связь. Реальную же связь абоненты одной сети имеют только на самом нижнем, первом, физическом уровне. В передающем абоненте информация проходит все уровни, начиная с верхнего и заканчивая нижним. В принимающем абоненте полученная информация совершает обратный путь: от нижнего уровня к верхнему (рис. 4.2).

Рис. 4.2

Путь информации от абонента к абоненту Рассмотрим подробнее функции разных уровней.

Прикладной уровень (Application), или уровень приложений, обеспечивает услуги, непосредственно поддерживающие приложения пользователя, например программные средства передачи файлов, доступа к базам данных, средства электронной почты, службу регистрации на сервере. Этот уровень управляет остальными шестью уровнями.

Представительский уровень (Presentation), или уровень представления данных, определяет и преобразует форматы данных и их синтаксис в форму, удобную для сети, то есть выполняет функцию переводчика. Здесь же выполняется шифрование и дешифрирование данных, а при необходимости — их сжатие.

Сеансовый уровень (Session) управляет проведением сеансов связи (то есть устанавливает, поддерживает и прекращает связь). Этот же уровень распознает логические имена абонентов, контролирует предоставленные им права доступа.

Транспортный уровень (Transport) обеспечивает доставку пакетов без ошибок и потерь, в нужной последовательности. Здесь же производится разбивка передаваемых данных на блоки, помещаемые в пакеты, и восстановление принимаемых данных.

Сетевой уровень (Network) отвечает за адресацию пакетов и перевод логических имен в физические сетевые адреса (и обратно), а также за выбор маршрута, по которому пакет доставляется по назначению (если в сети имеется несколько маршрутов).

Канальный уровень, или уровень управления линией передачи (Data link), отвечает за формирование пакетов стандартного вида, включающих начальное и конечное управляющие поля. Здесь же производится управление доступом к сети, обнаруживаются ошибки передачи" и производится повторная пересылка приемнику ошибочных пакетов.

Физический уровень (Physical) — это самый нижний уровень модели, который отвечает за кодирование передаваемой информации в уровни сигналов, принятые в среде передачи, и обратное декодирование. Здесь же определяются требования к соединителям, разъемам, электрическому согласованию, заземлению, защите от помех и т.д.

Большинство функций двух нижних уровней модели (1 и 2) обычно реализуются аппаратно (часть функций уровня 2 — программным драйвером сетевого адаптера). Именно на этих уровнях определяется скорость передачи и топология сети, метод управления обменом и формат пакета, то есть то, что имеет

непосредственное отношение к типу сети (Ethernet, Token-Ring, FDDI). Более высокие уровни не работают напрямую с конкретной аппаратурой, хотя уровни 3,4 и 5 еще могут учитывать ее особенности. Уровни 6 и 7 вообще не имеют к аппаратуре никакого отношения. Замены аппаратуры сети на другую они просто не заметят.

В уровне 2 (канальном) нередко выделяют два подуровня.

Верхний подуровень (LLC — Logical Link Control) осуществляет управление логической связью, то есть устанавливает виртуальный канал связи (часть его функций выполняется программой драйвера сетевого адаптера).

Нижний подуровень (MAC — Media Access Control) осуществляет непосредственный доступ к среде передачи информации (каналу связи). Он напрямую связан с аппаратурой сети.

Помимо модели OSI, существует также модель IEEE Project 802, принятая в феврале 1980 года (отсюда и число 802 в названии), которую можно рассматривать как модификацию, развитие, уточнение модели OSI. Стандарты, определяемые этой моделью (так называемые 802-спецификации), делятся на двенадцать категорий, каждой из которых присвоен свой номер.

802.1 — объединение сетей.

802.2 — управление логической связью.

802.3 — локальная сеть с методом доступа CSMA/CD и топологией «шина» (Ethernet).

802.4 — локальная сеть с топологией «шина» и маркерным доступом.

802.5 — локальная сеть с топологией «кольцо» и маркерным доступом.

802.6 — городская сеть (Metropolitan Area Network, MAN).

802.7 — широковещательная технология.

802.8 — оптоволоконная технология.

802.9 — интегрированные сети с возможностью передачи речи и данных.

802.10 — безопасность сетей.

802.11 — беспроводная сеть.

802.12 — локальная сеть с централизованным управлением доступом по приоритетам запросов и топологией «звезда» (lOOVG-AnyLAN).

Стандарты 802.3, 802.4, 802.5, 802.12 прямо относятся к подуровню MAC второго (канального) уровня эталонной модели OSI. Остальные 802-спецификации решают общие вопросы сетей.

4.2. Аппаратура локальных сетей

Аппаратура локальных сетей обеспечивает реальную связь между абонентами. Выбор аппаратуры имеет важнейшее значение на этапе проектирования сети, так как стоимость аппаратуры составляет наиболее существенную часть от стоимости сети в целом, а замена аппаратуры связана не только с дополнительными расходами, но зачастую и с трудоемкими работами. К аппаратуре локальных сетей относятся:

- кабели для передачи информации;
- разъемы для присоединения кабелей;
- согласующие терминаторы;
- сетевые адаптеры;
- репитеры;
- трансиверы;
- концентраторы;
- мосты;
- маршрутизаторы;
- шлюзы.

О первых трех компонентах сетевой аппаратуры уже говорилось в предыдущих главах. Сейчас мы остановимся на функциях остальных компонентов.

Сетевые адаптеры (они же контроллеры, карты, платы, интерфейсы, NIC -Network Interface Card) — это основная часть аппаратуры локальной сети, без которой сеть невозможна. Назначение сетевого адаптера — сопряжение компьютера (или другого абонента) с сетью, то есть обеспечение обмена информацией между компьютером и каналом связи в соответствии с принятыми правилами обмена. Именно они выполняют функции нижних уровней модели OSI. Как правило, сетевые адаптеры выполняются в виде платы, вставляемой в слоты расширения системной магистрали (шины) компьютера (чаще всего PCI). Плата сетевого адаптера обычно имеет также один или несколько внешних разъемов для подключения к ней кабеля сети.

Все функции сетевого адаптера делятся на магистральные и сетевые. К магистральным относятся те функции, которые осуществляют обмен адаптера с магистралью (системной шиной) компьютера (то есть

опознание своего магистрального адреса, пересылка данных в компьютер и из компьютера, выработка сигнала прерывания компьютера и т.д.). Сетевые функции обеспечивают общение адаптера с сетью.

Для нормальной работы платы адаптера в составе компьютера необходимо правильно установить ее основные параметры:

- базовый адрес порта ввода/вывода (то есть начальный адрес зоны адресов, по которым компьютер будет общаться с адаптером);
- номер используемого прерывания (то есть номер линии запроса, по которой адаптер будет сообщать компьютеру о необходимости обмена с ним);
- базовые адреса буферной и загрузочной памяти (то есть начальные адреса зон адресов памяти, входящей в состав адаптера, по которым компьютер будет общаться с данной памятью).

Эти параметры могут выбираться на плате адаптера с помощью устанавливаемых пользователем перемычек (джамперов) или переключателей, но могут задаваться и программно с помощью специальной программы инициализации адаптера, поставляемой вместе с платой (в так называемых Jumperless-адаптерах). При выборе всех параметров (адресов и номеров прерываний) необходимо следить, чтобы они отличались от тех, которые заняты другими устройствами компьютера (как системными, так и дополнительно подключенными). Современные сетевые адаптеры часто поддерживают режим Plug-and-Play, то есть не нуждаются в настройке параметров со стороны пользователя, настройка в них осуществляется автоматически при включении питания компьютера.

К основным сетевым функциям адаптеров относятся следующие:

- гальваническая развязка компьютера и кабеля локальной сети (для этого обычно используется передача сигналов через импульсные трансформаторы);
- преобразование логических сигналов в сетевые и обратно;
- кодирование и декодирование сетевых сигналов;
- опознание принимаемых пакетов (выбор из всех приходящих пакетов тех, которые адресованы данному абоненту);
- преобразование параллельного кода в последовательный при передаче и обратное преобразование при приеме;
- буферирование передаваемой и принимаемой информации в буферной памяти адаптера;
- организация доступа к сети в соответствии с принятым методом управления обменом;
- подсчет контрольной суммы пакетов при передаче и приеме.

Как правило, все сетевые функции выполняются специальными микросхемами высокой степени интеграции, что позволяет снизить стоимость адаптера и уменьшить площадь его платы.

Некоторые адаптеры позволяют реализовать функцию удаленной загрузки, то есть поддерживать работу в сети бездисковых компьютеров, загружающих свою операционную систему прямо из сети. Для этого в состав таких адаптеров включается постоянная память с соответствующей программой загрузки. Правда, не все сетевые программные средства поддерживают данный режим работы.

Если сетевой адаптер может работать с несколькими типами кабеля, то еще одним настраиваемым параметром может быть выбор типа кабеля. Например, на плате адаптера может находиться группа переключателей, перекоммутирующих нужные цепи для того или иного типа кабеля.

Все остальные аппаратные средства локальных сетей (кроме адаптеров) имеют вспомогательный характер, и без них часто можно обойтись

Трансиверы, или приемопередатчики (от английского TRANsmitter + reCEIVER), служат для передачи информации между адаптером и кабелем сети или между двумя сегментами (частями) сети. Трансиверы усиливают сигналы, преобразуют их уровни или преобразуют сигналы в другую форму (например, из электрической в световую и обратно). Трансиверами также часто называют встроенные в адаптер приемопередатчики.

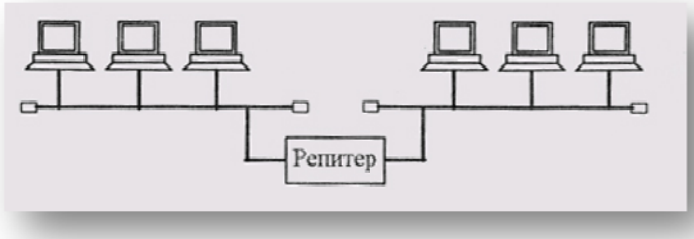


Рис. 4.3
Соединение репитером двух сегментов сети

Репитеры, или повторители (repeater), выполняют более простую функцию, чем трансиверы. Они не преобразуют ни уровни сигналов, ни их вид, а только восстанавливают ослабленные сигналы (их амплитуду и форму), приводя их форму к исходному виду. Цель такой ретрансляции сигналов состоит в увеличении длины сети (рис. 4.3). Однако часто репитеры выполняют и некоторые другие функции, например гальваническую развязку соединяемых сегментов. В любом случае, как репитеры, так и трансиверы не производят никакой информационной обработки проходящих через них сигналов.

Концентраторы (hub), как следует из их названия, служат для объединения в единую сеть нескольких сегментов сети. Концентраторы можно разделить на пассивные и активные.

Пассивные, или репитерные, концентраторы представляют собой собранные в едином конструктиве несколько репитеров. Они выполняют те же функции, что и репитеры (рис. 4.4). Преимущество подобных концентраторов по сравнению с отдельными репитерами только в том, что все точки подключения собраны в одном месте, что упрощает реконфигурацию сети, контроль за ней и поиск неисправностей. К тому же все репитеры в данном случае питаются от единого качественного источника питания.

Пассивные концентраторы иногда вмешиваются в обмен, помогая устранять некоторые явные ошибки обмена.

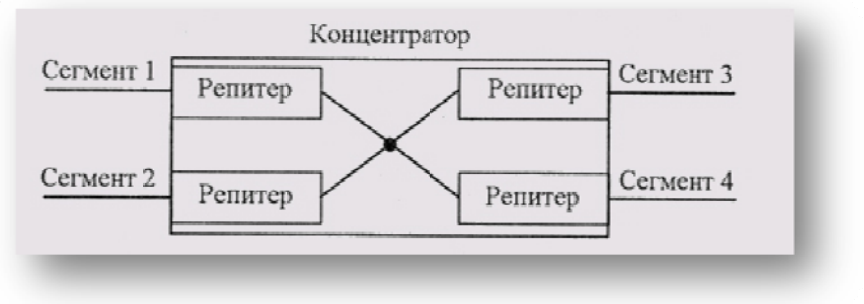


Рис. 4.4
Структура репитерного концентратора

Активные концентраторы выполняют более сложные функции, чем пассивные, например, они могут преобразовывать информацию и протоколы обмена. Правда, это преобразование очень простое. Примером активных концентраторов могут служить коммутирующие или переключающие концентраторы (switching hub), коммутаторы. Они передают из одного сегмента сети в другой сегмент не все пакеты, а только те, которые действительно адресованы компьютерам из другого сегмента. При этом сам пакет коммутатором не принимается. Это приводит к снижению интенсивности обмена в сети вследствие разделения нагрузки, так как каждый сегмент работает только со своими пакетами.

Мосты (bridge), маршрутизаторы (router) и шлюзы (gateway) служат для объединения в единую сеть нескольких разнородных сетей с разными протоколами обмена нижнего уровня, в частности, с разными форматами пакетов, разными методами кодирования, разной скоростью передачи и т.д. В результате их применения сложная и неоднородная сеть, содержащая в себе самые разные сегменты, с точки зрения пользователя выглядит обычной сетью — то есть обеспечивается «прозрачность» сети для протоколов высокого уровня. Естественно, мосты, маршрутизаторы и шлюзы гораздо сложнее и дороже, чем концентраторы, так как от них требуется довольно сложная обработка информации. Реализуются они на базе компьютеров, подключенных к сети с помощью сетевых адаптеров. По сути, это специализированные абоненты (узлы) сети.

Мосты — наиболее простые устройства, служащие для объединения сетей с разными стандартами обмена, например Ethernet и Arcnet, или нескольких сегментов (частей) одной и той же сети, например Ethernet (рис. 4.5). В последнем случае мост служит только для разделения нагрузок сегментов, повышая тем самым производительность сети в целом. В отличие от коммутирующих концентраторов, мосты принимают поступающие пакеты целиком и в случае необходимости производят их простейшую обработку.

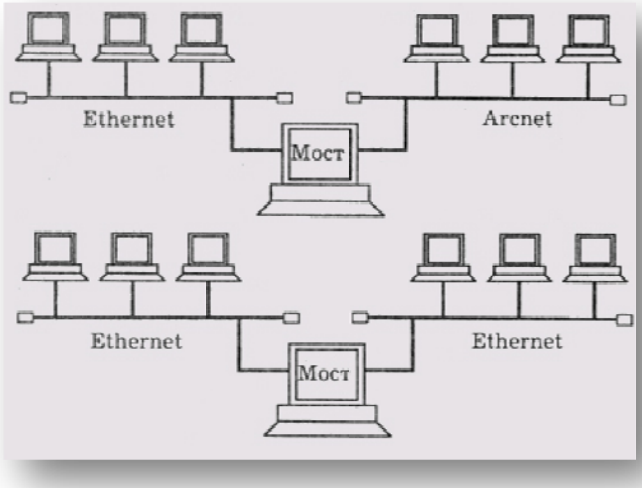


Рис. 4.5
Включение моста

Маршрутизаторы выполняют более сложную функцию, чем мосты. Их главная задача — выбор для каждого пакета оптимального маршрута для избегания чрезмерной нагрузки отдельных участков сети и обхода поврежденных участков. Они применяются, как правило, в сложных разветвленных сетях, имеющих несколько маршрутов между отдельными абонентами. Маршрутизаторы не преобразуют протоколы нижних уровней, поэтому они соединяют только сегменты одноименных сетей. Существуют также гибридные маршрутизаторы (brouter), представляющие собой гибрид моста и маршрутизатора. Они выделяют пакеты, которым нужна маршрутизация, и обрабатывают их как маршрутизаторы, а для остальных пакетов служат обычными мостами.

Шлюзы — это устройства для соединения совершенно различных сетей с сильно отличающимися протоколами, например для соединения локальных сетей с большими компьютерами или с глобальными сетями. Это самые дорогие и редко применяемые сетевые устройства.

Если обратиться к модели OSI, то можно считать, что репитеры и репи-терные концентраторы связывают сети или сегменты на первом уровне, мосты — на втором уровне, маршрутизаторы — на третьем уровне, а шлюзы — на более высоких уровнях (на 4, 5, 6 и 7). Соответственно, репитеры выполняют функции (не все, а только некоторые) первого уровня, мосты реализуют функции второго уровня (на первом уровне и частично на втором у них работают сетевые адаптеры), маршрутизаторы — третьего уровня, а шлюзы должны выполнять функции всех уровней.

4.3. Стандартные сетевые протоколы

Протокол — это набор правил и процедур, регулирующих порядок осуществления связи. Естественно, все компьютеры, участвующие в обмене, должны работать по одним и тем же протоколам, чтобы по завершении передачи вся информация восстанавливалась в первоначальном виде.

О протоколах самых нижних уровней (физического и канального), относящихся к аппаратуре, уже упоминалось в предыдущих разделах. В частности, к ним относятся методы кодирования и декодирования, методы управления обменом в сети. Подробнее о некоторых из них будет рассказано в специальных главах книги. А сейчас мы остановимся на особенностях протоколов более высоких уровней, реализуемых программно.

Связь сетевого адаптера с сетевым программным обеспечением осуществляют драйверы сетевых адаптеров. Именно благодаря драйверу компьютер может не знать никаких аппаратурных особенностей адаптера (ни его адресов, ни правил обмена с ним, ни его характеристик). Драйвер унифицирует, делает единообразным общение программных средств с любой платой данного класса. Сетевые драйверы, поставляемые вместе с сетевыми адаптерами, позволяют сетевым программам одинаково работать с платами разных поставщиков и даже с платами разных локальных сетей (Ethernet, Arcnet, Token-Ring и т.д.). Если говорить о стандартной модели OSI, то драйверы, как правило, выполняют часть функций верхнего подуровня (подуровень управления доступом к среде, MAC) канального уровня, хотя иногда они выполняют 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 и информируют компьютер о приеме пакета.

В любом случае перед приобретением платы адаптера не мешает ознакомиться со списком совместимого оборудования (Hardware Compatibility List, HCL), который публикуют все производители сетевых операционных систем. Выбор там довольно велик (например, для Microsoft Windows NT Server

список включает более сотни драйверов сетевых адаптеров). Если в список HCL не входит адаптер какого-то типа, лучше не рисковать и не покупать его.

Рассмотрим теперь кратко протоколы более высоких уровней.

Существует несколько стандартных наборов (или, как их еще называют, стеков) протоколов, получивших сейчас наиболее широкое распространение:

- набор протоколов ISO/OSI;
- IBM System Network Architecture (SNA);
- Digital DECnet;
- Novell NetWare;
- Apple AppleTalk;
- набор протоколов глобальной сети Internet, TCP/IP.

Включение в этот список протоколов глобальной сети вполне объяснимо, ведь модель OSI используется для любой открытой системы, как на базе локальной сети, так и на основе глобальной сети или комбинации локальной и глобальной сетей.

Протоколы перечисленных наборов делятся на три основные типа:

прикладные протоколы (выполняющие функции прикладного, представительского и сеансового уровней модели OSI);

транспортные протоколы (выполняющие функции транспортного и сеансового уровней OSI);

сетевые протоколы (выполняющие функции трех нижних уровней OSI).

Прикладные протоколы обеспечивают взаимодействие приложений и обмен данными между ними. К наиболее популярным из них относятся следующие:

- FT AM (File Transfer Access and Management) — протокол OSI доступа к файлам; >
- X.400 — протокол CCITT для международного обмена электронной почтой;
- X.500 — протокол CCITT служб файлов и каталогов на нескольких системах;
- SMTP (Simple Mail Transfer Protocol) — протокол глобальной сети Internet для обмена электронной почтой;
- FTP (File Transfer Protocol) — протокол глобальной сети Internet для передачи файлов;
- SNMP (Simple Network Management Protocol) — протокол для мониторинга сети, контроля за работой сетевых компонентов и управления ими;
- Telnet — протокол глобальной сети Internet для регистрации на удаленных хостах и обработки данных на них;
- Microsoft SMBs (Server Message Blocks, блоки сообщений сервера) и клиентские оболочки или редиректоры Microsoft;
- NCP (Novell NetWare Core Protocol) и клиентские оболочки или редиректоры Novell.

Транспортные протоколы поддерживают сеансы связи между компьютерами и гарантируют надежный обмен данными между ними. Наиболее популярны из них следующие:

- TCP (Transmission Control Protocol) — TCP/IP-протокол для гарантированной доставки данных, разбитых на последовательность фрагментов;
- SPX — часть набора протоколов IPX/SPX (Internetwork Packet Exchange/Sequential Packet Exchange) для данных, разбитых на последовательность фрагментов, предложенный фирмой Novell;
- NWLink — реализация протокола IPX/SPX от фирмы Microsoft;
- NetBEUI — (NetBIOS Extended User Interface, расширенный интерфейс NetBIOS) — устанавливает сеансы связи между компьютерами (NetBIOS) и предоставляет верхним уровням транспортные услуги (NetBEUI).

Сетевые протоколы управляют адресацией, маршрутизацией, проверкой ошибок и запросами на повторную передачу. Наиболее популярны из них следующие:

- IP (Internet Protocol) — TCP/IP-протокол для передачи данных;
- IPX (Internetwork Packet Exchange) — протокол фирмы NetWare для передачи и маршрутизации пакетов;
- NWLink — реализация протокола IPX/SPX фирмой Microsoft;
- NetBEUI — транспортный протокол, обеспечивающий услуги транспортировки данных для сеансов и приложений NetBIOS.

Все перечисленные протоколы могут быть поставлены в соответствие тем или иным уровням эталонной модели OSI. При этом надо учитывать, что разработчики протоколов не слишком строго придерживаются этих уровней. Например, некоторые протоколы выполняют функции, относящиеся сразу к нескольким уровням модели OSI, а другие — только часть функций одного из уровней. Это приводит к тому, что протоколы разных фирм часто оказываются несовместимы между собой, а также к тому, что протоколы могут быть успешно использованы исключительно в составе своего набора протоколов (стека), который выполняет более или менее законченную группу функций. Как раз это и делает сетевую операционную систему «фирменной», то есть, по сути, несовместимой со стандартной моделью открытой системы OSI.

Рассмотрим теперь подробнее некоторые наиболее распространенные протоколы.

Модель OSI допускает два различных метода взаимодействия в сети:

Метод взаимодействия без логического соединения (метод дейтаграмм) — самый старый и простейший метод, в котором каждый пакет рассматривается как самостоятельный объект (рис. 4.10). Пакет передается без установления логического канала, то есть без предварительного обмена служебными пакетами для выяснения готовности приемника, а также без ликвидации логического канала, то есть без пакета подтверждения окончания передачи. Дойдет пакет до приемника или нет — неизвестно (проверка факта получения переносится на более высокие уровни). Метод дейтаграмм предъявляет повышенные требования к аппаратуре (так как приемник всегда должен быть готов к приему пакета). Достоинство метода в том, что передатчик и приемник работают независимо друг от друга, к тому.же пакеты могут буферироваться и передаваться затем все вместе, можно также использовать широковещательную передачу, то есть адресовать пакет всем абонентам одновременно. Недостатки метода — это возможность потери пакетов, а также возможность бесполезной загрузки сети пакетами в случае отсутствия или неготовности приемника.

Метод с логическим соединением (рис. 4.11, см. также рис. 3.2) -это более поздняя разработка с более сложным порядком взаимодействия. Пакет передается только после того, как будет установлено логическое соединение (канал) между приемником и передатчиком. Каждому информационному пакету сопутствует один или несколько служебных пакетов (установка соединения, подтверждение получения, запрос повторной передачи, разъединение соединения). Логический канал может устанавливаться на время передачи одного или нескольких пакетов. Метод более сложен, чем метод дейтаграмм, но гораздо надежнее его, так как к моменту ликвидации логического канала передатчик уверен, что все его пакеты дошли до места назначения, причем дошли успешно. Не бывает при данном методе и перегрузки сети из-за бесполезных пакетов, как в случае метода дейтаграмм. Недостаток метода с логическим соединением состоит в том, что довольно сложно разрешить ситуацию, когда принимающий абонент по тем или иным причинам не готов к обмену, например из-за обрыва кабеля, отключения питания, неисправности сетевого оборудования, сбоя в компьютере. При этом требуется алгоритм обмена с повторением неподтвержденного пакета заданное количество раз, причем важен и тип неподтвержденного пакета.

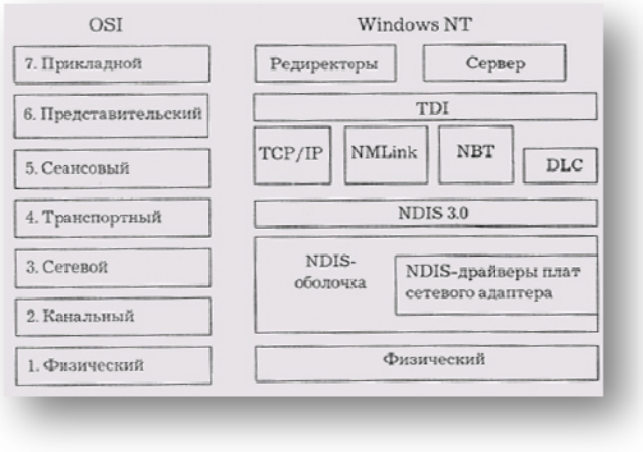


Рис. 4.7
Соотношение уровней модели OSI и протоколов операционной системы Windows NT

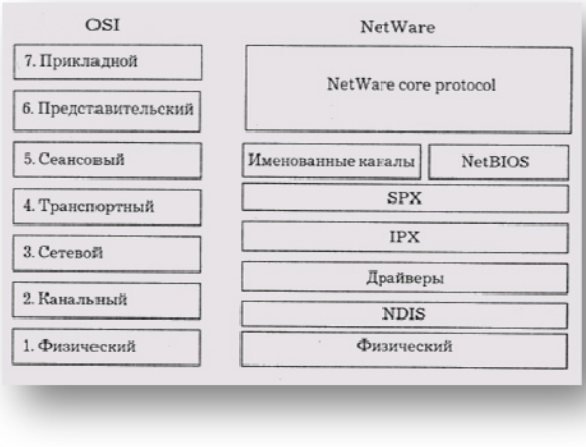


Рис. 4.8
Соотношение уровней модели OSI и протоколов операционной системы NetWare

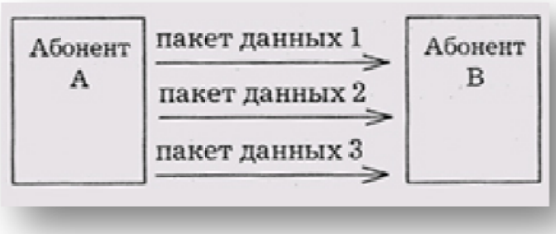


Рис. 4.10
Методдейта грамм

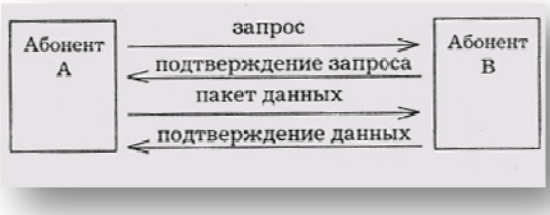


Рис. 4.11
Метод с логическим соединением

Примеры протоколов, работающих по первому методу — это IP и IPX, а протоколов, работающих по второму методу — это TCP и SPX. Именно поэтому эти протоколы используются в виде связанных наборов TCP/IP и IPX/SPX, в которых протокол более высокого уровня (TCP, SPX), работающий на базе протокола более низкого уровня (IP, IPX), гарантирует правильную доставку пакетов в требуемом порядке. Это позволяет объединить достоинства двух рассмотренных методов.

Протоколы IPX/SPX образуют набор, используемый в сетевых программных средствах локальных сетей фирмы Novell (NetWare), которые в наше время являются одними из самых популярных. Это сравнительно небольшой и быстрый протокол, поддерживающий маршрутизацию. Прикладные программы могут обращаться непосредственно к уровню IPX, например, для посылки широковещательных сообщений, но значительно чаще работают с уровнем SPX, гарантирующим быструю и надежную доставку пакетов. Если скорость не слишком важна, то используется еще более высокий уровень, например NetBIOS, предоставляющий более удобный сервис. Фирмой Microsoft предложена своя реализация IPX/SPX, называемая NWLink.

Протокол TCP/IP специально разработан для глобальных сетей и для межсетевого взаимодействия. Он рассчитан на низкое качество каналов связи, на большую вероятность ошибок и разрывов связей. Этот протокол принят во всемирной компьютерной сети Internet, значительная часть 1бонентов которой подключается по коммутируемым линиям (то есть эбычным телефонным линиям). Протокол TCP/IP также поддерживает маршрутизацию. На его основе работают протоколы более высоких уровней, такие как SMTP, FTP, SNMP. Недостаток протокола TCP/IP — низшая скорость работы.

Протокол NetBIOS (сетевая базовая система ввода/вывода) был разра-Зотан фирмой IBM первоначально для сетей IBM PC Network и IBM Foken-Ring no образцу системы BIOS персонального компьютера. С тех тор этот протокол стал фактическим стандартом (официально он не стандартизован), и многие сетевые операционные системы содержат в себе эмулятор NetBIOS для обеспечения совместимости. Первоначально NetBIOS реализовывал сеансовый, транспортный и сетевой уровни, од-яако в последующих сетях на более низких уровнях используются стандартные протоколы (например, IPX/SPX), а на долю эмулятора NetBIOS эстается только сеансовый уровень. NetBIOS обеспечивает более высокий уровень сервиса, чем IPX/SPX, но он работает медленнее. Протокол NetBEUI — это развитие протокола NetBIOS до транспортного уровня.

Наконец, упоминавшийся набор протоколов OSI — это полный стек про-гоколов, где каждый протокол точно соответствует конкретному уровню стандартной модели OSL Набор содержит маршрутизируемые и транспортные протоколы, серии протоколов IEEE 802, протокол сеансового уровня представительского уровня и несколько протоколов прикладного уровня. Пока широкого распространения этот набор протоколов не получил, хотя он и полностью соответствует эталонной модели.

4.4. Стандартные сетевые программные средства

Функции верхних уровней эталонной модели OSI выполняют сетевые программные средства. Для установки сети достаточно иметь набор сетевого оборудования, его драйверы, а также какое-нибудь сетевое программное обеспечение. От выбора этого программного обеспечения зависит очень многое: допустимый размер сети, удобство использования и контроля сети, режимы доступа к ресурсам, производительность сети в разных режимах и т.д. Правда, заменить одну программную систему на другую значительно проще, чем сменить оборудование.

С точки зрения распределения функций между компьютерами сети, все сети можно разделить на две группы.

Одноранговые сети, то есть сети, состоящие из равноправных (с точки зрения доступа к сети) компьютеров.

Сети на основе серверов, в которых существуют только выделенные (dedicated) серверы, занимающиеся исключительно сетевыми функциями. Выделенный сервер может быть единственным или их может быть несколько.

Соответственно этому делению существуют и типы программных средств, реализующих эти виды сетей.

Одноранговые сети (рис. 4.12) и соответствующие программные средства, как правило, используются при необходимости объединения небольшого количества компьютеров (до 10-20). Каждый компьютер такой сети может одновременно являться и сервером, и клиентом сети, хотя вполне возможно назначение какого-то компьютера только сервером, а какого-то — только клиентом. Принципиальна именно возможность совмещения функций клиента и сервера. Важно также то, что в одноранговой сети любой сервер может быть невыделенным (non-dedicated), то есть может не только обслуживать сеть, но и работать как автономный компьютер (правда, запросы к нему по сети могут сильно снизить скорость его работы). В одноранговой сети могут быть и выделенные серверы, только обслуживающие сеть, это не принципиально.

Рис. 4.12
Одноранговая сеть

Именно в данном случае наиболее правильно говорить о распределенных дисковых ресурсах, о виртуальном компьютере, а также о суммировании объемов дисков всех компьютеров сети. Если все компьютеры являются серверами, то любой файл, созданный на одном компьютере, сразу же становится доступным всем остальным компьютерам, его не надо передавать на централизованный сервер.

Достоинством одноранговых сетей является их высокая гибкость: в этом случае сеть может использоваться очень активно, а может и не использоваться совсем в зависимости от конкретной задачи. Из-за большой самостоятельности компьютеров в таких сетях редко бывает ситуация перегрузки сети (к тому же количество компьютеров обычно невелико). В одноранговых сетях допускается определение различных прав пользователей по доступу к сетевым ресурсам, но система разграничения прав не слишком развита. Также недостатком одноранговых сетей является слабая система контроля за сетью, протоколирования работы сети. К тому же выход из строя любого компьютера-сервера приводит к потере части общей информации, то есть все такие компьютеры должны быть по возможности высоконадежными. Эффективная скорость передачи информации по одноранговой сети часто оказывается недостаточной, так как трудно обеспечить высокую скорость процессоров, большой объем оперативной памяти и высокие скорости обмена с жестким диском для всех компьютеров сети. К тому же компьютеры сети работают не только на сеть, но решают и другие задачи.

Несколько примеров распространенных одноранговых сетевых программных средств:

- NetWare Lite фирмы Novell;
- LANtastic фирмы Artisoft;
- Windows for Workgroups фирмы Microsoft;
- Windows NT Workstation фирмы Microsoft;
- Windows 95 фирмы Microsoft.

Одноранговые сетевые программные средства могут быть сетевыми оболочками, работающими под управлением DOS (например, NetWare Lite), а могут быть встроены в операционную систему (Windows 95). Отличаются они друг от друга разными эффективными скоростями обмена (сеть LANtastic работает несколько медленнее, чем NetWare Lite, так как использует более медленные, хотя и более надежные протоколы обмена), разным удобством использования (встроенные сетевые средства Windows 95 не требуют никаких дополнительных затрат на установку сетевых программ).

Сетевые оболочки работают, перехватывая все запросы DOS. Те запросы, которые вызываются обращениями к сетевым устройствам, обрабатываются и выполняются сетевой оболочкой, а те, которые вызваны обращениями к «местным», несетевым ресурсам, возвращаются обратно в DOS и обрабатываются стандартным образом. Примерная схема этого механизма представлена на рис. 4.13. Программа, непосредственно обрабатывающая запросы, называется редиректором.

Сети на основе сервера применяются в тех случаях, когда в сеть должно быть объединено много пользователей. В этом случае быстродействия одноранговой сети может не хватить. Поэтому в сеть

включается специализированный компьютер — сервер, который обслуживает только сеть и не решает никаких других задач (рис. 4.14). Такой сервер называется выделенным. Серверы специально оптимизированы для быстрой обработки сетевых запросов на разделяемые ресурсы и для управления защитой файлов и каталогов. При больших размерах сети мощности одного сервера может оказаться недостаточно, и тогда в сеть включают несколько серверов. Серверы могут выполнять и некоторые другие задачи: сетевая печать, выход в глобальную сеть, связь с другой локальной сетью, обслуживание электронной почты и т.д. Количество пользователей сети на основе сервера может достигать нескольких тысяч. Одноранговой сетью такого размера просто невозможно было бы управлять.

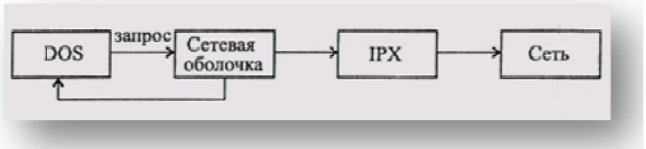


Рис. 4.13
Обработка запросов DOS сетевой оболочкой

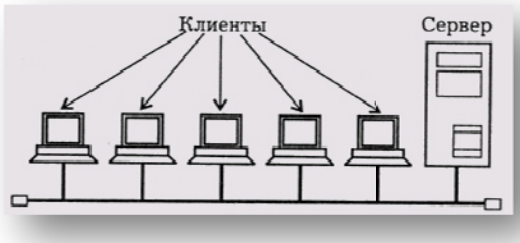


Рис. 4.14
Сеть на основе сервера

В любом случае в сети на основе сервера существует четкое разделение компьютеров на клиентов (или рабочие станции) и серверы. Клиенты не могут работать как серверы, а серверы — как клиенты и как автономные компьютеры. Очевидно, что все сетевые дисковые ресурсы могут располагаться только на сервере, а клиенты могут обращаться только к серверу, но не друг к другу. Однако это не значит, что они не могут общаться между собой, просто пересылка информации от одного клиента к другому возможна только через сервер, например через файл, доступный всем клиентам. В данном случае реализуется некоторая «логическая звезда» с сервером в центре, хотя физическая топология сети может быть любой.

Достоинством сети на основе сервера часто называют надежность. Это верно, но только с одной оговоркой: если сервер действительно очень на

дежен. В противном случае любой отказ сервера приводит к полному параличу сети в отличие от ситуации с одноранговой сетью, где отказ одного из компьютеров не приводит к полному отказу все сети. Бесспорное достоинство сети на основе сервера — высокая скорость обмена, так как сервер всегда оснащается быстрым процессором (или даже несколькими процессорами), оперативной памятью большого объема и быстрыми жесткими дисками. Так как все ресурсы сети собраны в одном месте, возможно применение гораздо более мощных средств управления доступом, защиты данных, протоколирования обмена, чем в одноранговых сетях.

К недостаткам сети на основе сервера относятся ее громоздкость в случае небольшого количества компьютеров, зависимость всех компьютеров-клиентов от сервера, более высокая стоимость сети вследствие использования дорогого сервера. Но, говоря о стоимости, надо также учитывать, что при одном и том же объеме сетевых дисков большой диск сервера получается дешевле, чем много дисков меньшего объема, входящих в состав всех компьютеров одноранговой сети.

Примеры некоторых распространенных сетевых программных средств на основе сервера:

- NetWare фирмы Novell;
- LAN Server фирмы IBM;
- VINES фирмы Banyan Systems;
- LAN Manager фирмы Microsoft;
- Windows NT Server фирмы Microsoft.

На файл-сервере в данном случае устанавливается сетевая операционная система, заменяющая DOS. Эта сетевая ОС специально оптимизирована для эффективного выполнения специфических операций по организации сетевого обмена. На рабочих станциях (клиентах) может устанавливаться как сетевая оболочка, работающая над DOS (как в случае NetWare), так и операционная система (как в случае Windows NT).

Для обеспечения надежной работы сети при авариях электропитания применяется бесперебойное электропитание сервера. В данном случае это гораздо проще, чем при одноранговой сети, где приходится оснащать источниками бесперебойного питания все компьютеры сети. Сервер может комплектоваться очень простым и дешевым видеомонитором, может даже вообще не иметь его, так как единственная функция этого монитора — контроль за запуском сетевого программного обеспечения.

Для администрирования сети (то есть управления распределением ресурсов, контроля за правами доступа, за защитой данных, за файловой системой, резервированием файлов и т.д.) в случае сети на основе

сервера необходимо выделять специального человека, имеющего соответствующую квалификацию. Централизованное администрирование облегчает обслуживание сети и позволяет оперативно решать все вопросы. Особенно это важно для надежной защиты данных от несанкционированного доступа. В случае же одноранговой сети можно обойтись и без специалиста-администратора, правда, все пользователи сети должны при этом иметь хоть какое-то представление об администрировании.

А теперь очень кратко остановимся на основных особенностях некоторых наиболее популярных типах сетевых программных средств.

4.4.1. Сетевые программные средства фирмы Novell

Сетевые операционные системы NetWare фирмы Novell на сегодняшний день наиболее популярны в мире. Более половины всех локальных сетей в мире используют различные версии именно этого программного обеспечения. Популярность NetWare определяется хорошей производительностью, способностью работать с разными аппаратными средствами и развитой системой средств защиты данных. Фирма Novell выпускает различные сетевые программные средства: несколько версий сетевых ОС на базе файловых серверов (среди них версия 4.0 для предприятий и версия 3.12), одноранговые сетевые ОС Personal NetWare и NetWare Lite, а также средства диагностики работы сетей.

Продуктам Novell NetWare присущи и недостатки, например, их стоимость для небольших сетей оказывается одной из самых высоких по сравнению с продуктами других производителей. Кроме того, их установка довольно сложна. Но они уже стали фактическим стандартом, поэтому их позиции на рынке довольно прочны.

Рассмотрим кратко особенности основных типов сетевых ОС.

NetWare 2.2 — это самая простая ОС (16-разрядная), имеющаяся на рынке. Выпускаются версии на число пользователей до 5, 10, 50 и 100, отличающиеся ценой (например, версия на 5 пользователей примерно в 6 раз дешевле версии на 100 пользователей). Первая цифра в обозначении версии говорит о минимальных требованиях к процессору компьютеров сети (2 означает процессор не хуже 80286). По сравнению с предшествующей версией 2.15 значительно упрощен процесс инсталляции сети. NetWare 2.2, в отличие от других версий, допускает работу без выделенного сервера, то есть сервер может работать как автономный компьютер, правда, с довольно низкой скоростью.

NetWare 3.12 — это 32-разрядная ОС, ориентированная на работу с процессорами не ниже 80386 (80386, 80486 или Pentium). Ее возможности су

щественно расширены по сравнению с версией 2.2. Например, она обеспечивает доступ к памяти до 4 Гб для кэширования, присоединение к одному серверу до 250 пользователей (выпускаются версии на 20, 100 и 250 пользователей), объем дисковой памяти до 32 Тб (триллионов байт), максимальный размер файла до 4 Гб. Стоимость версии на 20 пользователей примерно вчетверо ниже, чем версии на 250 пользователей.

NetWare 3.12 поддерживает рабочие станции с разными ОС (DOS, Macintosh, OS/2 и UNIX). Для этого предусмотрены специальные атрибуты имен файлов. Файлы, созданные под управлением одной ОС, доступны пользователям, имеющим другие ОС. Открытость архитектуры NetWare 3.12 обеспечивается также новым интерфейсом транспортного уровня (ТЫ — Transport Layer Interface), который допускает использование протоколов NetBIOS, IPX/SPX, LU6.2. Предусмотрена также поддержка протокола TCP/IP. Важной особенностью NetWare 3.12 является динамическое распределение памяти.

Инсталляция NetWare 3.12 довольно проста, не сложнее NetWare 2.2, она занимает не более 30 минут. Предусмотрена возможность включения 32-битового сетевого адаптера.

NetWare 4.0 — это ОС, появившаяся в 1993 году. Она рассчитана на работу с процессором не ниже 80386 и допускает одновременную работу до 1000 пользователей сети (выпускаются версии на 5, 10, 20, 50, 100, 250, 500 и 1000 пользователей). NetWare 4.0 полностью совместима с NetWare 2.2 и NetWare 3.12, так что пользователь не замечает никакой разницы между ними. Рабочие станции даже могут продолжать работу с сетевыми оболочками предыдущих версий. Однако возможности NetWare 4.0 шире, чем у предшественников. Например, пользователи получают возможность доступа к 54000 файловым серверам (в версии 3.12 — только к 8 файловым серверам).

В NetWare 4.0 предусмотрена система кэширования предполагаемого чтения, что увеличивает производительность сети, а также встроенная компрессия хранимых данных. В этой ОС улучшена также защита данных от несанкционированного доступа. Важное отличие от других продуктов — возможность централизованного управления всеми серверами с одной рабочей станции. Любой пользователь сети одновременно получает доступ ко всем ресурсам. Есть возможность автоматического дублирования информации, хранящейся в сетевых разделах.

Минимальный требуемый объем памяти составляет 6 Мб. Объем занимаемого пространства на диске колеблется от 12 Мб до 60 Мб в зависимости от выбранных при инсталляции характеристик.

Все сетевые ОС NetWare допускают подключение бездисковых рабочих станций (клиентов), что позволяет при необходимости значительно снизить стоимость сети в целом, а также (при отказе от флоппи-

дисководов) исключить возможность занесения компьютерных вирусов. Во всех рассмотренных продуктах предусмотрена поддержка сетевых мостов.

NetWare Lite и Personal NetWare — это простые и дешевые версии программных средств фирмы Novell для построения небольших одноранговых сетей. NetWare Lite появилась в 1991 году и представляла собой сетевую оболочку, работающую под управлением DOS. В 1993 году была представлена доработанная версия Personal NetWare, но и NetWare Lite продолжала продаваться. И тот, и другой продукты гораздо проще и дешевле рассмотренных сетевых ОС на основе файл-сервера. Цена в данном случае устанавливается в расчете на одну рабочую станцию и составляет менее 100 долларов, что в несколько раз меньше, чем у самой дешевой версия NetWare 2.2 на 5 пользователей.

Сетевая программа Personal NetWare рассчитана на работу в сети, содержащей от 2 до 25 пользователей. Как и NetWare Lite, она может работать с любым типом процессора и не требует доступа к расширенной или дополнительной памяти компьютера. Минимальный требуемый объем памяти составляет 640 Кб. Оба эти продукта могут работать совместно с NetWare 2.2, 3.12 и 4.0, что позволяет гибко комбинировать преимущества сетевых программных средств разных типов. Инсталляция Personal NetWare и NetWare Lite предельно проста. Предусмотрена защита от несанкционированного копирования программ, которая сводится к автоматической проверке каждой рабочей станцией, имеется ли в сети еще одна рабочая станция с точно такой же копией программного обеспечения.

В обоих продуктах предусмотрена возможность использовать компьютеры сети как серверы, как клиенты, как серверы и клиенты одновременно, а также как выделенные серверы (как правило, на ограниченное время).

Несмотря на свою простоту оба этих продукта предусматривают назначение прав доступа (хотя и не слишком развитое), систему паролей, они достаточно надежны. Правда, в начале выпуска NetWare Lite в ней были кое-какие неприятные ошибки, но в Personal NetWare они были исправлены.

4.4.2. Сетевые программные средства фирм Microsoft и IBM

Фирма Microsoft ведет свою работу по созданию сетевых программных продуктов по нескольким направлениям.

Одно из направлений связано с сотрудничеством с фирмой IBM и поддержкой ее операционной системы OS/2, которая появилась в 1987 году и была призвана заменить собой несовершенную DOS. Именно для совместной работы с OS/2 были предложены продукты LAN Manager фирмы Microsoft и LAN Server фирмы IBM. Однако эти продукты не получили большого распространения в связи с тем, что сама OS/2 не слишком популярна. К тому же они не обеспечивают той независимости от сетевых аппаратных средств, какую гарантируют ОС фирмы Novell (например, они хорошо работают с сетью Token-Ring, но не идеально совмещаются с Ethernet).

Система LAN Manager — это 16-разрядная система, а LAN Server — 32-разрядная система, что, конечно, сказывается на их быстродействии. В обоих продуктах предусмотрена возможность работы сервера как рабочей станции в одноранговой среде, но из соображений защиты данных никто не использует эти продукты для одноранговых сетей. Считается, что данные продукты прекрасно подходят для программирования приложений типа клиент/сервер.

Недостаток этих систем по сравнению с продуктами NetWare — большой требуемый объем дискового пространства для хранения программных и конфигурационных файлов (от 1 Мб до 3 Мб на каждой рабочей станции). Другой недостаток — больший требуемый объем оперативной памяти (90 Кб против 50-60 Кб в NetWare). Правда, в современных компьютерах обычно не ощущается нехватки памяти и дискового пространства.

В последние годы фирма Microsoft пошла своим путем, практически отказавшись от поддержки OS/2 и всячески продвигая свои собственные разработки Windows 95, Windows 98 и Windows NT. Именно исходя из этой концепции, в 1993 году была выпущена новая сетевая ОС Windows NT Advanced Server. Эта 32-разрядная ОС представляет собой дальнейшее развитие LAN Manager. Прежде всего, эта система может работать на платформах MIPS R4000 фирмы Intel и Альфа фирмы Digital (DEC). Кроме того, предусмотрена и возможность работы на мультипроцессорном компьютере.

По сравнению с предыдущими разработками существенно усилена защита данных, которая удовлетворяет требованиям уровня защиты С2, требуемого промышленными и военными сетями (имеется защита процедуры присоединения к сети, защита памяти, учет и контроль доступа). Система Windows NT Advanced Server использует протокол SMB на базе NetBIOS, что определяет ее совместимость с такими средствами, как LAN Manager, LAN Server, Windows for Workgroups и со старой ОС PC LAN Program. Предусмотрена поддержка стандартных протоколов TCP/IP и IPX/SPX.

Недостаток Windows NT Advanced Server по сравнению с сетевыми ОС NetWare — сравнительно низкое быстродействие, так как сетевое программное обеспечение в этом случае связано с платой сетевого адаптера слишком многими промежуточными слоями программного обеспечения. По сравнению с LAN Manager и LAN Server система Windows NT Advanced Server занимает больше места на диске и в памяти.

Помимо сетевых ОС на основе сервера, фирма Microsoft выпускает и одноранговые сетевые средства, причем их отличием от других продуктов того лее назначения является то, что сетевые средства встраиваются в операционную систему компьютера. При этом пользователь, приобретая компьютер с установленной операционной системой, автоматически получает и возможность выхода в сеть. Естественно, это во многих случаях гораздо удобнее, чем приобретать и устанавливать пусть даже и более совершенные продукты других фирм. К тому же пользователю не надо изучать интерфейс пользователя сетевой программы, так как он строится так же, как и интерфейс пользователя всех остальных частей операционной системы.

Речь в данном случае идет об ОС Windows for Workgroups, о более поздней разработке Windows 95, Windows 98 и Windows NT Workstation. Все эти ОС основаны на одних и тех же принципах сетевого обмена, что делает их совместимыми между собой. Предусмотрена поддержка совместного использования дисков (в том числе и гибких дисков и CD), а также принтеров. Имеется возможность объединения всех пользователей в рабочие группы для более удобного поиска требуемых ресурсов и организации доступа к ним. Пользователи имеют доступ к встроенной системе электронной почты, а также к совместному электронному ежедневнику. То есть все пользователи сети получают возможность совместно использовать многие ресурсы ОС своего компьютера.

По сравнению с ОС NetWare данные средства имеют меньшую совместимость с другими типами операционных систем и с аппаратными средствами (сетевыми адаптерами). Поэтому при ориентации на эти продукты надо обращать особое внимание на совместимость с ними приобретаемых сетевых адаптеров.

4.4.3. Сетевые программные средства других фирм

Кроме сетевых программных продуктов ведущих фирм Novell и Microsoft существует еще целый ряд сетевых средств других производителей. Особенно успешно конкурируют другие фирмы с этими гигантами на рынке одноранговых сетей.

LANtastic фирмы Artisoft в течение длительного времени была самой популярной одноранговой системой, которая по сути и создала данный рынок. Несмотря на то, что она не является самой быстродействующей, LANtastic имеет целый ряд замечательных особенностей, например, прекрасные возможности разделения принтера и CD-дисков, а также поддержку звуковой электронной почты. Она требует очень небольшого объема памяти (34Кб на рабочей станции и 60Кб на сервере), к тому же поддерживает совместимость с компьютерами Macintosh и с ОС Windows. В версии 5.0 имеются средства для работы в среде NetWare, в версии 6.0 добавлены средства работы с факсами в сети. Недостаток последних версий LANtastic состоит в том, что они ориентированы в основном на применение оригинальных адаптеров Ethernet производства фирмы Artisoft.

Правда, возможно и использование адаптеров других поставщиков при закупке специальных программ.

В сети LANtastic может работать от двух до трехсот рабочих станций. При большом количестве рабочих станций производительность сети заметно падает (так как LANtastic — это все-таки оболочка, работающая на базе DOS). Несколько улучшить ситуацию может использование нескольких компьютеров в качестве выделенных серверов (возможность этого предусмотрена).

LANtastic отличается невысокой ценой, проста в установке и надежна в администрировании.

POWERLan фирмы Performance Technology — это самая быстродействующая из одноранговых систем (сравнение ее с продуктами Novell представлено в табл. 4.1). Высокое быстродействие достигнуто за счет хорошей проработанности программ: используемая версия NetBIOS считается одной из лучших.

Табл. 4.1. Сравнение времен доступа одноранговых сетевых программных систем

Режим	POWERLan	NetWare Lite	Personal NetWare
На локальном накопителе рабочей станции:			
Чтение	10,20	11,03	10,95
Запись	8,60	8,95	8,15
На диске сервера при доступе с рабочей станции:			
Чтение	17,90	25,40	26,25
Запись	12,05	15,43	15,00
При одновременной работе четырех рабочих станций:			
Чтение	29,10	41,09	38,95

Запись	18,90	34,78	34,12

Существуют версии на 5,15 или неограниченное число пользователей (при этом ограничено только число одновременных присоединений к одному серверу). Сеть POWERLan допускает работу с серверами под управлением UNIX, LAN Server, LAN Manager, NetWare. Она поддерживает более 50 различных сетевых адаптеров. Защита данных довольно хорошо развита, предусмотрено кэширование диска.

На рабочей станции данная система занимает память около 69 Кб. Как и другие одноранговые сети, POWERLan проста в установке и использовании. По многим оценкам она имеет хорошие перспективы, особенно при сравнительно большом количестве абонентов, когда другие одноранговые системы работают медленно.

В заключение данной главы необходимо отметить, что пользователю, работающему с приложениями, вообще-то не слишком важно, какие программные средства, протоколы, аппаратура используются в его сети. Ему гораздо важнее то, что сеть существует, что она дает возможность удобного совместного использования ресурсов. Но такая ситуация сохраняется только до тех пор, пока возможности сети не слишком сдерживают работу приложений. Принципиальное значение имеют разрешенные режимы доступа к этим ресурсам, а также время доступа к ним, что и определяется характеристиками всех рассмотренных средств.

Глава 5. Стандартные локальные сети

Содержание пятой главы:

5.1. Сети Ethernet и Fast Ethernet

За время, прошедшее с появления первых локальных сетей, было разработано несколько сотен самых разных сетевых технологий, однако заметное распространение получили всего несколько сетей, что связано прежде всего с поддержкой этих сетей известными фирмами и с высоким уровнем стандартизации принципов их организации. Далеко не всегда стандартные сети имеют рекордные характеристики, обеспечивают наиболее оптимальные режимы обмена, но большие объемы выпуска их аппаратуры и, следовательно, ее невысокая стоимость обеспечивают им огромные преимущества. Немаловажно и то, что производители программных средств также в первую очередь ориентируются на самые распространенные сети. Поэтому пользователь, выбирающий стандартные сети, имеет полную гарантию совместимости аппаратуры и программ.

В настоящее время тенденция уменьшения количества типов используемых сетей все усиливается. Дело в том, что увеличение скорости передачи в локальных сетях до 100 и даже до 1000 Мбит/с требует применения самых передовых технологий, проведения серьезных и дорогих научных исследований. Естественно, это могут позволить себе только крупнейшие фирмы, которые, конечно же, поддерживают свои стандартные сети и их более совершенные разновидности. К тому же большинство потребителей уже установило у себя какие-то сети и вовсе не желает сразу и полностью заменять все сетевое оборудование на другое, пусть даже в чем-то лучшее. Поэтому в ближайшем будущем вряд ли стоит ожидать принятия принципиально новых стандартов.

На рынке имеются стандартные локальные сети всех возможных топологий, так что выбор у пользователей имеется. Стандартные сети обеспечивают большой диапазон допустимых размеров сети, допустимого количества абонентов сети и, что не менее важно, большой диапазон цен на аппаратуру. Но проблема выбора той или иной сети все равно остается непростой. Ведь в отличие от программных средств, заменить которые совсем не трудно, выбранная аппаратура обычно служит многие годы, так как ее замена ведет не только к большим затратам средств, но и к необходимости перекладки кабелей, а то и к пересмотру всей системы компьютерных средств фирмы. Поэтому ошибки в выборе аппаратуры гораздо дороже ошибок в выборе программных средств.

Мы остановимся в данной главе на основных особенностях аппаратуры наиболее популярных локальных сетей, что, как мы надеемся, поможет читателю сделать правильный выбор.

Наибольшее распространение среди стандартных сетей .получила сеть Ethernet. Впервые она появилась в 1972 году (разработчиком выступила известная фирма Xerox). Сеть оказалась довольно удачной, и вследствие этого ее в 1980 году поддержали такие крупнейшие фирмы, как DEC и Intel (объединение этих фирм, поддерживающих Ethernet, назвали DIX по первым буквам их названий). Стараниями этих фирм в 1985 году сеть Ethernet стала международным стандартом, ее приняли крупнейшие международные организации по стандартам: комитет 802 IEEE (Institute of Electrical and Electronic Engineers) и ECMA (European Computer Manufacturers Association).

Стандарт получил название IEEE 802.3 (по-английски читается как «eight oh two dot three»). Он определяет множественный доступ к моноканалу типа «шина» с обнаружением конфликтов и контролем передачи, то есть с уже упоминавшимся методом доступа CSMA/CD. Вообще-то надо сказать, что этому стандарту удовлетворяют и некоторые другие сети, так как он не очень сильно детализирован. В результате сети стандарта IEEE 802.3 нередко несовместимы между собой как по конструктивным, так и по электрическим характеристикам. Основные характеристики стандарта IEEE 802.3 следующие: топология — шина, среда передачи — коаксиальный кабель, скорость передачи — 10 Мбит/с, максимальная длина — 5 км, максимальное количество абонентов — до 1024, длина сегмента сети — до 500 м, количество абонентов на одном сегменте — до 100, метод доступа -CSMA/CD, передача узкополосная, то есть без модуляции (моноканал).

Строго говоря, между стандартами IEEE 802.3 и Ethernet существуют небольшие отличия, но о них обычно предпочитают не вспоминать.

Сеть Ethernet сейчас наиболее популярна в мире (более 70 миллионов абонентов сети в 1996 году, свыше 100 миллионов абонентов в 1997 году, или более 80% рынка), и нет сомнения, что таковой она и останется в ближайшие годы. Этому в немалой степени способствовало то, что с самого начала все характеристики, параметры, протоколы сети были открыты для всех, в результате чего огромное число производителей во всем мире стали выпускать аппаратуру Ethernet, полностью совместимую между собой.

В классической сети Ethernet применяется 50-омный коаксиальный кабель двух видов (толстый и тонкий). Однако в последнее время (с начала 90-х годов) все большее распространение получает версия Ethernet, использующая в качестве среды передачи витые пары. Определен также стандарт для применения в сети оптоволоконного кабеля. В стандарты были внесены соответствующие добавления. В 1995 году появился стандарт на более быструю версию Ethernet, работающую на скорости 100 Мбит/с (так называемый Fast Ethernet, стандарт IEEE 802.3u), использующую в качестве среды передачи витую пару или оптоволоконный кабель. Появилась и версия на скорость 1000 Мбит/с (Gigabit Ethernet, стандарт IEEE 802.3z).

Помимо стандартной топологии «шина» применяются также топологии типа «пассивная звезда» и «пассивное дерево». При этом предполагается использование репитеров и пассивных (репитерных) концентраторов, соединяющих между собой различные части (сегменты) сети (рис. 5.1). В качестве сегмента может также выступать единичный абонент. Коаксиальный кабель используется для шинных сегментов, а витая пара и оптоволоконный кабель — для лучей пассивной звезды (для присоединения к концентратору одиночных компьютеров). Главное — чтобы в полученной в результате топологии не было замкнутых путей (петель). Фактически получается, что абоненты соединены в физическую шину, так как сигнал от каждого из них распространяется сразу во все стороны и не возвращается назад (как в кольце). Максимальная длина кабеля всей сети в целом (максимальный путь сигнала) теоретически может достигать 6,5 км, но практически не превышает 2,5 км.

В сети Fast Ethernet не предусмотрена физическая топология «шина», используется только «пассивная звезда» или «пассивное дерево». К тому же в Fast Ethernet гораздо более жесткие требования к предельной длине сети. Ведь при увеличении в 10 раз скорости передачи и сохранении формата пакета его минимальная длина становится в десять раз короче (5,12 икс против 51,2 мкс в Ethernet). Допустимая величина двойного времени прохождения сигнала по сети уменьшается в 10 раз.

Для передачи информации в сети Ethernet применяется стандартный код Манчестер-П. При этом один уровень сигнала нулевой, а другой — отрицательный, то есть постоянная составляющая сигнала не равна нулю. При отсутствии передачи потенциал в сети нулевой. Гальваническая развязка осуществляется аппаратурой адаптеров, репитеров и концентраторов. При этом приемопередатчик сети гальванически развязан от остальной аппаратуры с помощью трансформаторов и изолированного источника питания, а с кабелем сети соединен напрямую.

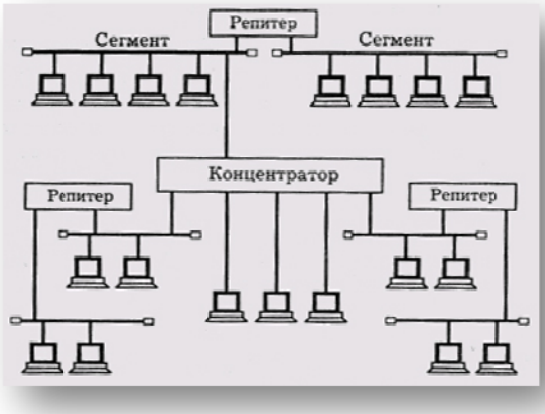


Рис. 5.1
Топология сети Ethernet

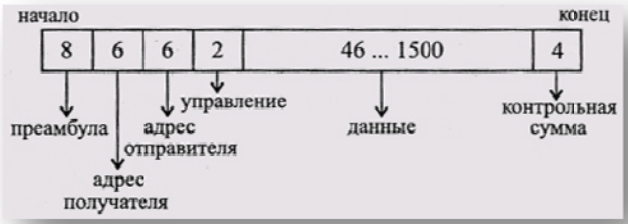


Рис. 5.2
Структура пакета сети Ethernet, (цифры показывают количество байт)

Доступ к сети Ethernet осуществляется по случайному методу CSMA/ CD, обеспечивающему полное равноправие абонентов. В сети используются пакеты переменной длины со структурой, представленной на рис. 5.2. Длина кадра Ethernet (то есть пакета без преамбулы) должна быть не менее 512 битовых интервалов, или 51,2 мкс (именно такова предельная

величина двойного времени прохождения в сети). Предусмотрена индивидуальная, групповая и широковещательная адресация.

В пакет Ethernet входят следующие поля:

Преамбула состоит из 8 байт, первые семь из которых представляют собой код 10101010, а последний восьмой — код 10101011. В стандарте IEEE 802.3 этот последний байт называется признаком начала кадра (SFD — Start of Frame Delimiter) и образует отдельное поле пакета.

Адрес получателя (приемника) и адрес отправителя (передатчика) включают по 6 байт и строятся по стандарту, описанному в разделе 3.2. Эти адресные поля обрабатываются аппаратурой абонентов.

Поле управления (L/T — Length/Type) содержит информацию о длине поля данных. Оно может также определять тип используемого протокола. Принято считать, что если значение этого поля не больше 1500, то оно определяет длину поля данных. Если же его значение больше 1500, то оно определяет тип кадра. Поле управления обрабатывается программно.

Поле данных должно включать в себя от 46 до 1500 байт данных. Если пакет должен содержать менее 46 байт данных, то поле данных дополняется байтами заполнения. Согласно стандарту IEEE 802.3, в структуре пакета выделяется специальное поле заполнения (pad data — незначащие данные), которое может иметь нулевую длину, когда данных достаточно (больше 46 байт).

Поле контрольной суммы (FCS — Frame Check Sequence) содержит 32-разрядную циклическую контрольную сумму пакета (CRC) и служит для проверки правильности передачи пакета.

Таким образом, минимальная длина кадра (пакета без преамбулы) составляет 64 байта (512 бит). Именно эта величина определяет максимально допустимую двойную задержку распространения сигнала по сети в 512 битовых интервалов (51,2 мкс для Ethernet, 5,12 мкс для Fast Ethernet). Стандарт предполагает, что преамбула может уменьшаться при прохождении пакета через различные сетевые устройства, поэтому она не учитывается. Максимальная длина кадра равна 1518 байтам (12144 бита, то есть 1214,4 мкс для Ethernet, 121,44 мкс для Fast Ethernet). Это важно для выбора размера буферной памяти сетевого оборудования и для оценки общей загруженности сети.

Для сети Ethernet, работающей на скорости 10 Мбит/с, стандарт определяет четыре основных типа среды передачи информации:

- 10BASE5 (толстый коаксиальный кабель);
- 10 BASE2 (тонкий коаксиальный кабель);
- 1OBASE-T (витая пара);
- 10BASE-FL (оптоволоконный кабель).

Обозначение среды передачи включает в себя три элемента: цифра «10» означает скорость передачи 10 Мбит/с, слово BASE означает передачу в основной полосе частот (то есть без модуляции высокочастотного сигнала), а последний элемент означает допустимую длину сегмента: «5» — 500 метров, «2» — 200 метров (точнее, 185 метров) или тип линии связи: «T» -витая пара (от английского «twisted-pair»), «F» — оптоволоконный кабель (от английского «fiber optic»).

Точно так же для сети Ethernet, работающей на скорости 100 Мбит/с (Fast Ethernet) стандарт определяет три типа среды передачи:

- 100BASE-T4 (счетверенная витая пара);
- 100BASE-TX (сдвоенная витая пара);
- 100BASE-FX (оптоволоконный кабель).

Здесь цифра «100» означает скорость передачи 100 Мбит/с, буква «T» означает витую пару, буква «F» — оптоволоконный кабель. Типы 1OOBASE-TX и 100BASE-FX иногда объединяют под именем 100BASE-X, а 100BASE-T4 и 100BASE-TX — под именем 100BASE-T.

Подробнее особенности аппаратуры Ethernet, а также алгоритма управления обменом CSMA/CD и алгоритма вычисления циклической контрольной суммы (CRC) будут рассмотрены далее в специальных разделах книги. Здесь же мы только отметим, что сеть Ethernet не отличается ни рекордными характеристиками, ни оптимальными алгоритмами, она уступает по ряду параметров другим стандартным сетям. Но благодаря мощной поддержке, высочайшему уровню стандартизации, огромным объемам выпуска технических средств, Ethernet резко выделяется среди других стандартных сетей, и поэтому любую другую сетевую технологию принято сравнивать именно с Ethernet.

5.2. Сеть Token-Ring

Сеть Token-Ring была предложена фирмой IBM в 1985 году (первый вариант появился в 1980 году). Назначением Token-Ring было объединение в сеть всех типов компьютеров, выпускаемых IBM (от персональных до больших). Уже тот факт, что ее поддерживает фирма IBM, крупнейший производитель компьютерной техники, говорит о том, что ей необходимо уделить особое внимание. Но не менее важно и то, что Token-Ring является в настоящее время международным стандартом IEEE 802.5. Это ставит данную сеть на один уровень по статусу с Ethernet.

Фирма IBM сделала все для максимально широкого распространения своей сети: была выпущена подробная документация вплоть до принципиальных схем адаптеров. В результате многие фирмы, например 3COM, Novell, Western Digital, Proteon приступили к производству адаптеров. Кстати, специально для этой

сети, а также для другой сети IBM PC Network была разработана концепция NetBIOS. Если в разработанной ранее сети PC Network программы NetBIOS хранились во встроенной в адаптер постоянной памяти, то в сети Token-Ring уже применялась эмулирующая NetBIOS программа, что позволяло более гибко реагировать на особенности конкретной аппаратуры, поддерживая при этом совместимость с программами более высокого уровня.

По сравнению с аппаратурой Ethernet аппаратура Token-Ring оказывается заметно дороже, так как использует более сложные методы управления обменом, поэтому распространена сеть Token-Ring значительно меньше. Однако ее применение становится оправданным, когда требуются большие интенсивности обмена (например, при связи с большими компьютерами) и ограниченное время доступа.

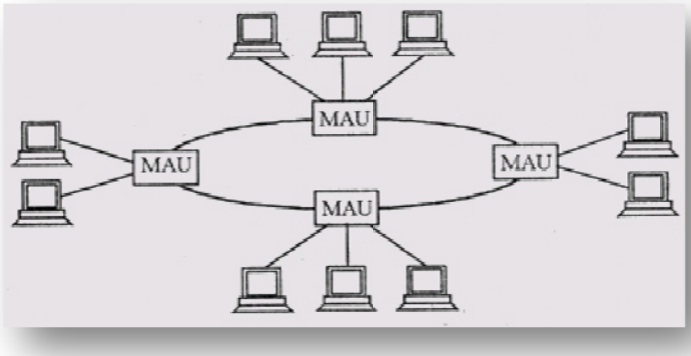


Рис. 5.3
Звездно-кольцевая топология сети Token-Ring

Сеть Token-Ring имеет топологию «кольцо», хотя внешне она больше напоминает «звезду». Это связано с тем, что отдельные абоненты (компьютеры) присоединяются к сети не прямо, а через специальные концентраторы или многостанционные устройства доступа (MSAU или MAU -Multistation Access Unit). Поэтому физически сеть образует звездно-кольцевую топологию (рис. 5.3). В действительности же абоненты объединяются все-таки в кольцо, то есть каждый из них передает информацию одному соседнему абоненту, а принимает информацию от другого соседнего абонента.

Концентратор (MAU) при этом только позволяет централизовать задание конфигурации, отключение неисправных абонентов, контроль за работой сети и т.д. (рис. 5.4). Для присоединения кабеля к концентратору применяются специальные разъемы, которые обеспечивают постоянство замкнутости кольца даже при отключении абонента от сети. Концентратор в сети может быть и единственным, в этом случае в кольцо замыкаются только абоненты, подключенные к нему.

В каждом кабеле, соединяющем адаптеры и концентратор (адаптерные кабели, adapter cable), находятся на самом деле две разнонаправленные линии связи. Такими же двумя разнонаправленными линиями связи, входящими в магистральный кабель (path cable), объединяются между собой в кольцо различные концентраторы (рис. 5.5), хотя для этой же цели может также использоваться и единственная однонаправленная линия связи (рис. 5.6).

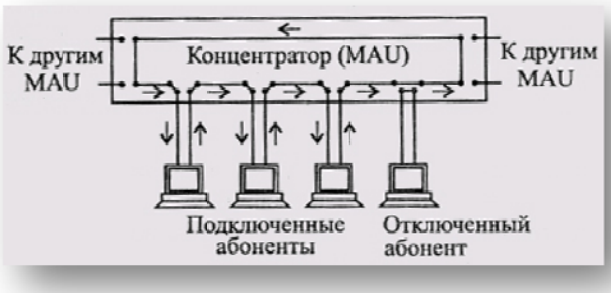


Рис. 5.4
Соединение абонентов сети Token-Ring в кольцо с помощью концентратора (MAU)

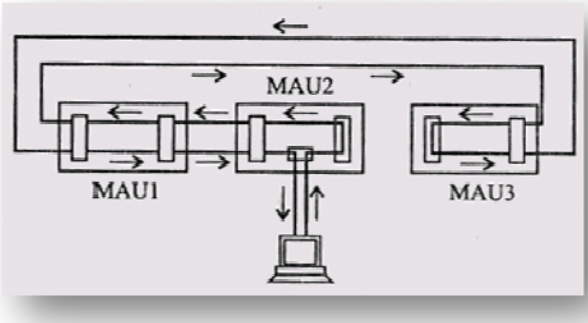


Рис. 5.5
Объединение концентраторов двунаправленной линией связи

Конструктивно концентратор представляет собой автономный блок с восемью разъемами для подключения абонентов (компьютеров) с помощью адаптерных кабелей и двумя (крайними) разъемами для подключения к другим концентраторам с помощью специальных магистральных кабелей (рис. 5.7). Существуют настенный и настольный варианты концентратора.

Несколько концентраторов могут конструктивно объединяться в группу, кластер (cluster), внутри которого абоненты также соединены в единое кольцо. Применение кластеров позволяет увеличивать количество абонентов, подключенных к одному центру (например, до 16, если в кластер входит два концентратора).

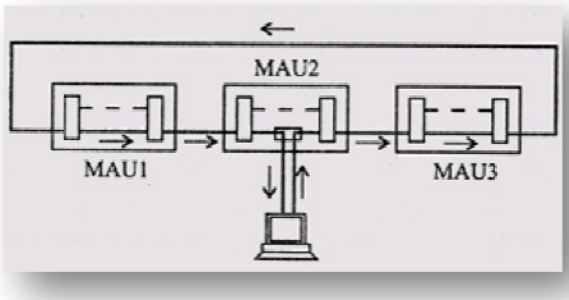


Рис. 5.6
Объединение концентраторов однонаправленной линией связи

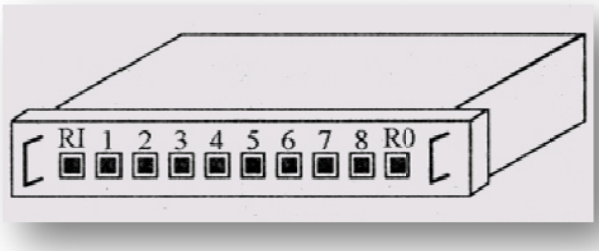


Рис. 5.7
Концентратор Token-Ring (8228 MAU)

В качестве среды передачи в сети IBM Token-Ring сначала применялась витая пара, но затем появились варианты аппаратуры для коаксиального кабеля, а также для оптоволоконного кабеля в стандарте FDDI. Витая пара применяется как неэкранированная (UTP), так и экранированная (STP).

Основные технические характеристики сети Token-Ring следующие.

Максимальное количество концентраторов типа IBM 8228 MAU — 12.

Максимальное количество абонентов в сети — 96.

Максимальная длина кабеля между абонентом и концентратором — 45 м.

Максимальная длина кабеля между концентраторами -45м.

Максимальная длина кабеля, соединяющего все концентраторы — 120м.

Скорость передачи данных — 4 Мбит/с и 16 Мбит/с.

Все приведенные характеристики относятся к случаю неэкранированной витой пары. В случае применения другой среды передачи характеристики сети могут отличаться. Например, при использовании экранированной витой пары количество абонентов может быть увеличено до 260 (вместо 96), длина кабеля — до 100 м (вместо 45), количество концентраторов -до 33, а полная длина кольца, соединяющего концентраторы — до 200 м. Оптоволоконный кабель позволяет увеличивать длину кабеля до 1 км.

Как видим, сеть Token-Ring уступает сети Ethernet как по допустимому размеру сети, так и по максимальному количеству абонентов. Что касается скорости передачи, то в настоящее время ведется разработка версий Token-Ring на скорость 100 Мбит/с и на 1000 Мбит/с. Фирма IBM вовсе не собирается отказываться от своей сети, рассматривая ее как достойного конкурента Ethernet.

Для передачи информации в Token-Ring используется вариант кода Ман-честер-П. Как и в любой звездообразной топологии, никаких дополнительных мер по электрическому согласованию и внешнему заземлению не требуется.

Для присоединения кабеля к сетевому адаптеру используется внешний 9-контактный разъем типа DIN. Так же, как и адаптеры Ethernet, адаптеры Token-Ring имеют на своей плате переключатели или перемычки для настройки адресов и прерываний системной шины. Если сеть Ethernet можно построить только на адаптерах и кабеле, то для сети Token-Ring обязательно нужно приобретать концентраторы. Это также увеличивает стоимость аппаратуры Token-Ring.

В то же время в отличие от Ethernet сеть Token-Ring лучше держит большую нагрузку (больше 30-40%) и обеспечивает гарантированное время доступа. Это крайне необходимо, например, в сетях производственного назначения, в которых задержка реакции на внешнее событие может привести к серьезным авариям.

В сети Token-Ring используется классический маркерный метод доступа, то есть по кольцу постоянно циркулирует маркер, к которому абоненты могут присоединять свои пакеты данных. Отсюда следует такое важное достоинство данной сети, как отсутствие конфликтов, но отсюда же следуют такие недостатки, как необходимость контроля за целостностью маркера и зависимость функционирования сети от каждого из абонентов (в случае неисправности абонент обязательно должен быть исключен из кольца).

Для контроля за целостностью маркера используется один из абонентов (так называемый активный монитор). Его аппаратура ничем не отличается от остальных, но его программные средства следят за временными соотношениями в сети и формируют в случае необходимости новый маркер. Активный монитор выбирается при инициализации сети, им может быть любой компьютер сети. Если активный монитор по какой-то причине выходит из строя, то включается специальный механизм, посредством которого другие абоненты (запасные мониторы) принимают решение о назначении нового активного монитора.

Маркер представляет собой управляющий пакет, содержащий всего три байта (рис. 5.8): байт начального разделителя (SD — Start Delimiter), байт управления доступом (AC — Access Control) и байт конечного разделителя (ED — End Delimiter). Начальный разделитель и конечный разделитель представляют собой не просто последовательность нулей и единиц, а содержат импульсы специального вида. Благодаря этому данные разделители нельзя спутать ни с какими другими байтами пакетов. Четыре бита разделителя представляют собой нулевые биты в принятой кодировке, а четыре других бита не соответствуют коду Манчестер-П: в течение двух битовых интервалов удерживается один уровень сигнала, а в течение двух остальных — другой уровень. В результате такой сбой синхронизации легко выявляется приемником.

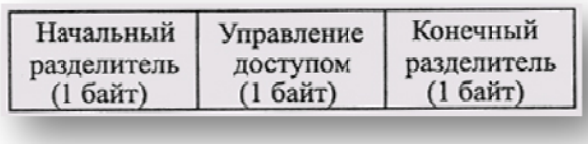


Рис. 5.8
Формат маркера сети Token-Ring

Рис. 5.9
Формат байта управления доступом

Байт управления разделен на четыре поля (рис. 5.9): три бита приоритета, бит маркера, бит монитора и три бита резервирования. Биты приоритета позволяют абоненту присваивать приоритет своим пакетам или маркеру (приоритет может быть от 0 до 7, причем 7 соответствует наивысшему приоритету, а 0 — наинизшему). Абонент может присоединить к маркеру свой пакет только тогда, когда его собственный приоритет такой же или выше приоритета маркера. Бит маркера определяет, присоединен ли к маркеру пакет (единица соответствует маркеру без пакета, нуль — маркеру с пакетом). Бит монитора, установленный в единицу, говорит о том, что данный маркер передан активным монитором. Биты резервирования позволяют абоненту зарезервировать свое право на дальнейший захват сети, то есть, так сказать, занять очередь на обслуживание. Если приоритет абонента выше, чем текущее значение поля резервирования, он может записать туда свой приоритет вместо прежнего.

Формат пакета Token-Ring представлен на рис. 5.10. Помимо начального и конечного разделителей, а также байта управления доступом, в пакет входят также байт управления пакетом, сетевые адреса приемника и передатчика, данные, контрольная сумма и байт состояния,пакета.

Рис. 5.10
Формат пакета сети Token-Ring (длина полей дана в байтах)

Назначение полей пакета следующее:

- Начальный разделитель (SD) является признаком начала пакета.
- Байт управления доступом (AC) имеет то же назначение, что и в маркере.
- Байт управления пакетом (FC — Frame Control) определяет тип пакета (кадра).

Шестибайтовые адреса отправителя и получателя пакета имеют стандартный формат, описанный в разделе 3.2.

Поле данных включает в себя передаваемую информацию или информацию управления обменом.

Поле контрольной суммы представляет собой 32-разрядную циклическую контрольную сумму пакета (CRC).

Конечный разделитель является признаком конца пакета. Кроме того, он определяет, является ли данный пакет промежуточным или заключительным в последовательности передаваемых пакетов, а также содержит признак ошибочности пакета (для этого выделены специальные биты).

Байт состояния пакета говорит о том, что происходило с данным пакетом: был ли он принят и скопирован в память приемника. По нему отправитель пакета узнает, дошел ли пакет по назначению и без ошибок или его надо передавать заново.

Отметим, что больший допустимый размер передаваемых данных в одном пакете по сравнению с сетью Ethernet может стать решающим фактором для увеличения производительности сети. Теоретически для скорости передачи 16 Мбит/с длина поля данных может достигать даже 18 Кбайт, что очень важно при передаче больших объемов данных. Но даже при скорости 4 Мбит/с благодаря маркерному методу доступа сеть Token-Ring часто обеспечивает большую фактическую скорость передачи, чем более быстрая сеть Ethernet (10 Мбит/с), особенно при больших нагрузках (свыше 30—40%), когда заметно сказывается несовершенство метода CSMA/CD, который в этом случае тратит много времени на разрешение повторных конфликтов.

Помимо маркера и обычного пакета, в сети Token-Ring может передаваться специальный управляющий пакет, служащий для прерывания передачи. Он может быть послан в любой момент и в любом месте потока данных. Пакет этот состоит всего из двух однобайтовых полей — начального и конечного разделителей описанного формата.

Интересно, что в более быстрой версии Token-Ring (16 Мбит/с и выше) применяется так называемый метод раннего формирования маркера (ETR -Early Token Release). Он позволяет избежать непроизводительного использования сети в то время, пока пакет данных не вернется по кольцу к своему отправителю. Метод ETR сводится к тому, что сразу после передачи своего пакета, присоединенного к маркеру, любой абонент выдает в сеть новый свободный маркер, то есть все другие абоненты могут начинать передачу своих пакетов сразу же после окончания пакета предыдущего абонента, не дожидаясь, пока он завершит обход всего кольца сети.

5.3. Сеть Arcnet

Сеть Arcnet (или ARCnet, от англ. Attached Resource Computer Net) — это одна из старейших сетей. Она была разработана фирмой Datapoint Corporation еще в 1977 году. Международные стандарты на эту сеть отсутствуют, хотя именно она считается родоначальницей метода маркерного доступа. Несмотря на отсутствие стандартов, сеть Arcnet до недавнего времени пользовалась довольно большой популярностью, даже серьезно конкурировала с Ethernet. Большое количество фирм (например, Datapoint, Standard Microsystems, Xircom и др.) производили аппаратуру для сети этого типа, но сейчас производство аппаратуры Arcnet практически прекращено.

Среди основных достоинств сети Arcnet можно назвать высокую надежность и гибкость, простоту диагностики аппаратных неисправностей, меньшие по сравнению с Ethernet ограничения на общую длину сети (на обычном тонком коаксиальном кабеле), а также сравнительно низкую стоимость адаптеров. Из недостатков сети наиболее существенным является низкая скорость передачи информации (всего лишь 2,5 Мбит/с).

Для передачи информации в сети Arcnet используется довольно редкий код, в котором логической единице соответствуют два импульса в течение битового интервала, а логическому нулю — один импульс. Очевидно, что такой код относится к самосинхронизирующимся, но он требует еще большей пропускной способности кабеля, чем даже Манчестер-П.

В качестве топологии сеть Arcnet использует шину (Arcnet-BUS) и пассивную звезду (Arcnet-STAR). Они показаны на рис 5.11 и 5.12.

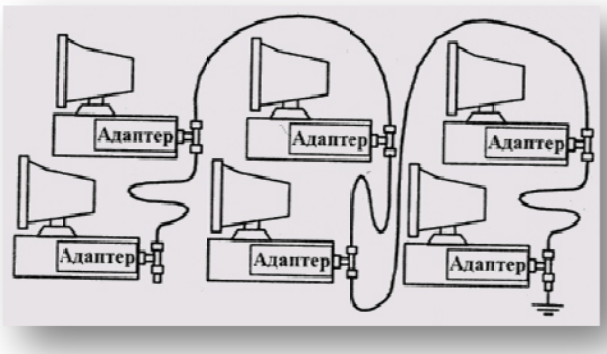


Рис. 5.11
Топология сети Arcnet типа «шина»

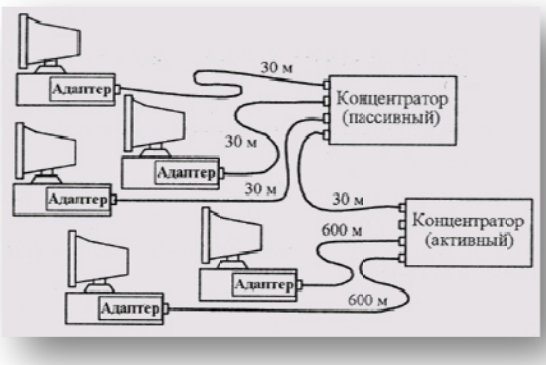


Рис. 5.12
Топология сети Arcnet типа «пассивная звезда»

Оборудование для топологии «шина» практически ничем не отличается от аналогичного, применяемого в сети Ethernet на тонком коаксиальном кабеле (10BASE2). Здесь точно так же используются Т-коннекторы и BNC-разъемы, а также терминаторы с заземлением и без него. Единственное, но важное отличие состоит в том, что в данном случае кабель должен быть с волновым сопротивлением 93 Ом, например, марки RG-62A/U, а не 50-омным, как в Ethernet. Соответственно 93-омными должны быть и согласующие терминаторы. Несмотря на большое сходство оборудования, кабельные системы Ethernet и Arcnet несовместимы между собой, и в случае перехода, например, с Arcnet на Ethernet, все кабели придется проложить заново. В связи с резким сокращением выпуска сетей Arcnet эта задача становится довольно актуальной для тех, кто ориентировался на эту сеть.

В случае топологии «пассивная звезда» (или «пассивное дерево», то есть при нескольких концентраторах, объединенных между собой) применяются концентраторы двух типов: активные (которые ретранслируют принимаемые сигналы перед передачей другим абонентам) и пассивные (без ретрансляции). Концентраторы рассчитаны на 4, 8, 16 и 32 канала. 4-ка-нальные концентраторы обычно выполняются в виде платы расширения для компьютера, 8- и 16-канальные — как правило, в виде отдельных конструктивных блоков с собственными источниками питания, что определяет их значительно большую стоимость.

Активные концентраторы используются также и при создании топологии шина. В этом случае к каждому порту концентратора подключается сегмент шины с несколькими абонентами (не более 8). Минимальное расстояние между абонентами в шине составляет 1 м. Отметим, что для топологий шина и звезда применяются различные адаптеры (правда, существуют и адаптеры с возможностью работы как в шине, так и в звезде).

Основные технические характеристики сети Arcnet следующие.

Среда передачи — коаксиальный кабель, витая пара.

Максимальная длина сети — 6 км.

Максимальная длина кабеля от абонента до пассивного концентратора — 30 м.

Максимальная длина кабеля от абонента до активного концентратора — 600 м.

Максимальная длина кабеля между активным и пассивным концентраторами — 30 м.

Максимальная длина кабеля между активными концентраторами — 600 метров.

Максимальное количество абонентов в сети1 — 255.

Максимальное количество абонентов на шинном сегменте — 8.

Максимальная длина сегмента — 300 м.

Скорость передачи данных — 2,5 Мбит/с.

При создании сложных топологий необходимо следить, чтобы задержка распространения сигналов в сети не превышала 30 мкс. Максимальное затухание сигнала в кабеле на частоте 5 МГц не должно превышать 11 дБ.

Как видим, Arcnet уступает Ethernet по допустимому количеству абонентов сети, но в реальности любая сеть довольно редко объединяет больше сотни абонентов.

В сети Arcnet используется маркерный метод доступа (метод передачи права), но он несколько отличается от применяемого в сети Token-Ring. Ближе всего этот метод к тому, который предусмотрен в стандарте IEEE 802.4. Последовательность действий абонентов при данном методе следующая:

Абонент, желающий передавать, ждет прихода маркера.

Получив маркер, он посылает запрос на передачу приемнику информации (то есть спрашивает, готов ли приемник принять его пакет).

Приемник, получив запрос, посылает ответ (то есть подтверждает свою готовность).

Получив подтверждение готовности, передатчик посылает свой пакет.

Получив пакет, приемник посылает подтверждение приема пакета.

Передатчик, получив подтверждение приема пакета, посылает маркер следующему абоненту.

Таким образом, в данном случае пакет передается только тогда, когда есть уверенность в готовности приемника принять его. Это существенно увеличивает надежность передачи. Так же, как и в случае Token-Ring, конфликты в Arcnet полностью исключены. Как и любая маркерная сеть, Arcnet хорошо держит нагрузку и гарантирует величину времени доступа к сети (в отличие от Ethernet). Другое дело, что невысокая пропускная способность сети (2,5 Мбит/с) в принципе не позволяет передавать больших потоков информации, но для небольших сетей, тем более с разовыми случайными передачами, этого часто и не требуется. Отметим также, что маркер передается в данном случае по логическому кольцу, хотя физическая топология сети не кольцевая, а шинная.

Размер пакета сети Arcnet составляет 0,5 Кб. Помимо данных в него входят также 8-битные адреса приемника и передатчика и 16-битная циклическая контрольная сумма (CRC).

Адаптеры сети Arcnet чаще всего выпускаются в виде плат расширения компьютера. Точно так же, как и адаптеры других сетей, перед установкой в компьютер они требуют настройки: выбора адресов портов и номера прерывания. Помимо этой общей настройки на каждой плате адаптера Arcnet необходимо с

помощью переключателей или перемычек установить свой собственный сетевой адрес (всего их может быть 255, так как последний, 256-ой адрес применяется в сети для режима широкого вещания).

Существовали варианты сети Arcnet, рассчитанные на скорость передачи 20 Мбит/с, но они не получили широкого распространения.

5.4. Сеть FDDI

Сеть FDDI (от английского Fiber Distributed Data Interface, оптоволоконный распределенный интерфейс данных) — это одна из новейших разработок стандартов локальных сетей. Стандарт FDDI, предложенный Аме

риканским национальным институтом стандартов ANSI (спецификация ANSI X3T9.5), изначально ориентировался на высокую скорость передачи (100 Мбит/с) и на применение перспективного оптоволоконного кабеля (длина волны света — 850 нм). Поэтому в данном случае разработчики не были стеснены рамками стандартов, ориентировавшихся на низкие скорости и электрический кабель.

Выбор оптоволокна в качестве среды передачи определил такие преимущества новой сети, как высокая помехозащищенность, максимальная секретность передачи информации и прекрасная гальваническая развязка абонентов. Высокая скорость передачи, которая в случае оптоволоконного кабеля достигается гораздо проще, позволяет решать многие задачи, недоступные менее скоростным сетям, например, передачу изображений в реальном масштабе времени. Кроме того, оптоволоконный кабель легко решает проблему передачи данных на расстояние нескольких километров без ретрансляции, что позволяет строить гораздо большие по размерам сети, охватывающие даже целые города и имеющие при этом все преимущества локальных сетей (в частности, низкий уровень ошибок). И хотя к настоящему времени аппаратура FDDI не получила еще широкого распространения, ее перспективы очень неплохие.

За основу стандарта FDDI был взят метод маркерного доступа, предусмотренный международным стандартом IEEE 802.5 Token-Ring. Небольшие отличия от этого стандарта определяются необходимостью обеспечить высокую скорость передачи информации на большие расстояния. Топология сети FDDI — это кольцо, причем применяется два разнонаправленных оптоволоконных кабеля, что позволяет в принципе использовать полнодуплексную передачу информации с удвоенной эффективной скоростью в 200 Мбит/с (при этом каждый из двух каналов работает на скорости 100 Мбит/с). Применяется и звездно-кольцевая топология с концентраторами, включенными в кольцо.

Основные технические характеристики сети FDDI следующие.

Максимальное количество абонентов сети — 1000.

Максимальная протяженность кольца сети — 20 км.

Максимальное расстояние между абонентами сети — 2 км.

Среда передачи — многомодовый оптоволоконный кабель (возможно применение электрической витой пары).

Метод доступа — маркерный.

Скорость передачи информации — 100 Мбит/с (200 Мбит/с для дуплексного режима передачи).

Как видим, FDDI имеет большие преимущества по сравнению со всеми рассмотренными ранее сетями. Даже сеть Fast Ethernet, имеющая такую же пропускную способность 100 Мбит/с, не может сравниться с FDDI по допустимым размерам сети и допустимому количеству абонентов. К тому же маркерный метод доступа FDDI обеспечивает в отличие от CSMA/CD гарантированное время доступа и отсутствие конфликтов при любом уровне нагрузки.

Отметим, что ограничение на общую длину сети в 20 км связано не с затуханием сигналов в кабеле, а с необходимостью ограничения времени полного прохождения сигнала по кольцу для обеспечения предельно допустимого времени доступа. А вот максимальное расстояние между абонентами (2 км при многомодовом кабеле) определяется как раз затуханием сигналов в кабеле (оно не должно превышать 11 дБ). Предусмотрена также возможность применения одномодового кабеля, и в этом случае расстояние между абонентами может достигать 45 километров, а полная длина кольца — 100 километров.

Имеется и реализация FDDI на электрическом кабеле (CDDI — Copper Distributed Data Interface или TPDDI — Twisted Pair Distributed Data Interface). При этом используется кабель категории 5 с разъемами RJ-45. Максимальное расстояние между абонентами в этом случае должно быть не более 100 м. Стоимость оборудования сети на электрическом кабеле в несколько раз меньше. Но эта версия сети уже не имеет столь очевидных преимуществ перед своими конкурентами, как изначальная FDDI.

Таблица 5.1. Код 4B/5B

Информация	Код4B/5B	Информация	Код4B/5B
0000	НПО	1000	10010
0001	01001	1001	10011
0010	10100	1010	10110

ООП	10101	1011	10111
0100	01010	1100	Пою
0101	01011	1101	поп
0110	01110	1110	11100
0111	01111	1111	11101

Для передачи данных в FDDI применяется уже упоминавшийся в первой главе код 4B/5B (см. табл. 5.1), специально разработанный для этого стандарта. Он обеспечивает скорость передачи 100 Мбит/с при пропускной способности кабеля 125 миллионов сигналов в секунду (или 125 МБод), а не 200 МБод, как в случае кода Манчестер-П. При этом каждым четырем битам передаваемой информации (каждому полубайту, или нибблу) ставится в соответствие пять передаваемых по кабелю битов. Это позволяет приемнику восстанавливать синхронизацию приходящих данных один раз на четыре принятых бита, то есть достигается компромисс между простейшим кодом NRZ и самосинхронизирующимся на каждом бите коде Манчестер-И.

Стандарт FDDI для достижения высокой гибкости сети предусматривает включение в кольцо абонентов двух типов.

Attachment Stations) подключаются к обоим (внутреннему и внешнему) кольцам сети. При этом реализуется возможность обмена со скоростью до 200 Мбит/с или же возможность резервирования кабеля сети (при повреждении основного кабеля используется резервный кабель). Аппаратура этого класса используется в самых критичных частях сети.

Абоненты (станции) класса B (они же абоненты одинарного подключения, SAS — Single-Attachment Stations) подключаются только к одному (внешнему) кольцу сети. Естественно, они могут быть более простыми и дешевыми, чем адаптеры класса A, но не имеют их возможностей. В сеть они могут включаться только через концентратор или обходной коммутатор, отключающий их в случае аварии.

Кроме собственно абонентов (компьютеров, терминалов и т.д.), в сети используются связные концентраторы (Wiring Concentrators), включение которых позволяет собрать в одно место все точки подключения с целью контроля за работой сети, диагностики неисправностей и упрощения реконфигурации. При применении кабелей разных типов (например, оптоволоконного кабеля и витой пары) концентратор выполняет также функцию преобразования электрических сигналов в оптические и наоборот. Концентраторы также бывают двойного подключения (DAC — Dual-Attachment Concentrator) и одинарного подключения (SAC — Single-Attachment Concentrator).

Пример простейшей конфигурации сети FDDI представлен на рис. 5.13.

FDDI определяет четыре типа портов абонентов (станций).

Порт A определен только для устройств двойного подключения, его вход подключается к первичному кольцу, а выход — к вторичному.

Порт B определен только для устройств двойного подключения, его вход подключается к вторичному кольцу, а выход — к первичному.

Порт M (Master) определен для концентраторов и соединяет два концентратора между собой или концентратор с абонентом.

Порт S (Slave) определен только для устройств одинарного подключения и используется для соединения двух абонентов или абонента и концентратора.

Стандарт FDDI предусматривает также возможность реконфигурации сети с целью сохранения ее работоспособности в случае повреждения кабеля (рис. 5.14). В показанном на рисунке случае поврежденный участок кабеля исключается из кольца, но целостность сети при этом не нарушается вследствие перехода на одно кольцо вместо двух (то есть абоненты класса A начинают работать как абоненты класса B).

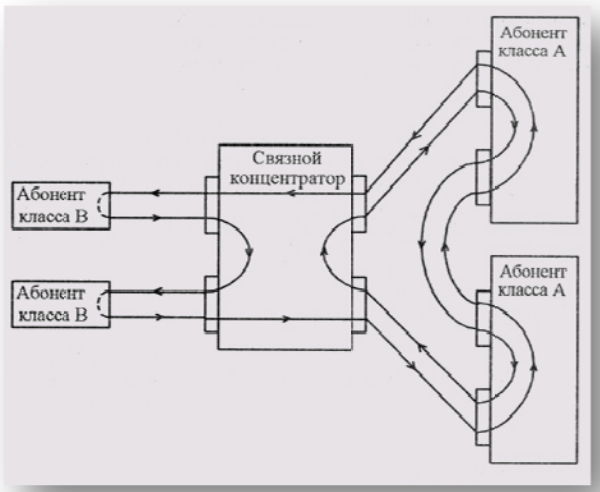


Рис. 5.13
Пример конфигурации сети FDDI

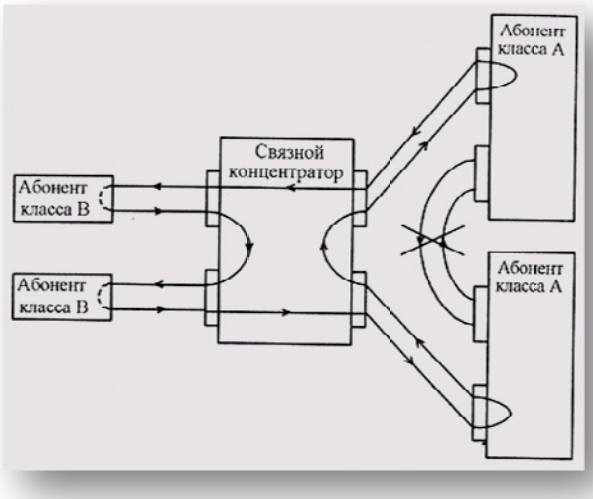


Рис. 5.14
Реконфигурация сети FDDI при повреждении кабеля

В отличие от метода доступа, предлагаемого стандартом IEEE 802.5, в FDDI применяется так называемая множественная передача маркера. Если в случае сети Token-Ring новый (свободный) маркер передается абонентом только после возвращения к нему его пакета, то в FDDI новый маркер передается абонентом сразу же после окончания передачи им пакета. Последовательность действий здесь следующая.

Абонент, желающий передавать, ждет маркера, который идет за каждым пакетом.

Когда маркер пришел, абонент удаляет его из сети и передает свой пакет.

Сразу после передачи пакета абонент посылает новый маркер.

Одновременно каждый абонент ведет свой отсчет времени, сравнивая реальное время обращения маркера (TRT) с заранее установленным контрольным временем его прибытия (PTT). Если маркер возвращается раньше, чем установлено PTT, то делается вывод, что сеть загружена мало, и, следовательно, абонент может спокойно передавать всю свою информацию. Если же маркер возвращается позже, чем установлено PTT, то сеть загружена сильно, и абонент может передавать только самую необходимую информацию. При этом величины контрольного времени PTT могут устанавливаться различными для разных абонентов. Такой механизм позволяет абонентам гибко реагировать на загрузку сети и автоматически поддерживать ее на оптимальном уровне.

Стандарт FDDI в отличие от стандарта IEEE 802.5 не предусматривает возможности установки приоритетов пакетов и резервирования. Вместо этого все абоненты разделяются на две группы: асинхронные и синхронные. Асинхронные абоненты — это те, для которых время доступа к сети не слишком критично. Синхронные — это те, для которых время доступа должно быть жестко ограничено. В стандарте предусмотрен специальный алгоритм, обслуживающий эти типы абонентов.

Форматы маркера (рис. 5.15) и пакета (рис. 5.16) сети FDDI несколько отличаются от форматов, используемых в сети Token-Ring. Назначение полей следующее.

Преамбула используется для синхронизации. Первоначально она содержит 64 бита, но абоненты, через которых проходит пакет, могут менять ее размер.

Начальный разделитель выполняет функцию признака начала кадра.

Адреса приемника и источника могут быть 6-байтовыми (аналогично Ethernet и Token-Ring) или 2-байтовыми.

Поле данных может быть переменной длины, но суммарная длина пакета не должна превышать 4500 байт.

Поле контрольной суммы содержит 32-битную циклическую контрольную сумму пакета.

Конечный разделитель определяет конец кадра.

Байт состояния пакета включает в себя бит обнаружения ошибки, бит распознавания адреса и бит копирования (все аналогично Token-Ring).

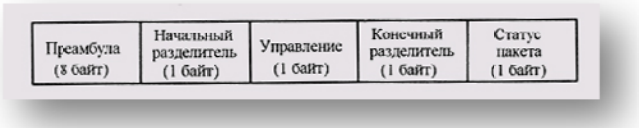


Рис. 5.15
Формат маркера FDDI

Рис. 5.16
Формат пакета FDDI

Формат байта управления сети FDDI следующий (рис. 5.17):

- Бит класса пакета определяет, синхронный или асинхронный это пакет.
- Бит длины адреса определяет, какой адрес (6-байтовый или 2-байтовый) используется в данном пакете.
- Поле формата кадра определяет, управляющий это кадр или информационный.
- Поле типа кадра определяет, к какому типу относится данный кадр.

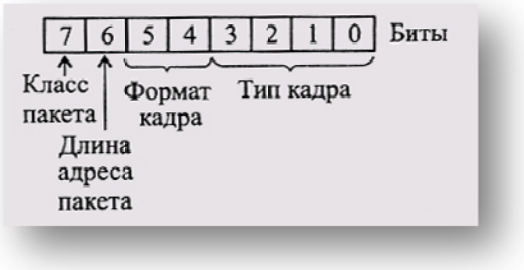


Рис. 5.17
Формат байта управления

В заключение отметим, что несмотря на очевидные преимущества FDDI данная сеть не получила пока широкого распространения, что связано главным образом с высокой стоимостью ее аппаратуры (порядка тысячи долларов). Основная область применения FDDI сейчас — это базовые, опорные (Backbone) сети, объединяющие несколько сетей. Применяется FDDI и для соединения мощных рабочих станций или серверов, требующих высокоскоростного обмена. Предполагается, что сеть Fast Ethernet может потеснить FDDI, однако преимущества оптоволоконного кабеля, маркерного метода управления и рекордный допустимый размер сети ставят в настоящее время FDDI вне конкуренции. А в тех случаях, когда стоимость аппаратуры имеет решающее значение, можно на некритичных участках применять версию FDDI на основе витой пары (TPDDI). К тому же стоимость аппаратуры FDDI может сильно уменьшится с увеличением объема ев выпуска.

5.5. Сеть 100VG-AnyLAN

Сеть lOOVG-AnyLAN — это одна из последних разработок высокоскоростных локальных сетей, недавно появившаяся на рынке. Она разработана фирмами Hewlett-Packard и IBM и соответствует стандарту IEEE 802.12, так что уровень ее стандартизации достаточно высокий. Главными достоинствами ее являются большая скорость обмена, сравнительно невысокая стоимость аппаратуры (примерно вдвое дороже по сравнению с наиболее популярной сетью Ethernet 10BASE-T), централизованный метод управления обменом без конфликтов и совместимость на уровне пакетов с популярными сетями Ethernet и Token-Ring. В названии сети цифра 100 соответствует скорости 100 Мбит/с, буквы VG обозначают дешевую витую пару категории 3 (Voice Grade), а AnyLAN (любая сеть) обозначает то, что сеть совместима с двумя самыми распространенными сетями.

Основные технические характеристики сети lOOVG-AnyLAN следующие.

Скорость передачи — 100 Мбит/с.

Топология — звезда с возможностью наращивания.

Метод доступа — централизованный, бесконфликтный (Demand Priority — с запросом приоритета).

Среда передачи — счетверенная неэкранированная витая пара (кабели UTP категории 3,4 или 5), сдвоенная витая пара (кабель UTP категории 5), сдвоенная экранированная витая пара (STP), а также оптоволоконный кабель. Сейчас в основном распространена счетверенная витая пара.

Максимальная длина кабеля между концентратором и абонентом и между концентраторами — 100 м (для UTP кабеля категории 3), 150 м (для UTP кабеля категории 5 и экранированного кабеля), 2 км (для оптоволоконного кабеля).

Таким образом, параметры сети 100VG-AnyLAN довольно близки к параметрам сети Fast Ethernet. Однако главное преимущество Fast Ethernet -это полная совместимость с наиболее распространенной сетью Ethernet (в случае lOOVG-AnyLAN для этого обязательно требуется коммутатор

или мост). В то же время, централизованное управление lOOVG-AnyLAN, исключающее конфликты и гарантирующее предельную величину времени доступа (чего не предусмотрено в сети Ethernet), также нельзя сбрасывать со счетов.

Пример структуры сети lOOVG-AnyLAN показан на рис. 5.18.

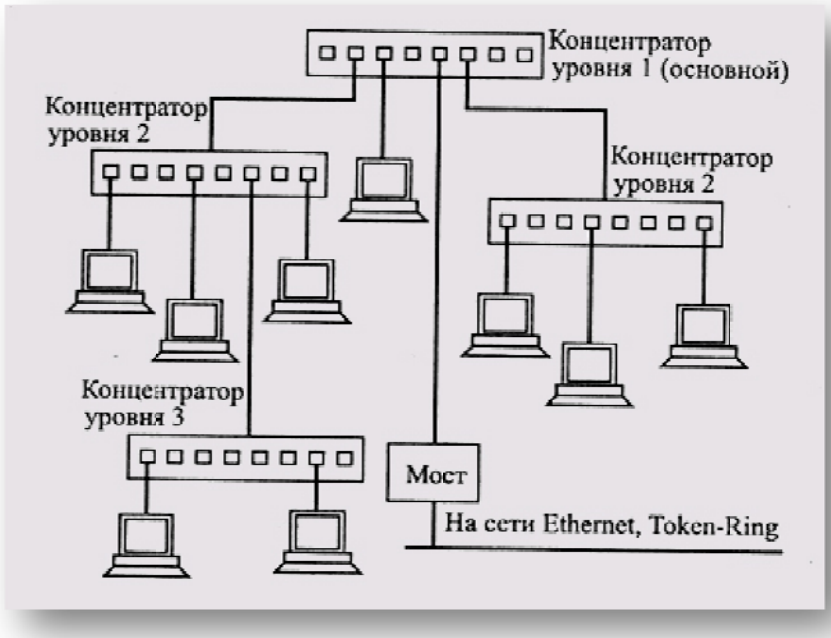


Рис. 5.18
Структура сети 10OVG-AnyLAN

Сеть lOOVG-AnyLAN состоит из центрального (основного) концентратора уровня 1, к которому могут подключаться как отдельные абоненты, так и концентраторы уровня 2, к которым в свою очередь подключаются абоненты и концентраторы уровня 3. При этом сеть может иметь не более трех таких уровней. Получается, что максимальный размер сети может составлять 600 метров для неэкранированной витой пары.

В отличие от неинтеллектуальных концентраторов других сетей (например, Ethernet), концентраторы сети lOOVG-AnyLAN — это интеллектуальные контроллеры, которые управляют всем доступом к сети. Для этого они непрерывно контролируют запросы, поступающие на все порты. Концентраторы принимают все приходящие пакеты и отправляют их только тем абонентам, которым они адресованы. Однако никакой обработки информации они не производят, то есть в данном случае получается все-таки не настоящая (активная) звезда, но и не пассивная звезда.

Каждый из концентраторов может быть настроен на работу с форматами пакетов Ethernet или пакетов Token-Ring. При этом концентраторы всей сети должны работать с пакетами только какого-нибудь одного формата. Для связи с сетями Ethernet и Token-Ring необходимы мосты, но мосты довольно простые.

Концентраторы имеют один порт верхнего уровня (для присоединения его к концентратору более высокого уровня) и несколько портов нижнего уровня (для присоединения абонентов). В качестве абонента может выступать компьютер (рабочая станция), сервер, мост, маршрутизатор, коммутатор, а также другой концентратор.

Каждый порт концентратора может быть установлен в один из двух возможных режимов работы.

Нормальный режим предполагает пересылку абоненту, присоединенному к порту, тольк о пакетов, адресованных лично ему.

Мониторный режим предполагает пересылку абоненту, присоединенному к порту, всех пакетов, приходящих на концентратор. Этот режим позволяет одному из абонентов контролировать работу всей сети в целом (выполнять функцию мониторинга).

Метод доступа к сети lOOVG-AnyLAN довольно типичен для сетей с топологией «звезда» и состоит в следующем.

Каждый желающий передавать абонент посылает концентратору свой запрос на передачу. Концентратор циклически прослушивает всех абонентов по очереди и дает право передачи абоненту, следующему по порядку за тем, который закончил передачу. То есть величина времени доступа гарантирована. Но этот простейший алгоритм усложнен в сети lOOVG-AnyLAN, так как запросы могут иметь два уровня приоритета:

- нормальный уровень приоритета используется для обычных приложений;
- высокий уровень приоритета используется для приложений, требующих быстрого обслуживания.

Запросы с высоким уровнем приоритета обслуживаются раньше, чем запросы с нормальным приоритетом. Если приходит запрос высокого приоритета, то нормальный порядок обслуживания прерывается, и после окончания приема текущего пакета обслуживается запрос высокого приоритета. Если таких высокоприоритетных запросов несколько, то возврат к нормальной процедуре обслуживания происходит только после полной обработки всех этих запросов. При этом концентратор следит за тем, чтобы не была превышена установленная величина гарантированного времени доступа. Если высокоприоритетных запросов слишком много, то запросы с нормальным приоритетом автоматически переводятся им в ранг высокоприоритетных. Таким образом, даже низкоприоритетные запросы не будут ждать своей очереди слишком долго.

Концентраторы более низких уровней также анализируют запросы абонентов, присоединенных к ним, и в случае необходимости пересылают их запросы к концентратору более высокого уровня. За один раз концентратор более низкого уровня может передать концентратору более высокого уровня не один пакет (как обычный абонент), а столько пакетов, сколько абонентов присоединено к нему.

Так, для примера на рис. 5.19 в случае одновременного возникновения заявок на передачу у всех абонентов (компьютеров) порядок обслуживания будет такой: компьютер 1~2, затем 1-3, потом 2-1, 2-4, 2-8, и далее 1~6. Однако так будет только при одинаковом (нормальном) приоритете всех запросов. Если же, например, от компьютеров 1-2, 2-4 и 2-8 поступят высокоприоритетные запросы, то порядок обслуживания будет таким: 1-2,2-4,2-8,1-3,2-1,1-6.

Помимо собственно передачи пакетов и пересылки запросов на передачу, в сети применяется также специальная процедура подготовки к связи (Link Training), во время которой концентратор и абоненты обмениваются между собой управляющими пакетами. При этом проверяется правильность присоединения линий связи и их исправность. Одновременно концентратор получает информацию об особенностях абонентов, подклю

ченных к нему, об их назначении и их сетевых адресах. Запускается данная процедура самим абонентом при включении питания или после подключения к концентратору, а также автоматически при большом уровне ошибок.

Интересно решена в сети lOOVG-AnyLAN проблема кодирования передаваемых данных.

Вся передаваемая информация проходит следующие этапы обработки.

Разделение на квинтеты (группы по 5 бит).

Перемешивание, скремблирование (scrambling) полученных квинтетов.

Кодирование квинтетов специальным кодом 5B6B (этот код обеспечивает в выходной последовательности не более трех единиц или нулей подряд, что используется для детектирования ошибок).

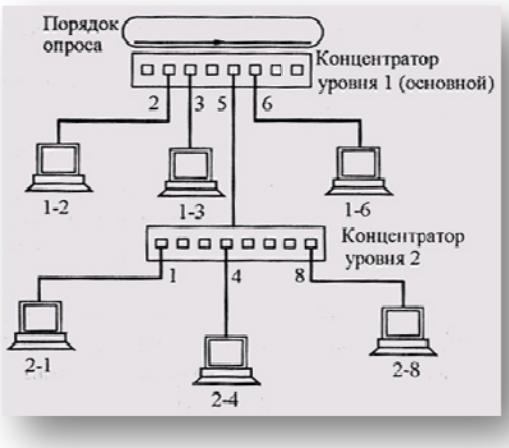


Рис. 5.19
Порядок обслуживания запросов абонентов на различных уровнях сети

Добавление начального и конечного разделителей кадра.

Сформированные таким образом кадры передаются в 4 линии передачи (при использовании счетверенной витой пары). При сдвоенной витой паре и оптоволоконном кабеле применяется временное мультиплексирование информации в каналах.

В результате этих действий достигается рандомизация сигналов, то есть выравнивание количества передаваемых единиц и нулей, снижение взаимовлияния кабелей друг на друга и самосинхронизация передаваемых сигналов без удвоения требуемой полосы пропускания, как в случае кода Манчестер-П.

В случае использования счетверенной витой пары передача по каждой из четырех витых пар производится со скоростью 30 Мбит/с (рис. 5.20). Суммарная скорость передачи составляет 120 Мбит/с. Однако полезная информация вследствие использования кода 5B6B передается при этом всего лишь со скоростью 100 Мбит/с. Таким образом, пропускная способность кабеля должна быть не менее 15 МГц. Этому требованию удовлетворяет кабель с витыми парами категории 3.

В сети 100 VG-AnyLAN предусмотрены два режима обмена: полудуплексный и полнодуплексный.

При полудуплексном обмене все четыре витые пары используются для передачи одновременно в одном направлении (от абонента к концентратору или наоборот). Он используется для передачи пакетов.

При полнодуплексном обмене две витые пары передают в одном направлении, а две другие — в другом направлении. Он используется для передачи управляющих сигналов.

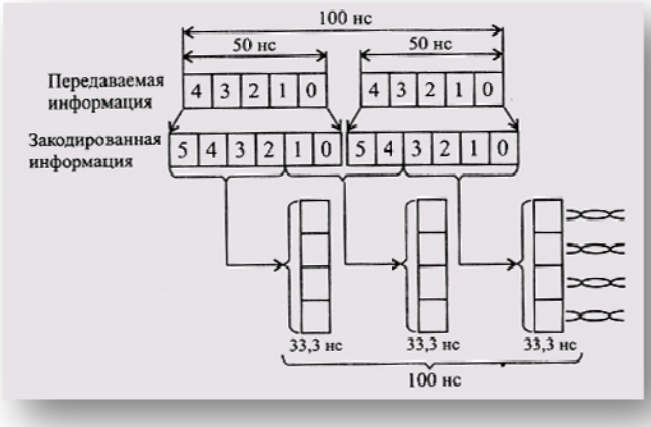


Рис. 5.20
Кодирование информации в сети 100VG-AnyLAN

Для управления используются два тональных сигнала. Первый из них представляет собой последовательность из 16 логических единиц и 16 логических нулей, следующих со скоростью 30 Мбит/с (в результате частота сигнала получается равной 0,9375 МГц). Второй тональный сигнал имеет вдвое большую частоту (1,875 МГц) и образуется чередованием восьми логических единиц и восьми логических нулей. Все управление сетью осуществляется комбинацией этих двух тональных сигналов.

Табл. 5.2. Расшифровка комбинаций управляющих тональных сигналов

Передаваемые сигналы	Расшифровка абонентом	Расшифровка концентратором
1 — 1	Нет информации для передачи	Нет информации для передачи
1 -2	Концентратор принимает пакет	Запрос нормального приоритета
2- 1	Зарезервировано	Высокоприоритетный запрос
2-2	Запрос процедуры подготовки к связи	Запрос процедуры подготовки к связи

В таблице 5.2 приведена расшифровка различных комбинаций этих сигналов, передаваемых абоненту и концентратору. Когда ни у абонента, ни у концентратора нет информации для передачи, оба они посылают по обеим линиям первый тоновый сигнал (1~1). Если принимаемый концентратором пакет может быть адресован данному абоненту, ему посылается комбинация сигналов 1-2. При этом абонент должен прекратить передачу управляющих сигналов концентратору и освободить эти две линии связи для пересылки информационных пакетов. Такая же комбинация (1 — 2), полученная концентратором, означает запрос на передачу пакета с нормальным приоритетом. Запрос на передачу пакета с высоким приоритетом передается комбинацией 2—1. Наконец, комбинация 2-2 сообщает как абоненту, так и концентратору о необходимости перейти к процедуре подготовки к связи.

Таким образом, сеть lOOVG-AnyLAN представляет собой довольно доступное решение для увеличения скорости передачи до 100 Мбит/с. Однако она не обладает полной совместимостью ни с одной из стандартных сетей, поэтому ее дальнейшая судьба проблематична. К тому же, в отличие от сети FDDI, она не имеет никаких рекордных параметров.

5.6. Сверхвысокоскоростные сети

Быстродействие сети Fast Ethernet, других сетей, работающих на скорости в 100 Мбит/с, в настоящее время удовлетворяет требованиям большинства задач, но в ряде случаев даже его оказывается недостаточно. Особенно это касается тех ситуаций, когда необходимо подключать к сети современные высокопроизводительные серверы или строить сети с большим количеством абонентов, требующих высокой интенсивности обмена. Например, все более широко применяется сетевая обработка трехмерных динамических изображений. Скорость компьютеров непрерывно растет, они обеспечивают все более высокие темпы обмена с внешними устройствами. В результате сеть может оказаться наиболее слабым местом системы, и ее пропускная способность будет основным сдерживающим фактором в увеличении быстродействия.

Работы по достижению скорости передачи в 1 Гбит/с (1000 Мбит/с) ведутся в последние годы довольно интенсивно в нескольких направлениях. Однако, скорее всего, наиболее перспективной окажется сеть Gigabit Ethernet. Это связано прежде всего с тем, что переход на нее окажется наиболее безболезненным, самым дешевым и психологически приемлемым. Ведь сеть Ethernet и ее более быстрая версия Fast Ethernet сейчас далеко опережают всех своих конкурентов по объему продаж и распространенности в мире.

Сеть Gigabit Ethernet — это естественный, эволюционный путь развития концепции, заложенной в стандартной сети Ethernet. Естественно, она наследует и все недостатки своих прямых предшественников, например, негарантированное время доступа к сети. Однако огромная пропускная способность приводит к тому, что загрузить сеть до тех уровней, когда этот фактор становится определяющим, довольно трудно. Зато сохранение преемственности позволяет довольно просто соединять сегменты Ethernet, Fast Ethernet и Gigabit Ethernet в единую сеть и, самое главное, переходить к новым скоростям постепенно, вводя гигабитные сегменты только на самых напряженных участках сети. (К тому же далеко не везде такая высокая пропускная способность действительно необходима.) Если же говорить о конкурирующих гигабитных сетях, то их применение может потребовать полной замены сетевой аппаратуры, что сразу же приведет к огромным затратам средств.

В сети Gigabit Ethernet сохраняется все тот же хорошо зарекомендовавший себя в предыдущих версиях метод доступа CSMA/CD, используются те же форматы пакетов (кадров) и те же размеры, то есть никакого преобразования протоколов в местах соединения с сегментами Ethernet и Fast Ethernet не потребуется. Единственно, что нужно, — это согласование скоростей обмена. Поэтому главной областью применения Gigabit Ethernet станет в первую очередь соединение концентраторов Ethernet и Fast Ethernet между собой.

С появлением сверхбыстродействующих серверов и распространением наиболее совершенных персональных компьютеров класса «high-end» преимущества Gigabit Ethernet будут становиться все более явными. Отметим, что 64-разрядная системная магистраль PCI, ставшая уже фактическим стандартом, вполне достигает требуемой для такой сети скорости передачи данных.

Работы по сети Gigabit Ethernet ведутся с 1995 года. В 1998 году принят стандарт, получивший наименование IEEE 802.3z. Разработкой занимается специально созданный альянс (Gigabit Ethernet Alliance), в который, в частности, входит такая известная фирма, занимающаяся сетевой аппаратурой, как 3Com.

Переход на такую огромную скорость передачи не столь прост, как может показаться. Для аппаратуры Gigabit Ethernet будут использоваться микросхемы, выполненные по самой современной 0,35-микронной технологии. Только они позволяют добиться требуемого быстродействия. Ожидается разработка 32-разрядного контроллера, имеющего и буферную память на кристалле, содержащем до миллиона логических элементов.

Номенклатура сегментов сети Gigabit Ethernet в настоящее время включает в себя следующие типы:

- 1000BASE-SX — сегмент на мультимодовом оптоволоконном кабеле с длиной волны светового сигнала 850 нм (длиной до 500 м).
- 1000BASE-LX — сегмент на мультимодовом (длиной до 500 м) и одномодовом (длиной до 2000 м) оптоволоконном кабеле с длиной волны светового сигнала 1300 нм.
- 1000BASE-CX — сегмент на экранированной витой паре (длиной до 25 м).
- 1000BASE-T — сегмент на счетверенной неэкранированной витой паре (длиной до 100 м).

Специально для сети Gigabit Ethernet предложен метод кодирования передаваемой информации 8B/10B, построенный по тому же принципу, что и код 4B/5B сети FDDI. Восьми битам информации, которую

нужно передать, ставится в соответствие 10 бит, передаваемых по сети. Этот код позволяет сохранять самосинхронизацию, легко обнаруживать несущую (факт передачи), но не требует удвоения полосы пропускания, как в случае кода Манчестер-П.

Для увеличения 512-битного интервала сети Ethernet, соответствующего минимальной длине пакета, (51,2 икс в сети Ethernet и 5,12 мкс в сети Fast Ethernet), разработаны специальные методы. В частности, минимальная длина пакета увеличена до 512 байт (4096 бит). В противном случае временной интервал 0,512 мкс чрезмерно ограничивал бы предельную длину сети Gigabit Ethernet. Все пакеты с длиной меньше 512 байт расширяются до 512 байт. Это требует дополнительной обработки пакетов.

Предполагается поддерживать передачу в сети Gigabit Ethernet как в полудуплексном режиме (с сохранением метода доступа CSMA/CD), так и в более быстром полнодуплексном режиме (как и в предшествующей сети Fast Ethernet).

Прежде всего Gigabit Ethernet, видимо, найдет применение в сетях, объединяющих компьютеры больших фирм, предприятий, которые располагаются в нескольких зданиях. Она позволит с помощью соответствующих коммутаторов, преобразующих скорости передачи, обеспечить каналы связи с высокой пропускной способностью между отдельными частями сложной сети (рис. 5.21) или линии связи коммутаторов со сверхбыстродействующими серверами (рис. 5.22).

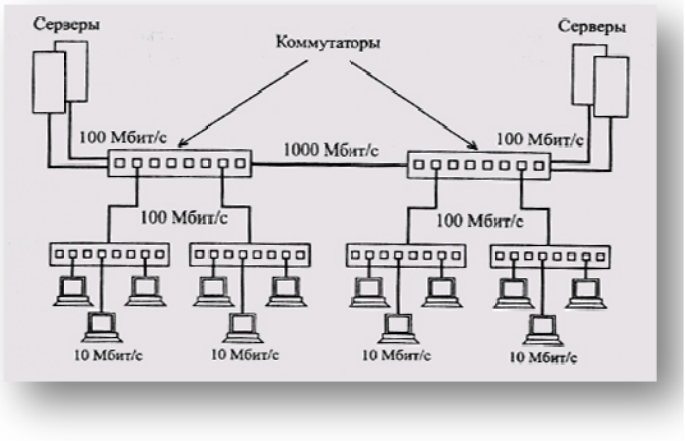


Рис. 5.21
Использование сети Gigabit Ethernet для соединения групп компьютеров

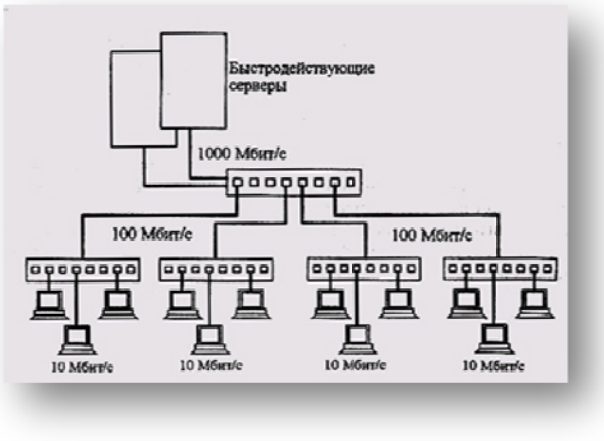


Рис. 5.22
Использование сети Gigabit Ethernet для подключения быстродействующих серверов

Вероятно, в ряде случаев Gigabit Ethernet будет вытеснять оптоволоконную сеть FDDI, которая в настоящее время все чаще используется для объединения в единую сеть нескольких локальных сетей, в том числе, и сетей Ethernet. Правда, FDDI может связывать абонентов, находящихся на гораздо большем расстоянии друг от друга, но по скорости передачи информации Gigabit Ethernet существенно превосходит FDDI.

Нас ждет принципиально важный прорыв в область скоростей передачи, еще недавно казавшихся фантастическими и даже, более того, никому не нужными. А там, возможно, появится и сеть со скоростью 10 000 Мбит/с, ведь такие разработки уже ведутся.

В заключение раздела несколько слов об альтернативном решении сверхбыстродействующей сети. Речь идет о сети с технологией ATM (Asynchronous Transfer Mode). Данная технология используется как в локальных, так и в глобальных сетях. Основная ее идея — передача цифровых, голосовых и мультимедийных данных по одним и тем же каналам. Строго говоря, жесткого стандарта на аппаратуру ATM не предполагает.

Первоначально была выбрана скорость передачи 155 Мбит/с (для настольных систем — 25 Мбит/с), затем — 662 Мбит/с, а сейчас ведутся работы по повышению скорости до 2488 Мбит/с. Как видим, по скорости ATM успешно конкурирует с Gigabit Ethernet. Кстати, появилась ATM раньше, чем Gigabit Ethernet.

В качестве среды передачи информации в локальной сети технология ATM предполагает использование оптоволоконного кабеля и неэкранированную витую пару. Используемые коды — 4B/5B и 8B/10B.

Принципиальное отличие ATM от всех остальных сетей состоит в отказе от привычных пакетов с полями адресации, управления и данных. Вся информация передается упакованной в микропакеты (ячейки, cells) длиной всего лишь в 53 бита. Каждая ячейка имеет идентификатор типа данных (двоичные данные, звук или изображение). Идентификатор позволяет интеллектуальным распределительным устройствам сортировать ячейки и следить за тем, чтобы ячейки передавались в нужной последовательности. Минимальный размер ячеек позволяет осуществлять коррекцию ошибок и маршрутизацию на аппаратном уровне. Он же обеспечивает равномерность всех существующих в сети информационных потоков.

Главный недостаток сетей с технологией ATM состоит в их полной несовместимости ни с одной из существующих сетей. Плавный переход на ATM в принципе невозможен, нужно менять сразу все

оборудование, а стоимость его пока что очень высока. Правда, работы по обеспечению совместимости ведутся, снижается и стоимость оборудования, так что перспективы у ATM неплохие. Тем более что задач по передаче изображений по компьютерным сетям становится все больше и больше.

Глава 6. Защита информации в локальных сетях

Содержание шестой главы:

6.1. Классические алгоритмы шифрования данных

В некоторых публикациях в периодической печати и в сети Internet под защитой информации понимается только часть из возможных и необходимых мероприятий в этом направлении, связанных с профилем работы конкретного коллектива исполнителей. Правильнее понимать под этим термином комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации и т.п. Поскольку, например, утрата информации может происходить по чисто «техническим», объективным и неумышленным причинам, под это определение попадают также и мероприятия, связанные с повышением надежности сервера из-за отказов или сбоев в работе винчестеров, недостатков в используемом программном обеспечении и т.д.

Вообще, переход от работы на персональных компьютерах к работе в сети усложняет защиту информации по следующим причинам.

Большое число пользователей в сети и их переменный состав. Защита на уровне имени и пароля пользователя недостаточна для предотвращения входа в сеть посторонних лиц.

Большая протяженность сети и наличие многих потенциальных каналов проникновения в сеть.

Уже упомянутые недостатки в аппаратном и программном обеспечении, которые зачастую обнаруживаются не на предприятия или организации). Преимущества организационных средств — возможность решения многих разнородных проблем, простота реализации, возможность быстрого реагирования на нежелательные действия в сети, неограниченные возможности модификации и развития. Недостатки — высокая зависимость от субъективных факторов, в том числе от общей организации работы в данном конкретном подразделении.

Шифрование данных представляет собой разновидность программных средств защиты информации и имеет особое значение на практике как единственная надежная защита информации, передаваемой по протяженным последовательным линиям, от утечки.

Понятие «шифрование» часто употребляется в связи с более общим понятием криптографии. Криптография включает шифрование и дополнительно рассматривает способы решения проблем, связанных с возможной подменой цифровых данных: как проверить достоверность цифровых данных и как по аналогии с рукописной подписью на бумаге проставить визу на электронных документах, имея в распоряжении лишь последовательности нулей и единиц. Эти проблемы и способы их решения будут рассмотрены далее.

Число используемых программ шифрования ограничено, причем часть из них являются стандартами де-факто или де-юре. Однако даже если алгоритм шифрования не представляет собой секрета, произвести дешифрование (или расшифровку) без знания закрытого ключа чрезвычайно сложно. Это свойство в современных программах шифрования обеспечивается в процессе многоступенчатого преобразования исходной открытой информации («plain text» в англоязычной литературе) с использованием ключа (или двух ключей — по одному для шифрования и дешифрования). В конечном счете каждый из используемых сложных методов (алгоритмов) шифрования представляет собой комбинацию относительно простых методов.

Различают следующие классические алгоритмы шифрования:

- подстановка (простая — одноаалфавитная, многоалфавитная однопетлевая, многоалфавитная многопетлевая);
- перестановка (простая, усложненная);
- гаммирование (смешивание с короткой, длинной или неограниченной маской).

Устойчивость каждого из перечисленных методов к дешифрованию бег знания ключа характеризуется количественно с помощью показателя S представляющего собой минимальный объем зашифрованного текста который может быть дешифрован посредством статистического анализа

Подстановка предполагает использование альтернативного алфавит; (или нескольких алфавитов) вместо исходного алфавита. В случае простой подстановки для символов английского алфавита можно предложить например, следующую замену (табл. 6.1).

Тогда слово «cache» в зашифрованном виде представляется как «usuxk»

Существует, однако, возможность дешифрования сообщения с помощьь известной статистической частоты повторяемости символов в произвольном, достаточно длинном тексте. Например, символ E встречается чащ всего — в среднем 123 раза на каждые 1000 символов или в 12,3% случаев далее следуют символы T — 9,6%, A — 8,1%, O — 7,9%, N — 1,2%, I — 7,2%, S — 6,6%, R — 6,0%, H — 5,1%, L — 4,0% и т.д. Приведенные цифры могут, конеч но, несколько варьироваться в зависимости от источника информацю Поэтому показатель устойчивости к дешифрованию SKB данном случа не превышает 20...30.

Табл. 6.1. Пример замены символов при подстановке

Исходный алфавит	A	B	C	D	E	F	G]	-I	i	J	K	L	X	Y	Z
Альтернативный алфавит	S	O	и	H	К	T	L :	X	N	W	м	Y	A	P	J

При многоалфавитной подстановке можно добиться того, что в зашифрс ванном тексте все символы будут встречаться примерно с одинаковс частотой, что существенно затруднит дешифрование без знания альте) нативных алфавитов и порядка, в котором они использовались при шифровании.

Перестановка потенциально обеспечивает большую по сравнению с по, становкой устойчивость к дешифрованию и выполняется с использов нием цифрового ключа или эквивалентного ключевого слова, как это п казано на следующем примере (см. табл. 6.2.).

Цифровой ключ состоит из неповторяющихся цифр, а соответствующ ему ключевое слово — из неповторяющихся символов. Исходный тек (plain text) записывается под ключом построчно. Зашифрованное сообщение (cipher text) выписывается по столбцам в том порядке, как это предписывают цифры ключа (или в том порядке, в котором расположены отдельные символы ключевого слова в алфавите).

Для рассматриваемого примера зашифрованное сообщение: TRANSPOSITION IS THE ENCIPHER METHOD будет выглядеть следующим образом: AIHHORTTPHPaEaaSNaRaTIalTOINMccNOEEDSSCEct.

Табл. 6.2. Пример использования простой перестановки (а — служебный символ, в данном случае означает пробел)

Ключевое слово	**S**	**E**	**C**	**и**	**R**	**I T**	**Y**
Цифровой ключ	5	2	1	7	4	3 6	8
Исходный текст (plain text), записанный построчно	T	R	A	N	S	P O	S
	I	T	I	O	N	a I	S"
	a	T	H	E	a	E N	C
	I	P	H	E	R	a M	E
	T	H	o	D	a	a a	a

Гаммирование (смешивание с маской) основано на побитном сложении по модулю 2 (или, что то же самое — в соответствии с логикой ИСКЛЮЧАЮЩЕЕ ИЛИ) исходного сообщения с заранее выбранной двоичной последовательностью (маской).

Компактным представлением маски могут служить числа в десятичной системе счисления или некоторый текст (в этом случае рассматривается внутренние коды символов — для английского текста таблица ASCII).

Операция суммирования по модулю 2 (ИСКЛЮЧАЮЩЕЕ ИЛИ) является обратимой, так что при сложении с той же маской (ключом) зашифрованного сообщения мы снова получим исходный текст (произойдет дешифрование).

В качестве маски (ключа) могут использоваться константы типа п или е, и тогда маска будет иметь конечную длину. Наибольшую устойчивость к дешифрованию может обеспечить использование маски с бесконечной длиной, которая образована генератором случайных (точнее, псевдослучайных) последовательностей. Такой генератор легко реализуется аппаратными или программными средствами, например, с помощью сдвигового регистра с обратными связями, который используется при вычислении помехоустойчивого циклического кода. Точное воспроизведение псевдослучайной последовательности в генераторе на приемном конце линии обеспечивается при установке такого же исходного состояния (содержимого сдвигового регистра) и той же структуры обратных связей, что и в генераторе на передающем конце.

Перечисленные классические методы шифрования (подстановка, перестановка и гаммирование) являются линейными в том смысле, что длина зашифрованного сообщения равна длине исходного текста.

Возможно нелинейное преобразование типа подстановки вместо исходных символов (или целых слов, фраз, предложений) заранее выбранных комбинаций символов другой длины.

Стандартные методы шифрования (национальные или международные) для повышения степени устойчивости к дешифрованию реализуют несколько этапов (шагов) шифрования, на каждом из которых используются различные классические методы шифрования в соответствии с выбранным ключом (или ключами). Существуют две принципиально различные группы стандартных методов шифрования:

- шифрование с использованием одних и тех же ключей (шифров) при шифровании и дешифровании (симметричное шифрование или системы с открытыми ключами — private-key systems);
- шифрование с использованием открытых ключей для шифрования и закрытых — для дешифрования (несимметричное шифрование).

Строгое математическое описание алгоритмов, используемых в стандартных методах шифрования, слишком сложно. Для пользователей важны в первую очередь потребительские свойства различных методов (степень устойчивости к дешифрованию, скорость шифрования и дешифрования, порядок и удобство распространения ключей), которые и рассматриваются ниже.

6.2. Стандартные методы шифрования

Стандарт шифрования данных США DES (Data Encryption Standard — стандарт шифрования данных) относится к группе методов симметричного шифрования и действует более 20 лет (принят в 1976 г.). Используемые операции — перестановка, гаммирование и нелинейная подстановка. Число шагов — 16. Длина ключа составляет 56 бит, из которых 8 бит — это проверочные разряды четности/нечетности.

Долгое время степень устойчивости к дешифрованию этого метода считалась достаточной, однако в 1998 г. появилось сообщение о создании специализированного компьютера (DES cracker), позволяющего вскрыть зашифрованный текст максимум за 9 дней (см. http://www.eff.org/ descracker). Впрочем, такого рода сообщения можно отнести и к одному из проявлений конкурентной борьбы.

Отечественный ГОСТ28147-89 — это аналог DES, но с длиной ключа 256 бит, так что его степень устойчивости к дешифрованию изначально существенно выше. Важно также и то, что в данном случае предусматривается целая система защиты, которая преодолевает «родовой» недостаток симметричных методов шифрования — возможность подмены сообщений. Такие усовершенствования, как имитовставки, хэш-функции и электронные цифровые подписи позволяют «авторизовать» передаваемые сообщения. Достоинством симметричных методов шифрования является высокая скорость шифрования и дешифрования, недостатком — малая степень защиты в случае, если ключ стал доступен третьему лицу.

Достаточно популярны, особенно при использовании электронной почты в сети Internet, несимметричные методы шифрования или системы с открытыми ключами — public-key systems. Типичный представитель этой группы методов — PGP (Pretty Good Privacy — достаточно хорошая секретность).

Каждый пользователь в этом случае имеет пару ключей. Открытые ключи предназначены для шифрования и свободно рассылаются по сети, но не позволяют произвести дешифрование. Для этого нужны секретные (закрытые) ключи.

Принцип шифрования в данном случае основывается на использовании так называемых односторонних функций. Прямая функция x -» f (x) легко вычисляется на основании открытого алгоритма (ключа). Обратное

преобразование f (x) —> x без знания закрытого ключа затруднено и должно занимать достаточно большое время, которое и определяет степень «трудновычислимости» односторонней функции.

Идею системы с открытыми ключами можно пояснить следующим образом (табл. 6.3). Для шифрования сообщений можно использовать обычную телефонную книгу, в которой имена абонентов расположены в алфавитном порядке и предшествуют телефонным номерам. Берется имя абонента, начинающееся на данную букву исходного слова, и номер телефона используется в качестве шифрованного сообщения.

Табл. 6.3. Пример шифрования в системе с открытыми ключами

Исходное слово	Выбранное имя абонента	Зашифрованное сообщение (телефонные номера)
S	Scott	3541920
A	Adleman	4002132
и	Ullman	7384502
N	Nivat	5768115

A	Aho	7721443

Понятно, что у пользователя имеется возможность выбора соответствия между символом в исходном тексте и именем абонента, т.е. это многоалфавитная система, что повышает ее степень устойчивости к дешифрованию. Легальный пользователь имеет «обратный» телефонный справочник, в котором в первом столбце располагаются телефонные номера по возрастанию, и легко производит дешифрование. Если же такого «обратного» справочника нет, то пользователю предстоит утомительное и многократное просматривание доступного прямого справочника в поисках нужных телефонных номеров. Это и есть практическая реализация трудновычислимой функции. Сам по себе метод шифрования на основе телефонных справочников вряд ли перспективен хотя бы из-за того, что никто не мешает потенциальному взломщику составить «обратный» телефонный справочник. Однако в используемых на практике методах шифрования данной группы в смысле надежности защиты все обстоит благополучно.

В отличие от симметричных методов шифрования, проблема рассылки ключей в несимметричных методах решается проще — пары ключей (открытый и закрытый) генерируются «на месте» с помощью специальных программ. Для рассылки открытых ключей используются специальные

технологии типа LDAP (Lightweight Directory Access Protocol — протокол облегченного доступа к справочнику). Рассылаемые ключи могут быть предварительно зашифрованы с помощью одного из симметричных методов шифрования.

6.3. Программные средства защиты информации

Встроенные средства защиты информации в сетевых ОС доступны, но не всегда, как уже отмечалось, могут полностью решить возникающие на практике проблемы. Например, сетевые ОС NetWare 3.x, 4.x позволяют осуществить надежную «эшелонированную» защиту данных от аппаратных сбоев и повреждений. Система SFT (System Fault Tolerance — система устойчивости к отказам) фирмы Novell предусматривает три основных уровня.

SFT Level I. Первый уровень предусматривает, в частности, создание дополнительных копий FAT и Directory Entries Tables, немедленную верификацию каждого в'новь записанного на файловый сервер блока данных, а также резервирование на каждом жестком диске около 2% от объема диска. При обнаружении сбоя данные перенаправляются в зарезервированную область диска, а сбойный блок помечается как «плохой» и в дальнейшем не используется.

SFT Level II содержит дополнительно возможности создания «зеркальных» дисков, а также дублирования дисковых контроллеров, источников питания и интерфейсных кабелей.

SFT Level III позволяет использовать в локальной сети дублированные серверы, один из которых является «главным», а второй, содержащий копию всей информации, вступает в работу в случае выхода «главного» сервера из строя.

Система контроля и ограничения прав доступа в сетях NetWare (защита от несанкционированного доступа) также содержит несколько уровней.

Уровень начального доступа (включает имя и пароль пользователя, систему учетных ограничений типа явного разрешения или запрещения работы, допустимого времени работы в сети, места на жестком диске, занимаемого личными файлами данного пользователя, и т.д.).

Уровень прав пользователей («персональные» ограничения на выполнение отдельных операций и/или ограничения на работу данного пользователя как члена определенного подразделения, в отдельных частях файловой системы сети).

Уровень атрибутов каталогов и файлов (ограничения на выполнение отдельных операций типа удаления, редактирования или создания, идущие со стороны файловой системы и касающиеся всех пользователей, пытающихся работать с данными каталогами или файлами).

Уровень консоли файл-сервера (блокирование клавиатуры файл-сервера на время отсутствия сетевого администратора до ввода им специального пароля).

Однако полагаться на эту часть системы защиты информации в ОС NetWare можно не всегда. Свидетельством тому являются многочисленные инструкции в Internet и готовые доступные программы, позволяющие взломать те или иные элементы защиты от несанкционированного доступа. То же замечание справедливо по отношению к другим мощным сетевым ОС со встроенными средствами защиты информации (Windows NT, UNIX).

Дело в том, что защита информации — это только часть из многочисленных задач, решаемых сетевыми ОС. «Выпячивание» одной из функций в ущерб другим (при понятных разумных ограничениях на объем, занимаемый данной ОС на жестком диске) не может быть магистральным направлением развития таких программных продуктов общего назначения, которыми являются сетевые ОС.

В то же время в связи с остротой проблемы защиты информации наблюдается тенденция интеграции (встраивания) отдельных, хорошо зарекомендовавших себя и ставших стандартными средств в сетевые ОС или разработка собственных «фирменных» аналогов известным программам защиты

информации. Так, в сетевой ОС NetWare 4.1 предусмотрена возможность кодирования данных по принципу «открытого ключа» (алгоритм RSA) с формированием электронной подписи для передаваемых по сети пакетов.

Специализированные программные средства защиты информации от несанкционированного доступа обладают в целом лучшими возможностями и характеристиками, чем встроенные средства сетевых ОС. Кроме программ шифрования, существует много других доступных внешних средств защиты информации. Из наиболее часто упоминаемых следует отметить следующие две системы, позволяющие ограничить информационные потоки.

Firewalls — брандмауэры (дословно firewall — огненная стена). Между локальной и глобальной сетями создаются специальные промежуточные сервера, которые инспектируют и фильтруют весь проходящий через них трафик сетевого/ транспортного уровней. Это позволяет резко снизить угрозу несанкционированного доступа извне в корпоративные сети, но не устраняет эту опасность совсем. Более защищенная разновидность метода — это способ маскарада (masquerading), когда весь исходящий из локальной сети трафик посылается от имени firewall-сервера, делая локальную сеть практически невидимой.

Proxy-servers (proxy — доверенность, доверенное лицо). Весь трафик сетевого/транспортного уровней между локальной и глобальной сетями запрещается полностью — попросту отсутствует маршрутизация как таковая, а обращения из локальной сети в глобальную происходят через специальные серверы-посредники. Очевидно, что при этом методе обращения из глобальной сети в локальную становятся невозможными в принципе. Очевидно также, что этот метод не дает достаточной защиты против атак на более высоких уровнях — например, на уровне приложения (вирусы, код Java и JavaScript).

Нет никакой возможности (да и необходимости) рассматривать различные аспекты проблем защиты информации в компьютерных сетях и возможные способы их решения более подробно. Этим специальным вопросам посвящено много книг, публикаций в периодической печати и в Internet. Имеются, наконец, жесткие законодательные акты. Авторы надеются, что приведенные в данном разделе сведения достаточны для первоначального введения в круг проблем и решений, связанных с защитой информации.

Глава 7. Алгоритмы сети Ethernet/Fast Ethernet

Содержание седьмой главы:

7.1. Метод управления обменом CSMA/CD

В данной главе мы рассмотрим подробнее два основных алгоритма, применяемых в самой распространенной на сегодняшний день сети Ethernet/ Fast Ethernet. Речь идет о методе управления обменом (методе доступа) CSMA/CD и о методе вычисления циклической контрольной суммы пакета CRC.

Эти же самые алгоритмы используются во многих других локальных сетях. Например, метод доступа CSMA/CD применяется в сетях IBM PC Network, AT&T Starlan, Corvus Omninet, PC Net, G-Net и др. Что касается алгоритма вычисления циклической контрольной суммы CRC, то он стал фактическим стандартом для любых локальных сетей. Так что все, о чем говорится в данной главе, относится ко многим локальным сетям.

Как уже говорилось в главе 3, метод управления обменом CSMA/CD (Carrier-Sense Multiple Access with Collision Detection — множественный доступ с контролем несущей и обнаружением коллизий) относится к децентрализованным случайным (точнее, квазислучайным) методам. Он используется как в обычных сетях типа Ethernet, так и в высокоскоростных сетях типа Fast Ethernet. Поскольку характеристики и области применения этих популярных на практике сетей связаны именно с особенностями используемого метода доступа, его стоит рассмотреть более подробно.

Сначала чуть подробнее о названии метода. В ранней сети типа Alohanet, работавшей с 1970 г. на Гавайских островах, использовался радиоканал и установленный на спутнике ретранслятор (отсюда слово «несущая» в названии метода), а также сравнительно простой метод доступа CSMA (без обнаружения коллизий). В сетях типа Ethernet и Fast Ethernet в качестве несущей выступает синхросигнал, «подмешиваемый» к передаваемым данным таким образом, чтобы обеспечить надежную синхронизацию на приемном конце за счет организации (при необходимости) дополнительных принудительных переходов сигнала между двумя (как в коде Ман-честер-П) или тремя электрическими уровнями (как в коде типа 8В6Т, используемом в сегменте Fast Ethernet 100BaseT4 на основе четырех неэкранированных витых пар). По сравнению с классическим методом CSMA в методе CSMA/CD добавлено обнаружение конфликтов (коллизий) во время передачи, что повышает надежность доставки информации.

При описании временных диаграмм сетей типа Ethernet и Fast Ethernet, а также предельных размеров пакетов (кадров) широко используются следующие термины.

IPG (interpacket gap, межпакетная щель) — минимальный промежуток времени между передаваемыми пакетами (9,6 мкс для Ethernet/0,96 мкс для Fast Ethernet). Другое название — межкадровый интервал.

BT (Bit Time, время бита) — интервал времени для передачи одного бита (100 не для Ethernet/ 10 не для Fast Ethernet).

PDV (Path Delay Value, значение задержки в пути) — время прохождения сигнала между двумя узлами сети (круговое, то есть удвоенное). Учитывает суммарную задержку в кабельной системе, сетевых адаптерах, повторителях и других сетевых устройствах.

Collision window (окно коллизий) — максимальное значение PDV для данного сегмента.

Collision domain (область коллизий, зона конфликта) — часть сети, на которую распространяется ситуация коллизии, конфликта.

Slot time (время канала) — максимально допустимое окно коллизий для сегмента (512 BT).

Minimum frame size — минимальный размер кадра (512 бит, или 64 байта).

Maximum frame size — максимальный размер кадра (1518 байт).

Maximum network diameter (максимальный диаметр сети) -максимальная допустимая длина сегмента, при которой его окно коллизий не превышает slot time, времени канала.

Truncated binary exponential back off (усеченная двоичная экспоненциальная отсрочка) — задержка перед следующей попыткой передачи пакета после коллизии (допускается максимум 16 попыток). Вычисляется она по следующей формуле:

RAND(0, 2min<N-IO>) • 512 • BT,

где N — значение счетчика попыток, RAND(a, b) — генератор случайных нормально распределенных целых чисел в диапазоне a...b, включая крайние значения. Дискрет изменения данного параметра равен минимальной длине пакета или максимально допустимой двойной задержке распространения сигнала в сети (PDV).

7.1.1. Алгоритм доступа к сети

На рис. 7.1 показана структурная схема алгоритма доступа к сети в соответствии с методом CSMA/CD для одного из абонентов, имеющих данные (кадры) для передачи.

В начале из кадра, предназначенного для передачи, абонент (узел) формирует пакет. Далее при обозначении блоков информации, передаваемых по сети при использовании алгоритма CSMA/CD, понятия «кадр» и «пакет» не различаются, что не совсем правильно, но соответствует сложившейся практике.

Если после подготовки пакета сеть свободна, то абонент (узел) может начать передачу. Но сначала он должен проверить, прошло ли минимально допустимое время IPG после предыдущей передачи (блок 1 на рисунке). Только после окончания времени IPG абонент может начать передачу битов своего пакета (блок 2 на рисунке).

После передачи каждого бита абонент поверяет наличие конфликта (коллизии) в сети. Если коллизий нет, передача битов продолжается до окончания пакета (блок 4 на рисунке). В этом случае считается, что передача прошла успешно.

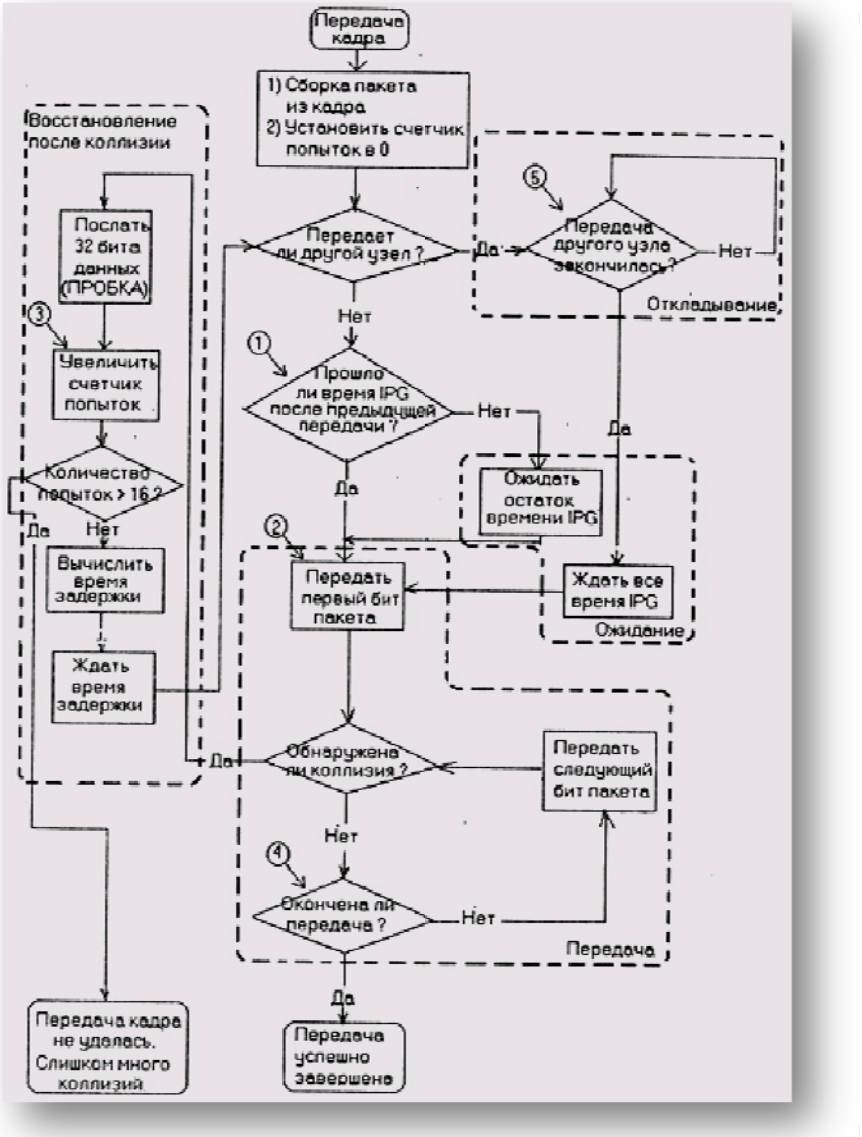


Рис. 7.1

Структурная схема алгоритма доступа к сети в соответствии с методом CSMA/CD

Если после передачи какого-то бита обнаружена коллизия, то передача пакета прекращается. Абонент (узел) усиливает коллизию, передавая 32

битовый сигнал ПРОБКА и начинает готовиться к следующей попытке передачи (блок 3 на рисунке). Сигнал ПРОБКА гарантирует, что факт наличия коллизии обнаружат все абоненты, участвующие в конфликте.

После передачи сигнала ПРОБКА абонент, обнаруживший коллизию, увеличивает значение счетчика числа попыток (перед началом передачи счетчик был сброшен в нуль). Максимальное число

попыток передачи должно быть не более 16, поэтому если счетчик попыток переполнился, то попытки передать пакет прекращаются. Считается, что в этом случае сеть сильно перегружена, в ней слишком много коллизий. Эта ситуация — аварийная, и обрабатывается она на более высоких уровнях протоколов обмена.

Если же количество попыток не превысило 16, то производится вычисление величины задержки по приведенной формуле, а затем и выдержка вычисленного временного интервала. Случайный характер величины задержки с высокой степенью вероятности гарантирует, что у всех абонентов, участвующих в конфликте, задержки будут различными. Затем попытка передать пакет повторяется с самого начала. Понятно, что тот абонент, у которого вычисленная задержка будет меньше, начнет следующую передачу первым и заблокирует все остальные передачи.

Если в момент возникновении заявки на передачу (после окончания подготовки пакета) сеть занята другим абонентом, ведущим передачу, то данный абонент ждет освобождения сети (блок 5 на рисунке). После освобождения сети он должен выждать после предыдущей передачи по сети время IPG до начала собственной передачи. Это связано с конечным быстродействием узлов, осуществляющих проверку наличия несущей (занятости среды каким-либо передающим абонентом).

Таким образом, получается, что метод CSMA/CD не только не предотвращает коллизии, наоборот, он их предполагает, он их даже провоцирует, а затем разрешает. Например, если заявки на передачу возникли у нескольких абонентов во время занятости сети, то после ее освобождения все эти абоненты одновременно начнут передачу и образуют коллизию. Коллизия возникает и в случае свободной сети, если заявки на передачу возникают у нескольких абонентов одновременно. В обоих этих случаях под словом «одновременно» понимается «в пределах интервала двойного прохождения сигнала по сети», то есть в пределах 512-битовых интервалов. Точно так же в пределах 512-битовых интервалов обнаруживаются все коллизии в сети.

Если коллизия обнаруживается раньше 480- битового интервала, то в результате в сети образуются пакеты, длина которых меньше нижнего установленного предела в 512-битовых интервалов (64 байта) даже с добавлением сигнала ПРОБКА. Такие, пакеты (кадры) называются карликовыми (runt frames). Если же коллизия обнаруживается в конце 512-битового интервала (после 480-битового интервала), то в результате может получиться пакет допустимой длины (вместе с сигналом ПРОБКА). Такие пакеты называть карликовыми не совсем правильно. Сигнал ПРОБКА, образующий 32 последних бита пакета, выступает в виде контрольной суммы пакета. Однако вероятность того, что ПРОБКА будет соответствовать правильной контрольной сумме пакета, крайне мала (примерно 1 случай на 4,2 миллиарда).

Коллизии (наложения пакетов в процессе передачи) могут и должны обнаруживаться до окончания передачи. Действительно, анализ принятого в конце каждого пакета поля FCS, фактически содержащего помехоустойчивый циклический код CRC (Cyclic Redundancy Check), привел бы к неоправданному снижению скорости передачи.

Практически коллизии обнаруживаются либо самим передающим абонентом, либо повторителями в сети, возможно, задолго до окончания передачи заведомо испорченного пакета. Если учесть, что длина пакетов в локальной сети типа Ethernet/Fast Ethernet может лежать в диапазоне от 64 до 1518 байт, то досрочное прекращение передачи и освобождение линии означает заметное повышение эффективности использования ее пропускной способности.

Первым признаком возникновения коллизии является факт получения сигнала ПРОБКА передающим абонентом во время передачи пакета. Другие признаки связаны с неверным форматом пакетов, передача которых была досрочно прекращена из-за возникновения коллизии:

- длина пакета меньше 64 байт (512 бит);
- пакет имеет неверную контрольную сумму FCS (точнее, неверный циклический код);
- длина пакета не кратна восьми.

Наконец, в сетях типа Ethernet используется код Манчестер-П и чисто аппаратный способ определения коллизии, основанный на анализе отклонения среднего значения сигнала от нуля.

Даже при загруженной сети для одного абонента число подряд следующих коллизий обычно не превышает 2—3. Этому способствует случайный характер возникновения запроса на передачу и случайная дискретная величина отсрочки следующей попытки передачи в случае возникновения коллизии. Всего же предусмотрено 16 попыток передачи, после чего

возникшая особая ситуация обрабатывается протоколом более высокого уровня. Число коллизий тем больше, чем больше диаметр (размер) сегмента и чем дальше расположены друг от друга абоненты с интенсивным трафиком.

7.1.2. Оценка производительности сети

Вопрос об оценке производительности сетей, использующих случайный метод доступа CSMA/CD, не очевиден из-за того, что существуют несколько различных показателей. Прежде всего, следует упомянуть три связанные между собой показателя, характеризующие производительность сети в идеальном случае — при отсутствии коллизий и при передаче непрерывного потока пакетов, разделенных только межпакетным

интервалом IPG. Очевидно, такой режим реализуется, если один из абонентов активен и передает пакеты с максимально возможной скоростью. Неполное использование пропускной способности в этом случае связано, кроме существования интервала IPG, с наличием служебных полей в пакете Ethernet (см. рис. 7.2).

Пакет максимальной длины является наименее избыточным по относительной доле служебной информации. Он содержит 12304 бит (включая интервал IPG), из которых 12000 бит являются полезными данными.

Поэтому максимальное скорость передачи пакетов (или, иначе, скорость в кабеле — wire speed) составит в данном случае

108 бит/с / 12304 бит = 8127,44 пакет/с.

Пропускная способность представляет собой скорость передачи полезной информации и в данном случае составит

8127,44 пакет/с • 1500 байт = 12,2 Мбайт/с.

Наконец, эффективность использования физической скорости передачи сети, в случае Fast Ethernet равной 100 Мбит/с, по отношению только к полезным данным составит

8127,44 пакет/с • 12000 бит / 10е бит/с = 98 %.

При передаче пакетов минимальной длины (с учетом интервала IPG -84 • 8 = 672 бит, из которых только 46 • 8 = 368 бит несут полезную информацию) возрастает скорость в кабеле (148809,52 пакет/с вместо 8127,44 пакет/с), что означает всего лишь факт передачи большого числа коротких пакетов. В то же время пропускная способность (6,8 Мбайт/с вместо 12,2 Мбайт/с) и эффективность (55% вместо 98 %) заметно ухудшаются.

Для реальных сетей типа Fast Ethernet с большим числом активных абонентов N пропускная способность на уровне 12,2 Мбайт/с для какого-либо абонента является пиковым, редко реализуемым значением. При одинаковой активности всех абонентов средняя пропускная способность для каждого из них составит 12,2/N Мбайт/с, а на самом деле может оказаться еще меньше из-за возникновения коллизий, ошибок в работе сетевого оборудования и влияния помех (в случае работы локальной сети в условиях, когда кабельная система подвержена влиянию больших внешних электромагнитных наводок). Влияние помех, так же как и поздних конфликтов (late collision) в некорректных сетях, отслеживается с помощью анализа поля FCS пакета.

Для реальных сетей более информативен такой показатель производительности, как показатель использования сети (network utilization), который представляет собой долю в процентах от суммарной пропускной способности (не поделенной между отдельными абонентами). Он учитывает коллизии и другие факторы. Ни сервер, ни рабочие станции не содержат средств для определения показателя использования сети, для этого предназначены специальные, не всегда доступные, из-за высокой стоимости аппаратно-программные средства типа анализаторов протоколов.

Считается, что для загруженных систем Ethernet и Fast Ethernet хорошим значением показателя использования сети является 30%. Это значение соответствует отсутствию длительных простоев в работе сети и обеспечивает достаточный запас в случае пикового повышения нагрузки. Однако если показатель использования сети значительное время составляет 80...90% и более, то это свидетельствует о практически полностью используемых (в данное время) ресурсах, но не оставляет резерва на будущее. Впрочем, для реальных сетей типа Fast Ethernet это скорее гипотетическая ситуация.

На рис. 7.2 приведена зависимость показателя использования сети от времени при условии, что предложенная нагрузка (offered load), т.е. текущий запрос на пропускную способность, линейно возрастает. Сначала показатель использования сети также линейно возрастает, но затем конкуренция за владение средой передачи порождает коллизии и рассматриваемый показатель достигает максимума (точка полной нагрузки на графике). При дальнейшем увеличении предложенной нагрузки показатель использования сети начинает уменьшаться, особенно резко после точки насыщения. Это «плохая» область работы сети. Считается, что сеть работает хорошо, если и предложенная нагрузка, и показатель использования сети высоки.

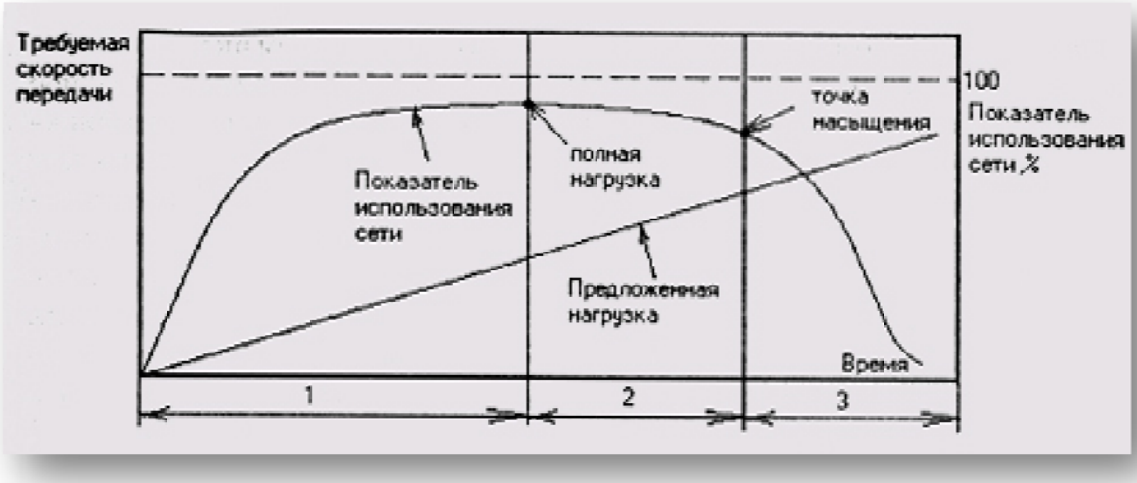


Рис. 7.2
Зависимость показателя использования сети от времени при линейном увеличении предложенной нагрузки (1 — наилучшая область работы, 2 — приемлемая, 3 — плохая)

Некоторые авторы предлагают использовать для широко распространенного понятия «перегрузка» (overload) сетей на основе метода доступа CSMA/CD следующее определение: сеть перегружена, если она не может работать при полной нагрузке в течении не менее 80% своего времени (предполагается, что при этом в течении не менее 20% времени показатель использования сети недопустимо мал из-за коллизий). После точки насыщения наступает крах Ethernet (Ethernet collapse), когда возрастающая предложенная нагрузка заметно превышает возможности сети.

Стоит заметить, что реально маловероятно, чтобы предложенная нагрузка постоянно увеличивалась во времени и надолго превышала пропускную способность сети типа Fast Ethernet. Более того, любой детерминированный метод доступа не может обеспечить реализацию сколь угодно большой предложенной нагрузки, существующей продолжительное время. Если данный вариант детерминированного метода доступа не предусматривает, как и метод CSMA/CD, систему приоритетов, то никакой из абонентов не может захватить сеть более чем на время передачи одного пакета, однако передача данных отдельными пакетами с долгими паузами между ними ведет к снижению скорости передачи для каждого абонента. Однако преимущество детерминированных методов состоит в возможности простой организации системы приоритетов, что полезно из-за существования определенной иерархии в любом крупном коллективе.

7.2. Использование помехоустойчивых кодов для обнаружения ошибок в сети

Сигналы, непосредственно передаваемые по последовательным линиям (типа витой пары, коаксиального кабеля или телефонной линии), подвержены влиянию ряда факторов, воздействие которых может привести к возникновению ошибок в принятой информации. Ошибки могут возникать вследствие влияния на канал связи наводок и помех естественного или искусственного происхождения, а также вследствие изменения конфигурации системы передачи информации с временным нарушением или без нарушения целостности канала связи (например, в случае подключения новых абонентов к существующей локальной информационной сети).

Некоторые из ошибок могут быть обнаружены на основании анализа вида принятого сигнала, так как в нем появляются характерные искажения. Примером может служить код Манчестер-П, используемый в сетях Ethernet. На передающем конце линии этот код обязательно содержит переход с низкого электрического уровня на высокий или обратно в середине каждого тактового интервала, требуемого для передачи одного бита информации. Он также имеет среднюю составляющую, близкую к нулю. Эти свойства кода Манчестер-П могут использоваться для обнаружения разного рода ошибок. В частности, отличие средней составляющей сигнала от нуля является одним из признаков возникновения коллизий (наложений пакетов от разных абонентов), характерных для метода доступа CSMA/CD в сетях типа Ethernet. Однако сколько-нибудь серьезную систему обнаружения ошибок, вызванных воздействием помех с непредсказуемым поведением, на этой основе построить невозможно.

Стандартные протоколы обмена информации в сетях предусматривают введение обязательного поля для размещения помехоустойчивого (корректирующего) кода. Если в результате обработки принятого пакета обнаружится несоответствие принятого и вновь вычисленного помехоустойчивого кода, с большой

долей вероятности можно утверждать, что среди принятых бит имеются ошибочные. Передачу такого пакета нужно будет повторить (в расчете на случайный характер помех).

7.2.1. Способы снижения числа ошибок в принятой информации

Имеется разрыв между требованиями к верности принимаемой информации и возможностями существующих каналов связи. В частности, стандартами международных организаций МККТТ и МОС установлено, что вероятность ошибки при телеграфной связи не должна превышать 3 • 10"5 (на знак), а при передаче данных — 10~6 (на единичный элемент, бит). На практике допустимая вероятность ошибки при передаче данных может быть еще меньше — 10~9. В то же время существующие каналы связи (особенно каналы большой протяженности и протяженные радиоканалы) обеспечивают вероятность ошибки на уровне 10~3...10"4 даже при использовании фазовых корректоров, регенеративных ретрансляторов и других устройств, улучшающих качество каналов связи.

Кардинальным способом снижения вероятности ошибок при приеме является введение избыточности в передаваемую информацию. В системах передачи информации без обратной связи данный способ реализуется в виде помехоустойчивого кодирования, многократной передачи информации или одновременной передачи информации по нескольким параллельно работающим каналам. Помехоустойчивое кодирование доступнее и при прочих равных условиях позволяет обойтись меньшей избыточностью и за счет этого повысить скорость передачи информации.

7.2.2. Характеристики и разновидности помехоустойчивых кодов

Помехоустойчивое кодирование предполагает введение в передаваемое сообщение, наряду с информационными, так называемых проверочных разрядов, формируемых в устройствах защиты от ошибок (кодерах-на передающем конце, декодерах — на приемном). Избыточность позволяет отличить разрешенную и запрещенную (искаженную за счет ошибок) комбинации при приеме, иначе одна разрешенная комбинация переходила бы в другую.

Помехоустойчивый код характеризуется тройкой чисел (n, k, d0), где n— общее число разрядов в передаваемом сообщении, включая проверочные (r), k=n-r — число информационных разрядов, d0— минимальное кодовое расстояние между разрешенными кодовыми комбинациями, определяемое как минимальное число различающихся бит в этих комбинациях. Число обнаруживаемых (tj и (или) исправляемых (t) ошибок (разрядов) связано с параметром d0 соотношениями

Иногда используются дополнительные показатели избыточности, производные от приведенных выше характеристик n, k:R = r/n- относительная избыточность, v = k / n — относительная скорость передачи.

Существующие помехоустойчивые коды можно разделить на ряд групп, только часть из которых используется для обнаружения ошибок в передаваемых по сети пакетах (на рис. 7.3 используемые для этой цели группы выделены утолщенными стрелками). В группе систематических (линейных) кодов общим свойством является то, что любая разрешенная комбинация может быть получена в результате линейных операций над линейно-независимыми векторами. Это способствует упрощению аппаратной и программной реализации данных кодов, повышает скорость выполнения необходимых операций.

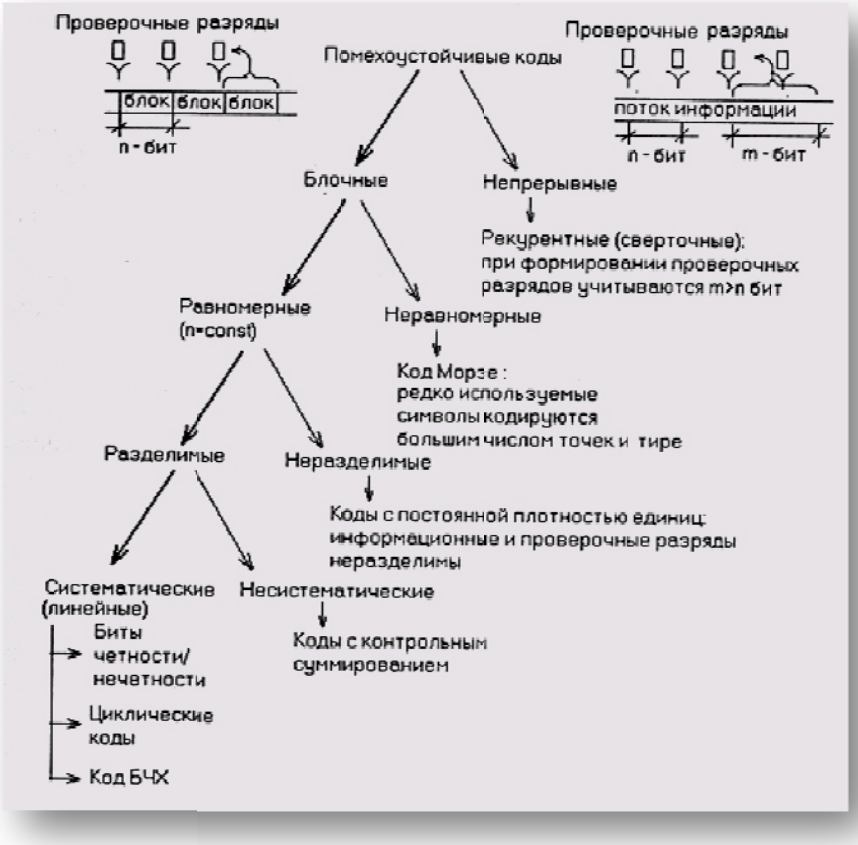


Рис. 7.3
Классификация помехоустойчивых кодов

Простейшими систематическими кодами являются биты четности/нечетности. Они не позволяют обнаружить ошибки четной кратности (т.е. ошибки одновременно в двух, четырех и т.д. битах) и поэтому используются при невысоких требованиях к верности принимаемых данных (или при малой вероятности ошибок в линии передачи). Примером может служить бит Parity (соответствие) в установках режимов работы последовательного порта с помощью команды MODE (MS DOS). Несмотря на ограниченные возможности обнаружения ошибок, биты четности/нечетности имеют большое значение в теории помехоустойчивого кодирования. Одни иг первых математически обоснованных и практически использовании? помехоустойчивых кодов — коды Хэмминга представляют собой простс совокупность перекрестных проверок на четность/нечетность. Циклические коды могут рассматриваться как обобщенные проверки на четность/ нечетность (см. далее).

7.2.3. Циклические коды (CRC)

Циклические коды — это целое семейство помехоустойчивых кодов, вклю чающее в себя в качестве одной из разновидностей коды Хэмминга, но : целом обеспечивающее большую гибкость с точки зрения возможност] реализации кодов с необходимой способностью обнаружения и исправ ления ошибок, определяемой параметром d0, по сравнению с кодами Хэм минга (для которых dQ=3 или d0=4). Широкое использование цикличес ких кодов на практике обусловлено также простотой реализаци соответствующих кодеров и декодеров.

Основные свойства и само название циклических кодов связаны с те!\ что все разрешенные комбинации бит в передаваемом сообщении (коде вые слова) могут быть получены путем операции циклического сдвиг некоторого исходного кодового слова:

$$(a_0 a_1 \ldots a_{n-1});$$
$$(a_{n-1} a_0 a_1 \ldots a_{n-2});$$
$$\ldots\ldots\ldots\ldots$$

Циклические коды задаются с помощью так называемых порождающр полиномов (многочленов) g(x) или их корней. Кроме того, вводятся понятия полинома исходного сообщения

Для этих полиномов, представляющих собой, по существу, альтерната ную запись чисел в двоичной системе счисления, определяются опер ции сложения, умножения и деления, необходимые для организации i

дирования н декодирования сообщения. Все эти операции выполняются по модулю 2.

Рассмотрим последовательность кодирования на примере циклического кода (7,4,3), имеющего g(x) = x3 + x + 1:

1) информационная часть сообщения записывается в виде полинома:

$$u(x) = u_{k-1}x^{k-1} + u_{k-2}x^{k-2} + \ldots + u_0$$

В рассматриваемом примере k = 4 и для сообщения 0111 получаем

$$u(x) = x^2 + x + 1;$$

2) и(x) умножается хг, что соответствует циклическому сдвигу исходного сообщения на г разрядов влево:

$$u(x)\,x^3 = (x^2 + x + 1)\,x^3 = x^5 + x^4 + x^3;$$

3) полученный многочлен делится на g(x):

$$\frac{u(x)\,x^r}{g(x)} = c(x) \oplus \frac{R(x)}{g(x)}$$

где с(x)-полином — частное с максимальной степенью (k-1); R(x)-полином — остаток с максимальной степенью (г-1); © — обозначение поразрядной операции суммирования по модулю 2 (исключающее ИЛИ).

Кодированное сообщение представляется в виде

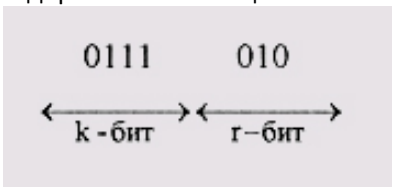
$$A(x) = u(x)\,x^r \oplus R(x),$$

то есть на месте младших, освобожденных после домножения на хг, разрядов, записываются проверочные разряды.

Для рассматриваемого примера:

$$\begin{array}{l} \oplus x^5 + x^4 + x^3 \quad \Big| \underline{x^3 + x + 1} \\ \underline{x^5 + x^3 + x^2} \quad\quad\; \Big| x^2 + x \;\; = c(x) \\ \oplus\; x^4 + x^2 \\ \underline{x^4 + x^2 + x} \\ x = R(x) \end{array}$$

Таким образом, в данном случае А(x) = (x3 + x4 + x3) © x = x5 + x4 + x3 + x. Передаваемое кодированное сообщение в обычной двоичной форме имеет вид:



Один из возможных вариантов аппаратурной реализации кодера для рассматриваемого примера представлен на рис. 7.4 вместе с последовательностью сигналов, подтверждающей получение тех же самых проверочных разрядов (010) на восьмом такте (г + k + 1 = 8).

Кодер представляет собой сдвиговый регистр с обратными связями, организуемыми с помощью элементов М2 (исключающее ИЛИ, сумматор по модулю 2). Структура обратных связей полностью определяется ненулевыми коэффициентами порождающего полинома g(x).

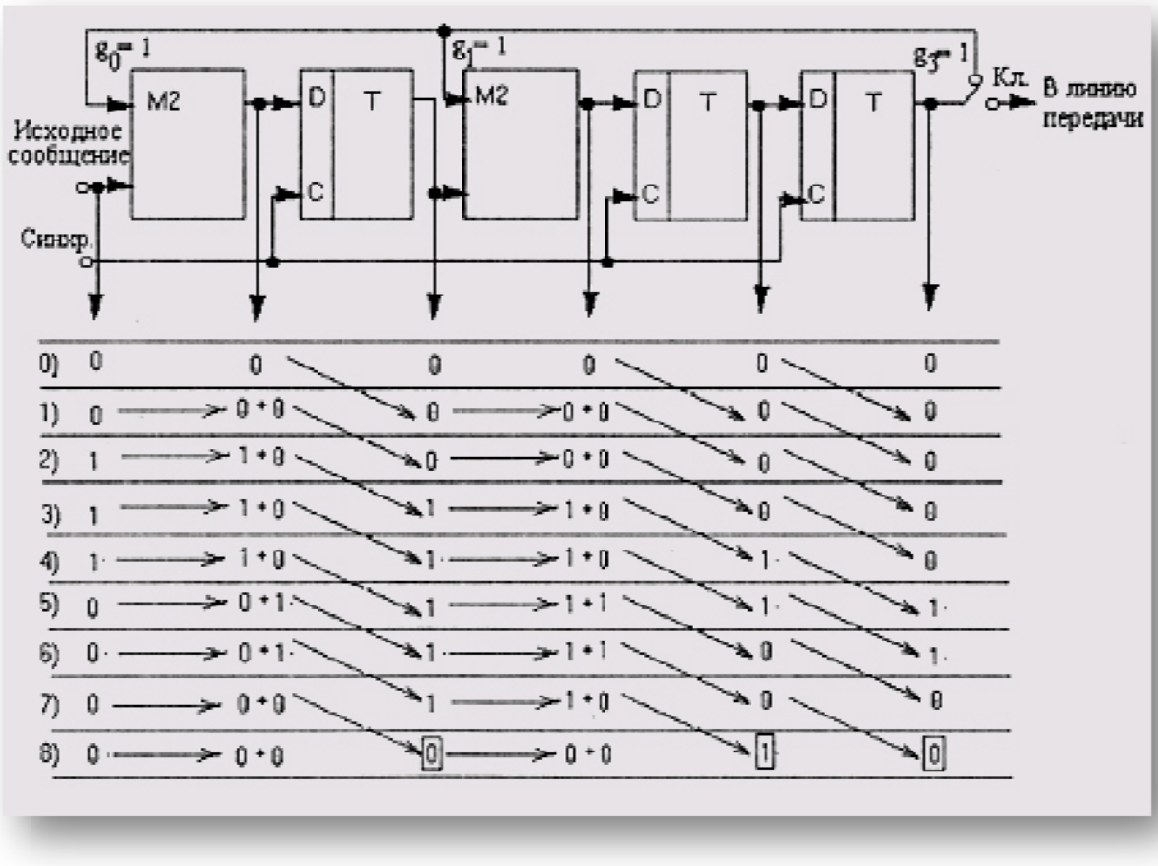


Рис. 7.4

Пример формирования циклического кода (сигнал обратной связи отличен от нуля на 5-м и 6-м тактах)

На первых восьми тактах ключ Кл. находится в верхнем положении и формируются проверочные разряды. Затем ключ Кл. устанавливается в

нижнее положение, что соответствует разрыву цепей обратных связей и передаче непосредственно в канал связи или на модулятор проверочных разрядов. Для временного хранения информационной части сообщения с целью последующей ее передачи вместе с проверочными разрядами кодер, очевидно, должен быть дополнен сдвиговым регистром длиной в k разрядов, ключами и соответствующими цепями управления. Однако, в целом, аппаратурные затраты при реализации кодеров в случае циклических кодов невелики — общее число триггеров и элементов М2 (исключая регистр временного хранения информационной части сообщения) не превышает 2 г и не зависит от длины информационной части сообщения.

Двухвходовый элемент М2, на один из входов которого подается в последовательной форме сообщение, на выходе формирует бит четности или нечетности (в зависимости от значения сигнала на втором входе элемента М2 — 0 или 1) для этого сообщения. В схеме кодера (рис. 7.4) элементы М2 включены между отдельными триггерами сдвигового регистра, причем сигналы обратной связи, поступающие на «свободные» входы элементов М2 (не связанные с передачей собственно сообщения через сдвиговый регистр), зависят как от предшествующих разрядов сообщения, так и от структуры обратных связей, принятой в кодере. В результате циклический код, формируемый таким кодером, можно считать совокупностью обобщенных бит четности и нечетности, тип которых (четность или нечетность) не определен заранее и может динамически меняться от такта к такту.

Порождающие полиномы, представляющие собой т. н. неприводимые многочлены (многочлены, которые делятся лишь на единицу и на самих себя), табулированы для разных значений n, k и dQ, например, п = 7...255, k = 3...247, d0= 3...127. Практически в компьютерных сетях используются циклические коды длиною в 2 или 4 байта (16 или 32 бита), а параметры п, k и d0 в явном виде не указываются. Это связано с возможностью выбора различной длины поля данных в пакете на этапе установления и выбора параметров соединения при неизменной длине поля циклического кода. Теоретическая вероятность ошибки при приеме в случае использования циклического кода не хуже рощ < 1/2г, так что для выполнения условия стандарта рош < 10"6 необходимое число проверочных разрядов г > log2106 = 20. Кроме случайно распределенных, циклический код позволяет обнаруживать подряд следующие ошибки (так называемые пакеты ошибок) длиною 1 = г или меньше. Это особенно важно в связи с возможностью возникновения продолжительных во времени помех, действующих на протяженные линии передачи в компьютерных сетях.

Хотя циклические коды обладают способностью исправления ошибок высокой кратности (при большом значении параметра d0) и известны технические решения декодеров с исправлением ошибок,

однако практическая реализация таких декодеров на современном этапе представляется затруднительной, особенно в случае широкополосных (высокоскоростных) каналов связи. В настоящее время более распространены декодеры с обнаружением ошибок. При использовании обнаруживающего декодера в системе передачи информации неверно принятая информация может игнорироваться либо может быть запрошена повторная передача той же информации; в последнем случае предполагается наличие сигнала подтверждения правильности принятой информации, поступающего от приемника к передатчику информации. По мере развития элементной базы следует ожидать появления в интегральном исполнении декодеров циклических кодов, способных не только обнаруживать, но и исправлять ошибки.

Отметим также, что кроме систем передачи информации, циклические коды используется в запоминающих устройствах (ЗУ) для обнаружения возможных ошибок в считываемой информации. При записи файлов на диск (в том числе при их архивировании) вместе с файлами формируются и записываются соответствующие циклические коды. При чтении файлов (в том числе при извлечении файлов из архива) вычисленные циклические коды сравниваются с записанными и таким образом обнаруживаются возможные ошибки. Свойства циклического кода лежат в основе сигнатурного анализа (эффективного способа поиска аппаратных неисправностей в цифровых устройствах различной сложности). Варианты практической реализации соответствующих кодеров и сигнатурных анализаторов имеют между собой много общего.

Следует сделать два замечания относительно сложившейся терминологии. Хотя понятие «циклические коды» достаточно широкое, на практике его обычно используют для обозначения только одной разновидности, описанной выше и имеющей в англоязычной литературе название CRC (Cyclic Redundancy Check — циклическая избыточная проверка). Более того, иногда поле пакета, фактически содержащее код CRC, называется «контрольной суммой», что в принципе не совсем верно, но встречается повсеместно.

Перспективными с точки зрения аппаратурной реализации представляются коды БЧХ (коды Боуза-Чаудхури-Хоквингема), так же, как и коды Хэмминга, входящие в семейство циклических кодов. Коды БЧХ не слишком большой длины (примерно до n = 1023) оптимальны или близки к оптимальным кодам, т.е. обеспечивают максимальное значение d0 при минимальной избыточности. Эти коды уже нашли практическое применение в цифровых системах записи звука (речи, музыки), причем в варианте, предусматривающем исправление обнаруженных ошибок. Понятно, что относительно невысокие частоты дискретизации звуковых сигналов (48 или 96 кГц) не препятствуют так жестко, как в случае высокоскоростных сетей, проведению дополнительных вычислений.

Глава 8. Стандартные сегменты Ethernet и Fast Ethernet

Содержание восьмой главы:

8.1. Аппаратура 100BASE-TX

Схема объединения компьютеров в сеть 100BASE-TX практически ничем не отличается от схемы в случае 10BASE-T (рис. 8.15). Однако в этом случае необходимо применение кабелей с неэкранированными витыми парами (UTP) категории 5 или выше.

Для присоединения кабелей так же, как и в случае 10BASE-T, используются 8-контактные разъемы типа RJ-45. Но эти разъемы (категории 5) несколько отличаются от разъемов категории 3. Как и для 10BASE-T, длина кабеля не может превышать 100 м, используется топология «пассивная звезда» с концентратором в центре. Только сетевые адаптеры должны быть Fast Ethernet, и концентратор должен быть рассчитан на подключение сегментов 100BASE-TX. Именно поэтому рекомендуется при установке сети 10BASE-T сразу же прокладывать кабель категории 5. Между адаптерами и кабелями сети могут включаться выносные трансиверы.

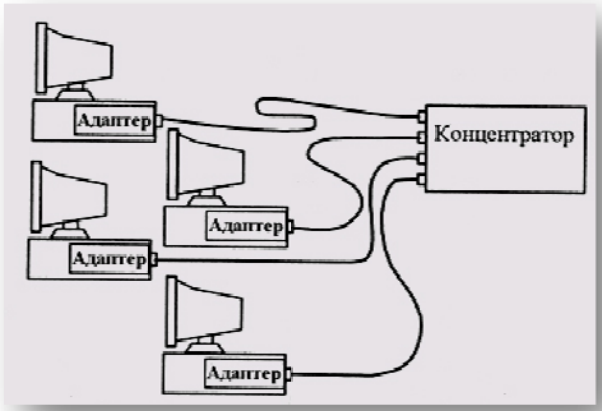


Рис. 8.15
Схема объединения компьютеров по стандарту 10OBASE-TX

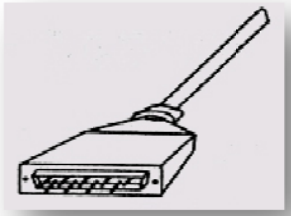


Рис. 8.16
Разъем DB-9

Хотя максимальная длина кабеля как в 10BASE-T, так и в 100BASE-TX равна 100 м, но природа этих ограничений различна. В случае 10BASE-T предельная длина кабеля в 100 м ограничена только качеством кабеля (точнее, затуханием сигнала в нем) и в принципе может быть увеличена при использовании более совершенного кабеля (например, до 150 м). А в случае 100BASE-TX предельная длина 100 м определяется заданными временными соотношениями обмена (установленным ограничением на двойное время прохождения) и не может быть увеличена ни при каких условиях. Поэтому стандарт даже рекомендует ограничиваться длиной сегмента в 90 м, чтобы иметь 10-процентный запас.

Табл. 8.3. Распределение контактов разъема типа RJ-45

Контакт	Назначение	Цвет провода
1	TX+	Белый/оранжевый
2	тх-	Оранжевый/белый
3	RX+	Белый/зеленый
4	Не используется	
5	Не используется	1
6	RX-	Зеленый/белый
7	Не используется	
8	Не используется	

Из восьми контактов разъема RJ-45 используется только 4 контакта (табл. 8.3): два для передачи информации (TX+ и TX-) и два для приема информации (RX+ и RX-). Передача производится дифференциальными сигналами. Стандарт предусматривает также возможность применения экранированного кабеля с двумя витыми парами проводов (волновое сопротивление — 150 Ом). В этом случае должен применяться 9-контактный экранированный разъем DB-9, он же разъем STP IBM типа 1 (рис. 8.16), такой же, как в сети Token-Ring. Назначение контактов этого разъема приведено в табл. 8.4.

Табл. 8.4. Распределение контактов разъема DB9

Контакт	Назначение	Цвет провода
1	RX+	Оранжевый
2	Не используется	
3	Не используется	
4	Не используется	
5	TX+	Красный
6	RX-	Черный
7	Не используется	
8	Не используется	
9	тх-	Зеленый

Как и в случае 10BASE-T, в сети 100BASE-TX могут использоваться два типа кабеля: прямой и перекрестный (рис. 8.17). Для соединения двух компьютеров без применения концентраторов используется стандартный перекрестный (crossover) кабель. А для присоединения компьютера к концентратору применяется прямой (direct) кабель с соединенными между собой одинаковыми контактами разъемов. Если перекрестное соединение предусмотрено внутри концентратора, то соответствующий порт его должен быть помечен буквой «X». Как видим, здесь все точно так же, как и в случае 10BASE-T.

Для контроля целостности сети в 100BASE-TX предусмотрена передача в интервалах между сетевыми пакетами специальных сигналов (FLP — Fast Link Pulse), выполняющих также функцию автоматического согласования скорости передачи аппаратных средств (Auto-Negotiation).

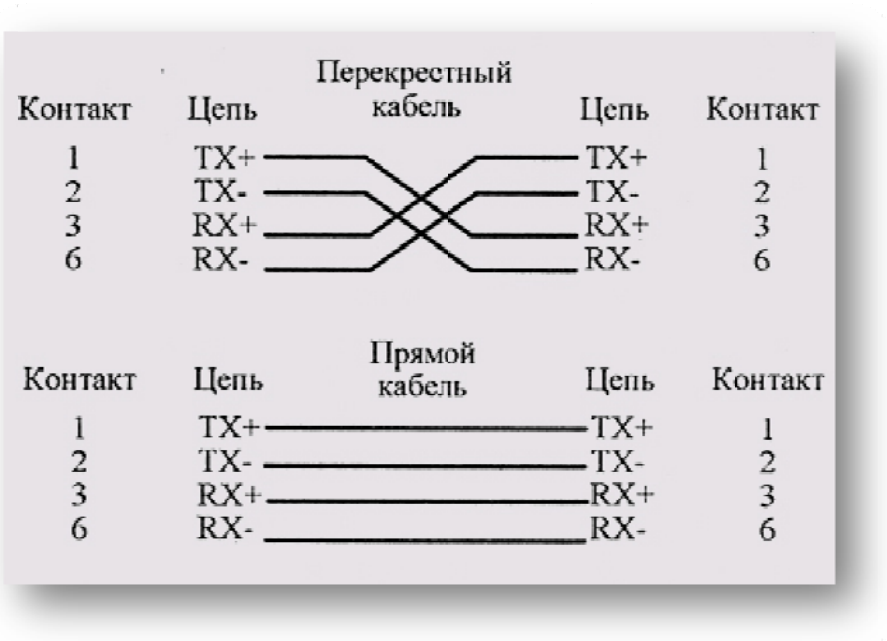


Рис. 8.17
Прямой и перекрестный кабели, применяемые в сегменте 10OBASE-TX

8.2. Аппаратура 100BASE-T4

Основное отличие аппаратуры 100BA5E-T4от 100BASE-TX состоит в том, что передача производится не по двум, а по четырем неэкранированным витым парам. При этом кабель может быть менее качественным, чем в случае 100BASE-TX (категории 3,4 или 5). Принятая в 100BASE-T4 система кодирования сигналов обеспечивает ту же самую скорость 100 Мбит/с на любом из этих кабелей, хотя стандарт рекомендует, если есть такая возможность, использовать кабель категории 5.

Схема объединения компьютеров в сеть ничем не отличается от 100BASETX (рис. 8.15). Компьютеры присоединяются к концентратору по схеме пассивной звезды. Длина кабелей точно так же не может превышать 100 м (стандарт и в этом случае рекомендует ограничиваться 90 м для 10-процентного запаса). Между адаптерами и кабелями в случае необходимости могут включаться выносные трансиверы.

Как и в случае 100BASE-TX, для подключения сетевого кабеля к адаптеру (трансиверу) и к концентратору используются 8-контактные разъемы типа RJ-45. Но в данном случае задействованы все 8 контактов разъема. Назначение контактов разъемов представлено в таблице 8.5.

Обмен данными идет по одной передающей витой паре, по одной приемной витой паре и по двум двунаправленным витым парам с использованием трехуровневых дифференциальных сигналов.

Табл. 8.5. Распределение контактов разъема типа RJ-45 для сегмента 10OBASE-T4 (TX — передача данных, RX — прием данных, BI — двунаправленная передача)

Контакт	Назначение	Цвет провода
1	TX_D1 +	Белый / оранжевый
2	TX_D1-	Оранжевый / белый
3	RX_D2+	Белый / зеленый
4	BI_D3+	Голубой / белый
5	BI_D3-	Белый / голубой
6	RXJD2-	Зеленый / белый
7	BIJD4+	Белый / коричневый
8	BIJD4-	Коричневый / белый

Для связи двух компьютеров без применения концентраторов используется перекрестный кабель. В обычном же прямом кабеле, применяемом для соединения компьютера с концентратором, соединены одноименные контакты обоих разъемов. Схемы кабелей приведены на рис 8.18. Если перекрестное соединение предусмотрено внутри концентратора, то соответствующий порт должен помечаться буквой «X». Как видим, и здесь все точно так же, как в случае 100BASE-TX и 10BASE-T.

Для реализации передачи информации со скоростью 100 Мбит/с по кабелю с малой полосой пропускания (категории 3) в сегменте 100BASE-T4 используется оригинальный принцип кодирования информации, называющийся 8B/6T. Его идея состоит в том, что 8 бит, которые надо передать, преобразуются в 6 тернарных (трехуровневых с уровнями -3,5 В, +3,5 В и О В) сигналов, которые затем передаются за два такта по трем витым парам. При шестиразрядном трехзначном коде общее число возможных состояний равно 36 = 729, что больше, чем 28 = 256, то есть никаких проблем из-за уменьшения количества разрядов не возникает. В результате по каждой витой паре передается информация со скоростью 25 Мбит/с, то есть требуется полоса пропускания всего 12,5 МГц (рис. 8.19). Для передачи информации одновременно используются две двунаправленные витые пары (BI_D3 и BI_D4) и одна однонаправленная (TX_D1 или RX_D2). Четвертая витая пара, не участвующая в передаче информации (TX_D1 или RX_D2), используется для обнаружения коллизий.

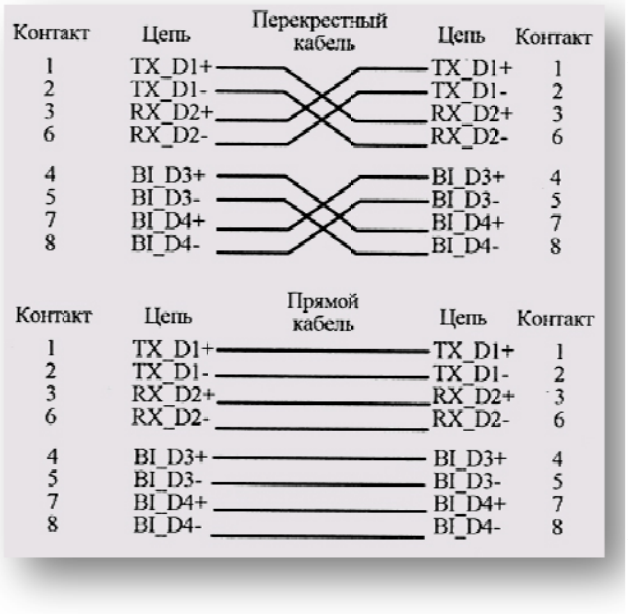


Рис. 8.18
Прямой и перекрестный кабель сети 10OBASE-T4

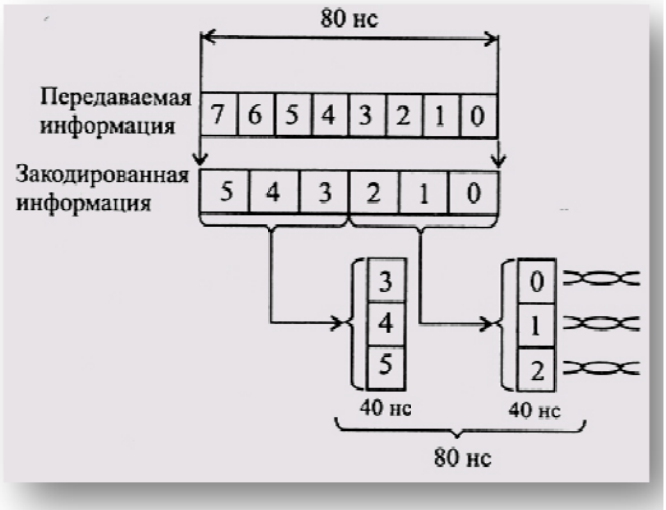


Рис. 8.19
Кодирование информации 8B/6T в сегменте 10OBASE-T4

Для контроля целостности сети в 100BASE-T4 также предусмотрена передача специального сигнала FLP между сетевыми пакетами. Наличие связи индицируется светодиодами «Link».

8.3. Аппаратура 100BASE-FX

Применение оптоволоконного кабеля в сегменте 100BASE-FX позволяет существенно увеличить протяженность сети, а также избавиться от электрических наводок и повысить секретность передаваемой информации.

Аппаратура 100BASE-FX очень близка к аппаратуре 10BASE-FL. Точно так же здесь используется топология «пассивная звезда» с подключением компьютеров к концентратору с помощью двух разнонаправленных оптоволоконных кабелей (рис. 8.20). Между сетевыми адаптерами и кабелями возможно включение выносных трансиверов. Как и в случае сегмента 10BASE-FL, оптоволоконные кабели подключаются к адаптеру (трансиверу) и к концентратору с помощью разъемов типа SC, ST или FDDI. Для присоединения разъемов SC и FDDI достаточно просто вставить их в гнездо, а разъемы ST имеют байонетный механизм.

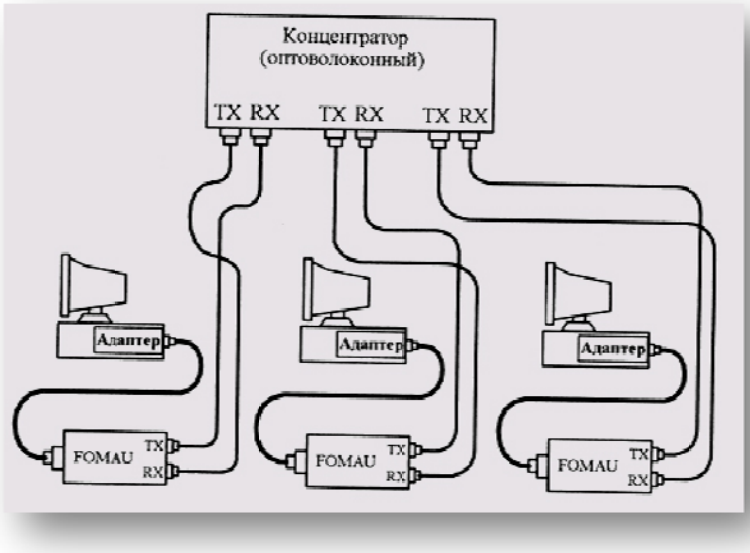


Рис. 8.20
Подключение компьютеров к сети 10OBASE-FX

Максимальная длина кабеля между компьютером и концентратором составляет 412м, причем это ограничение определяется не качеством кабеля, а установленными временными соотношениями. Согласно стандарту,

применяется мультимодовый или одномодовый кабель с длиной волны света 1,35 мкм. В последнем случае потери мощности сигнала в сегменте (в кабеле и разъемах) не должны превышать 11 дБ. При этом надо учитывать, что потери в кабеле составляют 1-5 дБ на километр длины, а потери в разъеме — от 0,5 до 2 дБ (при условии, что разъем установлен качественно).

Как и в других сегментах Fast Ethernet, в 100BASE-FX предусмотрен контроль за целостностью сети, для чего в промежутках между сетевыми пакетами по кабелю передается специальный сигнал. Целостность сети индицируется светодиодами «Link».

8.4. Автоматическое определение типа сети (Auto-Negotiation)

Функция автоматического определения типа сети, предусмотренная стандартом Ethernet, не является обязательной. Однако ее реализация в сетевых адаптерах и концентраторах позволяет существенно облегчить жизнь пользователям сети. Особенно это важно на современном этапе, когда широко применяются как более ранняя версия Ethernet со скоростью обмена 10 Мбит/с, так и более поздняя версия Fast Ethernet со скоростью 100 Мбит/с.

Функция автодиалога или автосогласования (так можно перевести Auto-Negotiation) позволяет адаптерам, в которых предусмотрено переключение скорости передачи, автоматически подстраиваться под скорость обмена в сети, а концентраторам, в которых предусмотрен авто диалог, самим определять скорость передачи адаптеров, подключенных к их портам. При этом пользователь сети не должен следить за тем, на какую скорость обмена настроена его аппаратура: система сама выберет максимально возможную скорость.

Сразу отметим, что режим автодиалога применяется только в сетях на основе сегментов, использующих витые пары: 10BASE-T, 100BASE-TX и 100BASE-T4. Для сегментов на базе коаксиального кабеля и оптоволоконного кабеля автодиалог не предусмотрен. Шинные сегменты на коаксиальном кабеле не дают возможности двухточечной связи, а в оптоволоконных сегментах применяется другая система служебных сигналов.

Автодиалог основан на использовании сигналов, передаваемых в Fast Ethernet, которые называются FLP (Fast Link Pulse) по аналогии с сигналами NLP (Normal Link Pulse), применяемыми в сегментах 10BASE-T. Так же, как и NLP, сигналы FLP начинают вырабатываться с включением питания соответствующей аппаратуры (адаптера или концентратора) и формируются в паузах между передаваемыми сетевыми пакетами, поэтому они никак не влияют на загрузку сети. Именно сигналы FLP и передают информацию о возможностях подключенной к данному сегменту аппаратуры.

Так как аппаратура 10BASE-T разрабатывалась до создания механизма автодиалога, для автоматического определения типа сети необходимо обрабатывать не только сигналы FLP, но и сигналы NLP. Это также предусмотрено в аппаратуре, поддерживающей автодиалог. Естественно, в такой аппаратуре, как правило, предусматривается и возможность отключения режима автодиалога, чтобы пользователь сам мог задать режим работы своей сети.

Помимо уже упоминавшихся сегментов 10BASE-T, 100BASE-TX и 100BASE-T4, автодиалог предусматривает обслуживание так называемых полнодуплексных (full duplex) сегментов сети Ethernet (10BASE-T Full Duplex) и сети Fast Ethernet (100BASE-TX Full Duplex).

Как известно из теории связи, связь бывает симплексная (всегда только в одну сторону), полудуплексная (по очереди то в одну сторону, то в другую) и полнодуплексная (одновременно в две стороны). Классический Ethernet использует полудуплексную связь: по его кабелю в разное время может проходить разнонаправленная информация. Это позволяет легко реализовать обмен между большим количеством абонентов, но требует сложных методов доступа к сети (CSMA/CD). Полнодуплексная версия Ethernet гораздо проще. Она предназначена для обмена только между двумя абонентами по двум разнонаправленным кабелям, причем передавать могут оба абонента сразу. Два преимущества такого подхода понятны сразу: во-первых, не требуется никакого механизма доступа к сети, а во-вторых, в идеале пропускная способность такой линии связи оказывается вдвое выше, чем при полудуплексной передаче. Полнодуплексные версии Ethernet и Fast Ethernet находятся еще на стадии стандартизации, поэтому единых правил обмена пока не выработано, и аппаратура разных производителей может основываться на разных принципах обмена. Тем не менее, автодиалог уже ориентирован на их распознавание и использование.

При проведении автодиалога применяется таблица приоритетов (табл. 8.6), в которой полнодуплексные версии имеют более высокие приоритеты, чем классические полудуплексные, так как они более быстрые.

Из таблицы следует, что если аппаратура на обоих концах сегмента поддерживает обмен с двумя скоростями, например, в режимах 10BASE-T и 100B ASE-TX, то в результате автодиалога будет выбран режим 100BASETX, как имеющий больший приоритет (обеспечивающий большую скорость).

Табл. 8.6. Приоритеты автодиалога (1 — высший приоритет, 5 — низший приоритет)

Приоритет	Тип сети
1	100BASE-TX Full Duplex
2	100BASE-T4
3	100BASE-TX
4	10BASE-T Full Duplex
5	10BASE-T

Автодиалог предусматривает также разрешение ситуаций, когда на одном конце кабеля подключена двухскоростная аппаратура, а на другом -односкоростная. Например, если двухскоростной адаптер присоединен к концентратору 10BASE-T, в котором не предусмотрена возможность автодиалога, то он не будет получать сигналов FLP, а будет получать только сигналы NLP. В результате действия механизма автодиалога адаптер будет переключен в режим концентратора 10BASE-T. Точно так же, если двухскоростной концентратор присоединен к односкоростному адаптеру 100BASE-TX, не рассчитанному на автодиалог, то концентратор перейдет в режим адаптера 100BASE-TX. Этот механизм одностороннего определения типа сети называется параллельным детектированием (Parallel Detection).

Естественно, в любом случае автодиалог не может обеспечить большей скорости, чем самый медленный из компонентов сети. То есть если к ре-питерному концентратору, в котором предусмотрена функция автодиалога, подключены два адаптера: односкоростной 10BASE-T и двухскоростной (10BASE-T и 100BASE-TX), то вся сеть будет настроена на работу как 10BASE-T, так как никакого накопления информации и никакой ее обработки в репитерном концентраторе не предусмотрено. Присоединение к такому концентратору двух неперестраиваемых (односкоростных) адаптеров с разными скоростями делает сеть

неработоспособной. Иногда в конструкции репитеров предусматривается автоматическое отключение портов, к которым присоединены неперестраиваемые низкоскоростные (10BASE-T) адаптеры. Некоторые концентраторы (самые сложные) могут автоматически перекоммутировать порты таким образом, чтобы сегменты со скоростью 10 Мбит/с обменивались информацией только между собой, а сегменты со скоростью 100 Мбит/с — между собой.

Отметим также, что помимо собственно определения типа сети и выбора максимально возможной скорости обмена автодиалог обеспечивает и некоторые дополнительные возможности. В частности, он позволяет определять, почему нарушилась связь в процессе работы, а также обмениваться информацией об ошибках. Для передачи этой дополнительной информации используется тот же самый механизм, что и для основного автодиалога, но только после того, как установлен тип сети и скорость передачи. Данная функция называется «функцией следующей страницы» (Next Page function).

А теперь рассмотрим автодиалог несколько подробнее.

Обмен информацией при автодиалоге производится посылками (пакетами) FLP-импульсов, которыми кодируется 16-битное слово. Каждая посылка содержит от 17 до 33 импульсов, идентичных импульсам NLP, которые используются в 10BASE-T. Посылки имеют длительность около 2 мс и передаются с периодом 16,8 мс (рис. 8.21).

Для кодирования битов в FLP применяется следующий код. В начале каждого битового интервала передается импульс. В середине бита, соответствующего логической единице, передается еще один импульс. В середине бита, соответствующего логическому нулю импульса нет. Этот код иллюстрируется рис. 8.22. В начале посылки передается стартовый нулевой бит, именно поэтому общее количество импульсов в посылке FLP может изменяться в пределах от 17 до 33.

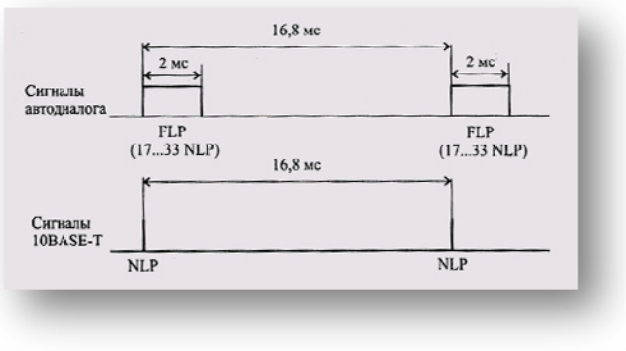


Рис. 8.21
Временная диаграмма автодиалога и 10BASE-T

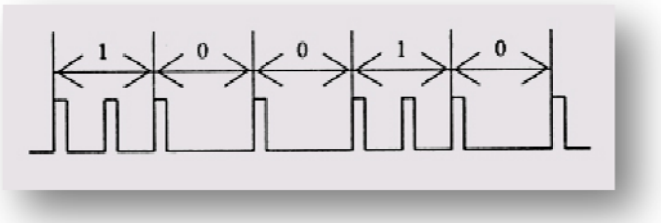


Рис. 8.22
Код, применяемый при автодиалоге

Обмен информацией при автодиалоге осуществляется 16-битными словами, называемыми LCW (Link Code Word), с форматом, представленным на рис. 8.23.

Пятиразрядное поле селектора (Selector Field) определяет один из 32 возможных типов стандарта сети. В настоящее время для него используется только два кода: код 00001 соответствует стандарту IEEE 802.3, а код 00010 соответствует стандарту IEEE 802.9.

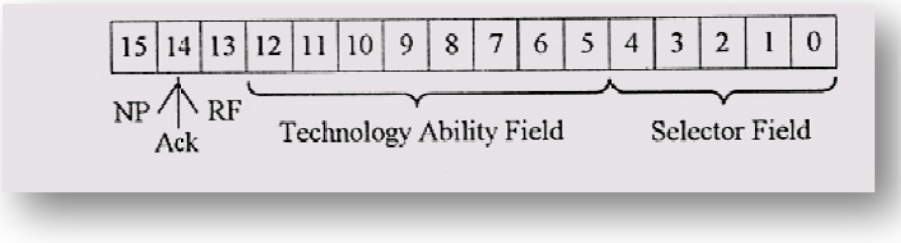


Рис. 8.23
формат слова LCW, применяемого в автодиалоге

Восьмиразрядное поле технологических особенностей (Technology Ability Field) определяет тип сети в пределах стандарта, заданного битами поля селектора. Для стандарта IEEE 802.3 пока что определены пять типов, представленные в таблице 8.6.

Бит удаленной ошибки RF (Remote Fault) позволяет передавать информацию о наличии ошибок. Бит подтверждения Ack (Acknowledge) используется для подтверждения получения посылки. Наконец, бит следующей страницы NP (Next Page) говорит о поддержке функции следующей страницы, о том, что абонент собирается передавать еще и дополнительную информацию.

В автодиалоге используется специально разработанный протокол с многократным подтверждением принятия посылок. В случае, если автодиалог происходит между абонентами 1 и 2, последовательность действий абонентов будет такой.

1. Абонент 1 передает свою посылку (LCW) с неустановленным (равным нулю) битом Ack.
2. Абонент 2 в ответ начинает передавать последовательные ответные посылки (LCW).
3. Когда абонент 1 получает три последовательные посылки от абонента 2 (бит Ack при этом игнорируется), он передает посылку с установленным (равным единице) битом Ack (подтверждает правильный прием LCW от абонента 2).
4. Абонент 2 продолжает передавать свои LCW с установленным битом Ack.
5. Когда абонент 1 получает три последовательные посылки от абонента 2 с установленным битом Ack, он понимает, что абонент 2 правильно принял его LCW.
6. Абонент 1 передает свое LCW с установленным битом Ack 6—8 раз для гарантии, что диалог завершен полностью.
7. В результате оба абонента получают информацию о своем партнере и могут выбрать тот режим работы, который обеспечит наилучшие характеристики обмена.

Отметим, что в соответствии с этим алгоритмом действуют оба абонента, участвующие в авто диалоге. Как видим, здесь реализуется механизм многократного взаимного подтверждения, что существенно гювышает надежность передачи данных об аппаратуре абонентов. При этом также легко детектируются различные ошибочные ситуации, например, неисправности аппаратуры абонентов, нарушения целостности кабеля, несовместимость аппаратуры абонентов и т.д.

Для реализации функции следующей страницы используется бит NP (см. рис. 8.23). Если оба абонента устанавливают его в своих LCW, то есть оба они поддерживают эту функцию, то между ними может быть произведен дополнительный обмен информацией такими же 16-разрядными словами, но с другим форматом. В этих словах 11 битов отводится на информацию, а пять битов используются как служебные. В частности, это позволяет производить более полную диагностику аппаратуры, а также выявлять повышенный уровень помех в линии связи.

Вероятно, в дальнейшем принцип автодиалога будет совершенствоваться и развиваться, включая в себя другие стандарты и типы сети, давая возможность решения все новых задач. Но его реализация в принципе невозможна при стандартной топологии «шина», поэтому, скорее всего, доля шинных сегментов (10BASE2 и 10BASE5) будет все больше сокращаться. В новых сетях (Fast Ethernet, Gigabit Ethernet) шинные сегменты вряд ли появятся.

Глава 9. Оборудование Ethernet и Fast Ethernet

Содержание девятой главы:

9.1. Адаптеры Ethernet и Fast Ethernet

Так как сеть Ethernet/Fast Ethernet в настоящее время распространена наиболее широко, ее аппаратура выпускается наибольшим числом производителей и ее перспективы представляются самыми благоприятными, остановимся подробнее на некоторых особенностях ее аппаратных средств. Впрочем, многое из сказанного в этом разделе относится не только к Ethernet, но и к аппаратуре других, менее популярных сетей.

9.1.1. Характеристики адаптеров

Сетевые адаптеры (NIC, Network Interface Card) Ethernet и Fast Ethernet могут сопрягаться с компьютером через один из следующих стандартных интерфейсов:

- шина ISA (Industry Standard Architecture);
- шина PCI (Peripheral Component Interconnect);
- шина EISA (Enhanced ISA);
- шина MCA (Micro Channel Architecture);
- шина VLB (VESA Local Bus);
- шина PC Card (она же PCMCIA);
- параллельный порт Centronics (LPT);
- последовательный порт RS232-C (COM).

Наиболее часто встречаются адаптеры, рассчитанные на системную шину (магистраль) ISA, так как эта шина пока еще распространена больше других, ее слоты расширения имеет подавляющее большинство настольных компьютеров. Именно поэтому адаптеры данного типа самые дешевые. Адаптеры для ISA выпускаются 8- и 16-разрядными. 8-разрядные адаптеры дешевле, а 16-разрядные — быстрее. Правда, обмен информацией по шине ISA не может быть слишком быстрым (в пределе — 16 Мбайт/с, реально — не более 8 Мбайт/с). Поэтому адаптеры Fast Ethernet, требующие для эффективной работы больших скоростей обмена, для этой системной шины практически не выпускаются.

Шина PCI сейчас постепенно вытесняет шину ISA и становится основной шиной расширения для компьютеров. Она обеспечивает обмен 32- и 64-разрядными данными и отличается высокой пропускной способностью (теоретически до 264 Мбайт/с), что вполне удовлетворяет требованиям не только Fast Ethernet, но и более быстрой Gigabit Ethernet. Важно еще и то, что шина PCI применяется не только в компьютерах типа IBM PC, но и в компьютерах типа PowerMac, а также то, что она поддерживает режим автоматического конфигурирования оборудования Plug-and-Play. Видимо, в ближайшем будущем именно на шину PCI будет ориентировано большинство сетевых адаптеров. Недостаток PCI по сравнению с шиной ISA в том, что количество ее слотов расширения в компьютере невелико (обычно 3 слота).

Шины MCA, EISA и VLB некоторое время конкурировали с PCI (все они обеспечивают 32-разрядный обмен данными), но не выдержали конкуренции и быстро отмирают. На вновь выпускаемых компьютерах они уже не предусматриваются. Поэтому исчезают и сетевые адаптеры, рассчитанные на эти шины. Отметим, что адаптеры ISA полностью совместимы с разъемами EISA. Но это единственный пример подобной взаимной совместимости перечисленных интерфейсов.

Шина PC Card (старое название PCMCIA) применяется пока только в портативных компьютерах класса Notebook. В этих компьютерах внутренняя шина PCI обычно не выводится наружу. Интерфейс PC Card предусматривает простое подключение к компьютеру миниатюрных плат расширения, причем скорость обмена с этими платами достаточна высока. Однако все больше портативных компьютеров оснащается встроенными сетевыми адаптерами, так как возможность доступа к сети становится неотъемлемой частью стандартного набора функций. Эти встроенные адаптеры опять же подключены к внутренней шине PCI.

При выборе сетевого адаптера, ориентированного на ту или иную шину, необходимо прежде всего убедиться, что свободные слоты расширения данной шины есть в компьютере, включаемом в сеть. Не мешает также оценить трудоемкость установки приобретаемого адаптера и перспективы выпуска плат данного типа. Последнее может понадобиться в случае выхода адаптера из строя.

Наконец, параллельный (принтерный) порт LPT и последовательный порт COM применяются для подключения сетевых адаптеров довольно редко. Главное достоинство такого подхода состоит в том, что для подключения адаптеров не нужно вскрывать корпус компьютера. Кроме того, в данном случае адаптеры не занимают системных ресурсов компьютера, таких как каналы прерываний и ПДП, а также адреса памяти и устройств ввода/ вывода. Однако скорость обмена информацией между ними и компьютером в обоих этих случаях значительно ниже, чем при использовании системной шины. К тому же они требуют больше процессорного времени на обмен с сетью, замедляя тем самым работу компьютера в целом. Важно и то, что адаптерам в этом случае требуется внешний источник питания, так как на разъемы LPT и COM питание компьютера не выведено.

Перечислим важнейшие характеристики сетевых адаптеров:

- способ конфигурирования адаптера;
- размер установленной на плате буферной памяти и режимы обмена с ней;
- возможность установки на плату ПЗУ удаленной загрузки (BootROM).
- возможность подключения адаптера к разным типам среды передачи (витая пара, тонкий и толстый коаксиальный кабель, оптоволоконный кабель);
- используемая адаптером скорость передачи по сети и возможность ее переключения;
- возможность использования адаптером полнодуплексного режима обмена;
- совместимость адаптера (точнее, драйвера адаптера) с используемыми сетевыми программными средствами.

Конфигурирование адаптера подразумевает настройку на использование системных ресурсов компьютера (адресов ввода/вывода, каналов прерываний и прямого доступа к памяти, адресов буферной памяти и памяти удаленной загрузки). Конфигурирование может осуществляться путем установки в нужное положение переключателей (джамперов) или с помощью прилагаемой к адаптеру DOS-программы конфигурирования (Jumperless, Software configuration). При запуске такой программы

пользователю предлагается установить конфигурацию аппаратуры при помощи простого меню: выбрать параметры адаптера. Эта же программа позволяет произвести самотестирование адаптера. Выбранные параметры хранятся в энергонезависимой памяти адаптера. В любом случае при выборе параметров необходимо избегать конфликтов с системными устройствами компьютера и с другими платами расширения. Конфигурирование может выполняться и автоматически в режиме Plug-and-Play при включении питания компьютера. Адаптеры, поддерживающие этот режим, может легко установить любой неподготовленный пользователь.

В простейших адаптерах обмен с внутренней буферной памятью адаптера (Adapter RAM) осуществляется через адресное пространство устройств ввода/вывода. В этом случае никакого дополнительного конфигурирования адресов памяти не требуется. Базовый адрес буферной памяти, работающей в режиме разделяемой памяти, необходимо задавать. Он приписывается к области верхней памяти компьютера (UMA, Upper Memory Address) в диапазоне адресов AOOOOh-FFFFFh. В эту же зону адресов помещается и ПЗУ удаленной загрузки (Boot ROM), если предполагается его использование для создания бездисковой рабочей станции. При выборе значений адресов надо следить, чтобы не было конфликтов с другими устройствами компьютера.

Все операции по конфигурированию сетевого адаптера необходимо проводить в строгом соответствии с документацией, поставляемой вместе с ним, так как каждый из многочисленных производителей адаптеров обычно вносит в них что-то свое, оригинальное. Поэтому никакие более подробные универсальные рекомендации попросту невозможны. Впрочем, это относится к любым электронным устройствам.

От размера буферной памяти адаптера зависит как скорость работы адаптера, так и его способность держать высокие информационные нагрузки. Размер памяти обычно составляет от 8 Кбайт до нескольких мегабайт. Чем больше память, тем больше сетевых пакетов может в ней храниться. Для адаптеров, работающих на выделенном сервере, большой объем буферной памяти просто необходим, ведь через него

пойдут все информационные потоки сети. Впрочем, самая большая буферная память не поможет, эсли компьютер работает медленно, не успевает перекачивать приходящую по сети информацию.

Все функции по обслуживанию обмена по сети в сетевом адаптере, как правило, выполняет одна специализированная микросхема или неболь-лой комплект микросхем (2-3 штуки). Этим и объясняется достаточно низкая цена адаптеров. Поставщиков подобных комплектов микросхем к так много, поэтому очень многие адаптеры выполнены по сходным схемам. Однако организация обмена шины компьютера с адаптером может быть различной, поэтому показатели производительности адаптеров от разных изготовителей и показатели надежности их работы, особенно в экстремальных условиях, сильно различаются.

Адаптер может быть рассчитан только на один тип среды передачи, к примеру, на витую пару, но может поддерживать возможность подключения и нескольких разных сред передачи, например, тонкий и толстый коаксиальные кабели. Для этого на плате устанавливаются соответствующие разъемы. Наиболее универсальны так называемые адаптеры «Combo», которые имеют полный набор разъемов (BNC, RJ-45 и AUI для Ethernet). Для выбора конкретного типа среды иногда используются переключатели (джамперы), как правило, их несколько и переключать их надо обязательно все вместе.

Адаптеры Fast Ethernet выпускаются как односкоростными (100 Мбит/ с), так и двухскоростными (10 Мбит/с и 100 Мбит/с). Двухскоростные платы (их обычно помечают «10/100») несколько дороже односкоростных, но зато они могут работать в любой сети Ethernet/Fast Ethernet без всяких проблем. Поэтому лучше в данном случае не экономить на мелочах.

Все сетевые адаптеры должны быть сертифицированы. Сертификат FCC класса А позволяет использовать адаптер в бизнесе, сертификат FCC класса В — в домашних условиях. Стандарт предусматривает безопасный уровень электромагнитного излучения сетевого адаптера.

При выборе адаптера очень важно обращать внимание на совместимость . его драйвера с сетевым программным обеспечением. Все поставщики сетевых программных средств (Novell, Microsoft и др.) проводят работу по сертификации драйверов. Если такой сертификат имеется, то можно быть уверенным, что проблем по совместимости не будет. С другой стороны, все сетевые программные продукты поставляются с набором протестированных драйверов, совместимых с ними. Если драйвер приобретенной платы входит в этот набор, то проблем тоже, скорее всего, не будет. Солидные производители сетевых адаптеров регулярно распространяют обновленные, более быстрые и универсальные версии драйверов для своих плат. Низкая цена некоторых адаптеров может объясняться как раз отсутствием сертификата, плохой совместимостью с программными средствами.

Несколько слов о производительности адаптера.

Реальная скорость обмена информацией по сети представляет собой интегральный параметр, зависящий не только от адаптера, но и от компьютера (быстродействия процессора и диска, объема памяти), от среды передачи (уровня помех), от программных средств, от величины загрузки сети и т.д. Поэтому выбор самого быстрого (и дорогого) адаптера далеко не всегда гарантирует заметный выигрыш в скорости обмена. Например, переход с 8-разрядного адаптера ISA на 16-разрядный или с ISA адаптера на 32-разрядный PCI адаптер может практически не сказаться на скорости. Тем не менее, нередки ситуации, когда именно адаптер становится самым узким местом в системе и его замена может резко увеличить производительность сети.

Косвенные показатели производительности адаптера уже были перечислены: производительнее всего работают те, которые рассчитаны на PCI, поддерживают режим разделения буферной памяти и имеют буферную память большего объема. Быстрее будут те адаптеры, которые максимальное количество функций выполняют без участия процессора, опираясь на свой собственный встроенный интеллект.

Но получить реальные количественные показатели производительности можно только в результате тестирования всей сети в целом. Для этого существует целый ряд тестовых программ, наиболее известны из которых Performs фирмы Novell и Netbench 3.0 фирмы Ziff-Davis. Любые тестовые программы слабо отражают реальную ситуацию в сети, но позволяют сравнивать между собой различные сетевые адаптеры в условиях, близких к реальным, и в реальной конфигурации аппаратных средств.

9.1.2. Адаптеры с внешними трансиверами

Адаптеры Fast Ethernet могут выпускаться с внешним, выносным модулем трансивера для подключения к среде передачи (PHY). В этом случае для присоединения внешнего модуля трансивера к адаптеру используется интерфейс МП (Media-Independent Interface), предусматривающий использование 40-контактного разъема, подобного разъему компьютерного интерфейса SCSI. Сменный модуль трансивера может устанавливаться непосредственно на плате адаптера (в специальный вырез платы), а может связываться с платой адаптера внешним кабелем длиной до 0,5 м (рис. 9.1 и 9.2). При вычислении полного времени задержки в сети необходимо учитывать и задержку в этом трансиверном кабеле.

На плате трансивера располагается микросхема приемопередатчика и разъем, зависящий от типа среды (MDI — Medium Dependent Interface), например, RJ-45 для витой пары. Таким образом, один и тот же

адаптер может поддерживать обмен с любым типом среды за счет простой замены сравнительно дешевого трансивера. Понятно, что в целом подобные составные адаптеры оказываются дороже обычных адаптеров со встроенными приемопередатчиками, но иногда их применение оправдано, если предполагается постепенная замена среды передачи, например, на оптоволоконные кабели.

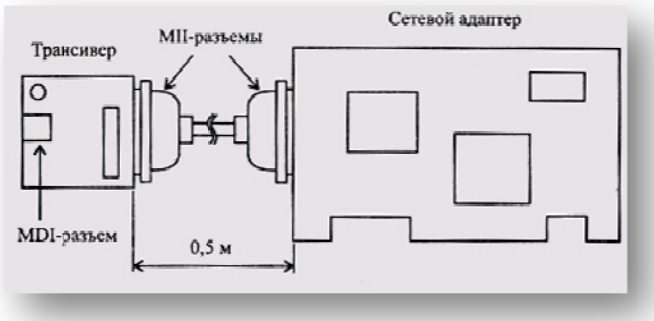


Рис.9.1
Сетевой адаптере внешнимтрансивером на МП-кабеле

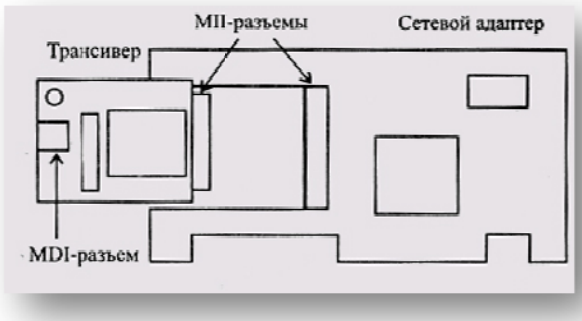


Рис. 9.2
Сетевой адаптер с внешним трансивером, устанавливаемым на плату

9.2. Репитеры и концентраторы Ethernet и Fast Ethernet

Использование репитеров и концентраторов в сети Ethernet не является обязательным. Небольшие сети на основе сегментов 10BASE2 или 10BASE5 вполне могут обойтись без них. Для сетей из нескольких таких сегментов необходимы простейшие репитеры. А при выборе в качестве среды передачи витой пары или оптоволоконного кабеля уже необходимы концентраторы (если, конечно, в сеть объединяются не два компьютера, а хотя бы три). Для сети Fast Ethernet концентраторы совершенно необходимы.

9.2.1. Функции репитеров и репитерных концентраторов

Репитеры (повторители), как уже отмечалось, ретранслируют приходящие на них (на их порты) сигналы, восстанавливают их амплитуду и форму, что позволяет увеличивать длину сети. То же самое делают и простейшие репитерные концентраторы. Но помимо этой основной функции концентраторы Ethernet и Fast Ethernet обычно выполняют еще ряд функций по обнаружению и исправлению некоторых простейших ошибок сети. К этим ошибкам относятся следующие:

- ложная несущая (FCE — False Carrier Event);
- множественные коллизии (ECE — Excessive Collision Error);
- затянувшаяся передача (Jabber).

Все эти ошибки могут вызываться неисправностями оборудования абонентов, высоким уровнем шумов и помех в кабеле, плохими контактами в разъемах и т.д.

Под ложной несущей понимается ситуация, когда концентратор получает от одного из своих портов (от абонента или из сегмента) данные, не содержащие ограничителя начала потока данных (то есть признака начала кадра). Если после начала передачи кадр не начался в течение заданного временного интервала (5 мкс для Fast Ethernet, 50 мкс для Ethernet), то концентратор посылает сигнал «Пробка» всем остальным портам, чтобы они гарантированно обнаружили коллизию. Длительность этого сигнала также составляет 5 или 50 мкс. Затем выявленный порт переводится в состояние «Связь неустойчива» (Link Unstable) и отключается. Обратное включение порта концентратором может произойти только при поступлении от него правильного пакета, без ложной несущей.

Ситуация множественных коллизий фиксируется при выявлении в данном порту более 60 коллизий подряд. Концентратор считает количество коллизий в каждом порту и сбрасывает счетчик, если получает пакет без коллизии. Порт, в котором возникают множественные коллизии, отключается и подключается снова, если в течение заданного времени (5 мкс для Fast Ethernet, 50 мкс для Ethernet) не будет зафиксировано коллизий.

Ситуация затянувшейся передачи фиксируется в случае, когда передача продолжается в течение более 400 мкс для Fast Ethernet или 4000 мкс для Ethernet. Это более чем в три раза превышает максимально возможную длительность пакета. При обнаружении такой затянувшейся передачи соответствующий порт отключается и включается снова только после ее окончания.

Кроме перечисленных функций концентратор также активно способствует обнаружению любых коллизий в сети. При одновременном поступлении на его порты двух и более пакетов он, как и любой

абонент, усиливает столкновение путем передачи во все порты сигнала «Пробка» в течение 32 битовых интервалов. В результате все передающие абоненты всех сегментов обязательно обнаруживают факт коллизии и прекращают свою передачу.

Таким образом, даже самый простой репитерный концентратор представляет собой довольно сложное устройство, позволяющее автоматически устранять некоторые неисправности и временные сбои, то есть концентратор не только объединяет точки включения кабелей сети, но и активно улучшает условия обмена, повышает производительность сети, отключая время от времени неисправные или неустойчиво работающие сегменты.

Как и сетевые адаптеры, концентраторы и репитеры могут быть одно-скоростными и двухскоростными. Для большей свободы в проектировании сети лучше выбирать именно двухскоростные (10/100 Мбит/с) концентраторы и репитеры.

Чаще всего репитеры и концентраторы выполняются в виде отдельных автономных блоков, имеющих внутренний или внешний источник питания. Некоторые концентраторы рассчитаны на подключение жестко заданного количества сегментов определенного типа (например, на четыре сегмента 10BASE2 или же на восемь сегментов 10BASE-T). Другие, более дорогие концентраторы, называемые наращиваемыми (Stackable), имеют модульную структуру и позволяют гибко приспосабливать их к заданной конфигурации сети. В этом случае в каркас (стек) концентратора может быть установлено различное число (обычно до 8) сменных модулей, каждый из которых ориентирован на один или несколько сегментов какого-нибудь типа и имеет соответствующие разъемы для подключения кабеля сети (например, BNC, AUI, RJ-45, ST-разъемы). Как правило, количество подключаемых сегментов (портов концентратора) выбирается кратным четырем: 4, 8,12,16, 24, то есть наращиваемый концентратор может поддерживать, к примеру, 192 порта (восемь модулей, каждый из которых рассчитан на 24 сегмента). Структура такого наращиваемого концентратора показана на рис. 9.3.

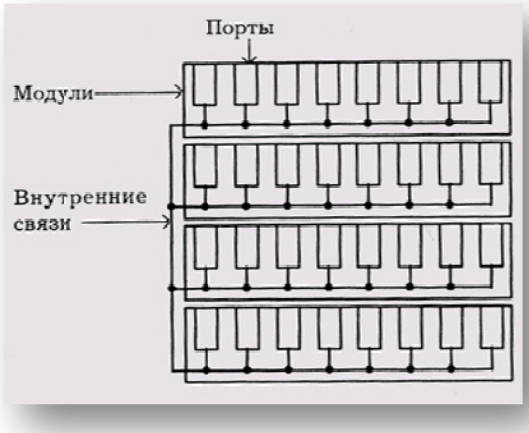


Рис. 9.3
Структура наращиваемого концентратора

Рис. 9.4
Концентратор на основе шасси

Самые сложные концентраторы на базе единого шасси (рис. 9.4) позволяют путем перекоммутации связей на контактной задней панели строить сложные конфигурации сетей. Например, они могут одновременно поддерживать несколько типов сетей (Token-Ring, Ethernet и FDDI), допускают включение не только модулей репитерных концентраторов, но и модулей маршрутизаторов и коммутаторов. На основе такого концентратора можно также организовывать одновременно несколько независимых однотипных сетей (например,'Ethernet) для разделения информационных потоков между ними, снижения нагрузки на сеть.

Как правило, концентраторы на базе шасси предусматривают возможность довольно сложного управления обменом. Количество портов таких концентраторов может доходить до 288. Правда, этот тип концентратора оказывается обычно самым дорогим в расчете на один порт. Считается, что их применение становится экономически оправданным только в случае необходимости поддержки большого количества портов (около 100).

Существуют также совсем простые и самые дешевые репитеры и концентраторы, выполненные в виде платы, вставляемой в разъем системной шины ISA компьютера (из компьютера они берут при этом только питание). Недостаток такого решения состоит в том, что для работы сети необходимо, чтобы компьютер, в который включена плата репитера (концентратора), был постоянно включен (в идеале — круглосуточно). При выключении питания этого компьютера связь по сети становится невозможной.

9.2.2. Концентраторы класса I и класса II

Стандарт IEEE 802.3 определяет два класса репитерных концентраторов, отличающихся друг от друга своими функциональными возможностями и возможными областями применения. Каждый концентратор должен иметь маркировку своего класса в виде римской цифры I или II, заключенной в кружок.

Концентраторы (репитеры) класса II — это классические концентраторы, использовавшиеся с самого начала в сетях Ethernet. Именно поэтому их применение было разрешено и в сетях Fast Ethernet. Эти концентраторы отличаются тем, что непосредственно повторяют приходящие на них из сегмента сигналы и передают их в другие сегменты без какого бы то ни было преобразования. (То есть они не могут преобразовывать методы кодирования сетевых сигналов.) Поэтому к ним можно подключать только сегменты, использующие одну систему сигналов. Например, к концентратору могут подключаться только одинаковые сегменты 10BASE-T или только одинаковые сегменты 100BASE-TX. Могут, правда, подключаться и разные сегменты, но они должны использовать один код передачи, например 10BASE-T и 10BASE-FL или 100BASE-TX и 100BASE-FX. Но данные концентраторы не могут объединять сегменты с разными системами кодирования, например 100BASE-TX и 100BASE-T4.

Задержка сигналов в концентраторах класса II меньше, чем в концентраторах класса I. Согласно стандарту, она должна составлять от 46 битовых интервалов (для 100BASE-TX/FX) до 67 битовых интервалов (для 100BASE-T4). Отсюда следуют ограничения на наращиваемость таких концентраторов и на количество их портов (как правило, оно не превышает 24). Зато меньшая задержка концентратора позволяет использовать кабели большей длины, так как на работоспособность сети влияет суммарная задержка сигнала в сети, включающая в себя как задержки концентраторов, так и задержки в кабелях.

Для соединения концентраторов класса II между собой используется специальный порт расширения (UpLink port). Каждый концентратор подключается этим портом к одному из обычных портов другого концентратора (рис. 9.5).

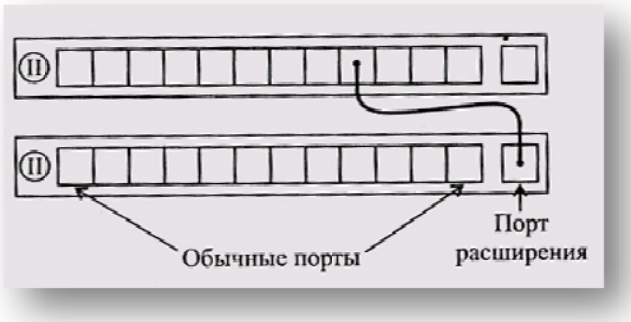


Рис. 9.5
Соединение двух концентраторов класса II

Концентраторы класса II сложнее в производстве, чем концентраторы класса I, так как временные требования, предъявляемые к ним, жестче. Но при этом возможности их меньше, поэтому в настоящее время их постепенно вытесняют концентраторы класса I.

Концентраторы (репитеры) класса I характеризуются тем, что они преобразуют приходящие по сегментам сигналы в цифровую форму, прежде чем передавать их во все другие сегменты. В отличие от концентраторов класса II, они способны преобразовывать коды, применяемые в разных сегментах, поэтому к ним можно одновременно подсоединять сегменты разных типов, например 100BASE-TX, 100BASE-T4 и 100BASE-FX. Но этот процесс преобразования требует времени, поэтому данные концентраторы оказываются медленнее (по стандарту, их задержка составляет не более 140 битовых интервалов).

Концентраторы класса I более гибкие, они имеют более широкие возможности по наращиваемости. Именно из них строятся сложные концентраторы на базе шасси. К тому же благодаря внутренним цифровым шинам сигналов они допускают управление с удаленных рабочих станций, позволяющих контролировать нагрузку сети, состояние портов, интенсивность ошибок в сети, а также автоматически отключать неисправные сегменты. При этом для обмена с управляющей станцией применяется специально разработанный протокол обмена SNMP (Simple Network Management Protocol — простой протокол управления сетью). Такой концентратор, допускающий удаленное управление, называется интеллектуальным (Intelligent Hub).

Протокол SNMP был предложен в 1988 году комиссией IAB (Internet Activities Board). Он описывается документами RFC 1067, RFC 1098, RFC 1157. Комиссия IAB определила также и метод описания данных для этого протокола под названием ASN.l (Abstract Syntax Notation). Протокол SNMP относится к прикладному уровню, он работает с протоколами IP и IPX. Он позволяет как собирать информацию о сети, так и управлять устройствами сети.

Протокол SNMP подразумевает хранение информации об устройствах сети в формате ASN.1 в виде текстовых файлов, каждый из которых называется MIB (Management Information Base — база управляющей информации). Например, в случае интеллектуального концентратора с него можно считать информацию о количестве пакетов, переданных и полученных каждым из портов, можно также включить и выключить каждый порт. Но это далеко не все возможности управления с помощью SNMP.

Чтобы управлять устройством сети, контроллер этого устройства должен выполнять программу агента SNMP. Программа агента собирают данные о системе, в которой они запущены и управляют объектами данных системы.

Рабочая станция, управляющая сетью (NMS — Network Management Station) — это один из компьютеров, подключенных к сети, на котором запущен специальный пакет прикладных программ, которые в удобном графическом виде отображают состояние сетевых устройств и позволяют управлять ими.

Протокол SNMP поддерживает три типа команд:

- Команда GET читает значения объектов данных устройства (из MIB) в произвольном порядке.
- Команда GET NEXT читает следующее по порядку значение объекта данных устройства.
- Команда SET применяется для изменений (записи) значений объектов данных устройства.

Команды и реакции протокола SNMP передаются посредством модулей данных в составе дейтаграмм (PDU — Protocol Data Unit). Протокол предусматривает также передачу информации о типе кодирования MIB, поэтому в разных устройствах MIB может иметь различный формат. Существует ряд фирменных и стандартных форматов MIB для сетевых адаптеров (MIB-II), концентраторов, мостов и сети в целом (RMON MIB), поддерживаемых SNMP.

9.3. Коммутирующие концентраторы Ethernet и Fast Ethernet

Коммутирующие концентраторы (Switched Hubs), они же коммутаторы или переключатели, могут рассматриваться, как простейший и очень быстрый мост. Они позволяют разделить единую сеть на несколько сетей для увеличения допустимого размера сети или для снижения нагрузки (трафика) в отдельных частях сети.

Как уже отмечалось, в отличие от мостов, коммутирующие концентраторы не принимают приходящие пакеты, а только переправляют из одной части сети в другую те пакеты, которые в этом нуждаются. Они в реальном темпе поступления битов распознают адрес приемника пакета и принимают решение о том, надо ли это пакет переправлять, и если надо, то кому. Никакой обработки пакетов не производится, поэтому коммутаторы практически не замедляют обмена по сети, но они не могут преобразовывать формата пакетов и протоколов обмена по сети. Так как коммутаторы работают с информацией, находящейся внутри кадра, часто говорят, что они ретранслируют кадры, а не пакеты, как репитерные концентраторы.

Коллизии коммутатором не ретранслируются, что выгодно отличает его от более простого репитерного концентратора.

Логическая структура коммутатора довольно проста (рис. 9.6). Она включает в себя так называемую перекрестную матрицу (crossbar matrix), во всех точках пересечения которой могут устанавливаться связи на время передачи пакета. В результате пакет, поступающий из любого сегмента, может быть передан в любой другой сегмент (рис. 9.6) или, в случае широковещательного пакета, — во все другие сегменты одновременно (рис. 9.7).

Коммутаторы выпускаются на различное число портов. Чаще всего встречаются коммутаторы с 6, 8, 12, 16 и 24 портами. Отметим, что мосты, как правило, редко поддерживают более 4 портов. Различаются коммутаторы и допустимым количеством адресов на один порт. Этот показатель определяет предельную сложность подключаемых к порту сегментов (количество компьютеров в каждом сегменте). Некоторые коммутаторы позволяют разбивать порты на группы, работающие независимо друг от друга, то есть один коммутатор может работать как два или три.

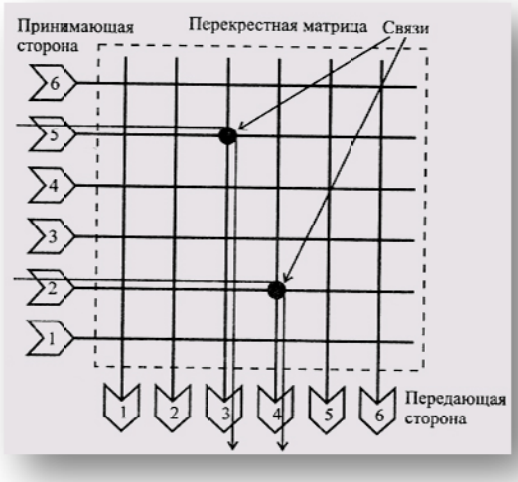


Рис. 9.6
Логическая схема коммутатора

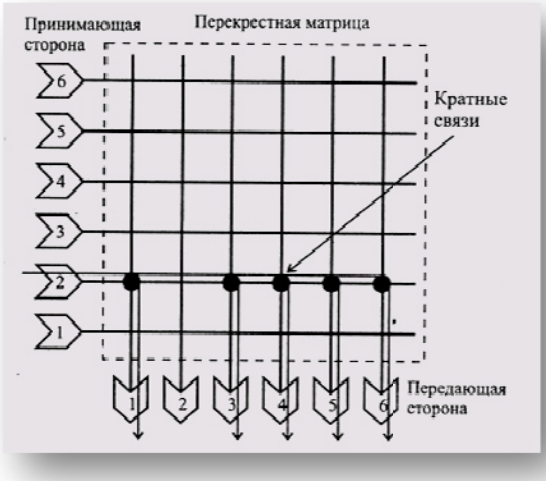


Рис. 9.7
Ретрансляция широковещательного пакета

Коммутаторы характеризуются двумя показателями производительности: максимальной и совокупной скоростью ретрансляции пакетов. Максимальная скорость ретрансляции измеряется при передаче пакетов из одного порта в другой, когда все остальные порты отключены. Совокупная скорость измеряется при активной работе всех имеющихся портов. Совокупная скорость больше максимальной, но максимальная скорость, как правило, не может быть обеспечена на всех портах одновременно, хотя коммутаторы и способны одновременно обрабатывать несколько пакетов (в отличие от моста).

Главное правило, которого надо придерживаться при разбиении сети на части (сегменты) с помощью коммутатора, называется «правило 80/20». Только при его выполнении коммутатор работает эффективно. Согласно этому правилу, надо обеспечить, чтобы не менее 80 процентов всех передач происходило в пределах одной части (одного сегмента) сети. И только 20 процентов всех передач должно быть между разными частями (сегментами) сети, проходить через коммутатор. На практике это обычно сводится к тому, что сервер и активно работающие с ним рабочие станции (клиенты) располагаются на одном сегменте. Это же правило 80/20 применимо и к мостам.

Существует два класса коммутаторов, отличающихся уровнем интеллек^-та и способами коммутации:

- коммутаторы со сквозным вырезанием (Cut-Through);
- коммутаторы с накоплением и ретрансляцией (Store-and-Forward, SAF).

Рассмотрим кратко их особенности.

9.3.1. Коммутаторы Cut-Through

Коммутаторы Cut-Through — самые простые и быстрые, они не производят никакого буферирования пакетов и никакой их селекции. Они буфе-рируют только головную часть пакета, чтобы прочитать 6-байтовый адрес приемника пакета и принять решение о коммутации, на которое у некоторых коммутаторов уходит около 10 битовых интервалов. В результате время ожидания ретрансляции (задержка на коммутаторе), включающее как время буферирования, так и время коммутации, может составлять около 150 битовых интервалов. Конечно, это больше задержки репитерного концентратора, но гораздо меньше задержки ретрансляции любого моста.

Недостаток данного типа коммутатора состоит в том, что он ретранслирует любые пакеты с нормальной головной частью, в том числе и заведомо ошибочные пакеты (например, с неправильной контрольной суммой) и карликовые пакеты (длиной менее 512 битовых интервалов). Ошибки одного сегмента ретранслируются в другой сегмент, что приводит к снижению пропускной способности сети в целом.

Еще одна проблема состоит в том, что коммутаторы данного типа часто перегружаются и плохо обрабатывают ситуацию перегрузки. Например, из двух или более сегментов поступают пакеты, адресованные одному и тому же сегменту. Но коммутатор не может одновременно передать несколько пакетов в один сегмент, поэтому часть пакетов пропадает. Не может коммутатор ретранслировать и пакеты, которые приходят из порта, в который коммутатор передает в данный момент.

Именно поэтому коммутаторы Cut-Trough постепенно вытесняются более совершенными.

Одно из усовершенствований коммутаторов получило название Interim Cut-Trough Switching (ICS). Оно направлено на то, чтобы избежать ретрансляции карликовых кадров. Для этого на принимающей стороне коммутатора все порты имеют буферную память FIFO на 512 бит. Если пакет заканчивается раньше, чем заполнится буфер, то содержимое буфера автоматически отбрасывается. Однако все остальные недостатки метода Cut-Through в данном случае сохраняются. Задержка ретрансляции коммутаторов данного типа увеличивается примерно на 400 битовых интервалов по сравнению с обычным Cut-Trough.

9.3.2. Коммутаторы Store-and-Forward

Коммутаторы Store-and-Forward (SAF) представляют собой наиболее дорогие, сложные и совершенные устройства данного типа. Они уже гораздо ближе к мостам и лишены перечисленных недостатков коммутаторов Cut-Trough. Главное их отличие состоит в полном буферировании во внутренней буферной памяти FIFO всех ретранслируемых пакетов. Размер каждого буфера при этом должен быть не меньше максимальной длины пакета. Соответственно значительно возрастает и задержка коммутации, она составляет не менее 12000 битовых интервалов. Карликовые и ошибочные кадры таким коммутатором отфильтровываются. Перегрузки возникают гораздо реже. /

Буферная память может размещаться на принимающей стороне всех портов (накопление перед коммутацией), на передающей стороне портов (накопление перед ретрансляцией), а также может быть общей для всех портов, причем эти методы часто комбинируются для достижения наибольшей гибкости и наивысшей производительности. Чем больше объем памяти, тем лучше коммутатор справляется с перегрузкой. Но с ростом объема памяти возрастает и стоимость оборудования. Иногда в состав коммутатора включается и процессор, но чаще коммутаторы выполняются на специализированных быстродействующих микросхемах, жестко специализированных именно на задачах коммутации пакетов.

Коммутаторы SAF, в отличие от других типов коммутаторов, могут поддерживать одновременно разные скорости передачи (10 Мбит/с и 100 Мбит/с). Полное буферирование пакета вполне позволяет передавать его не с той скоростью, с которой он поступил. В результате часть портов коммутатора может работать с сетью Ethernet, другая часть — с Fast Ethernet, причем некоторые коммутаторы автоматически настраивают свои порты на скорость передачи подключенного к порту сегмента. Поэтому коммутаторы SAF значительно облегчают переход с Ethernet на Fast Ethernet. Существуют уже коммутаторы, поддерживающие обмен с Gigabit Ethernet на скорости 1000 Мбит/с. Но в отличие от мостов коммутаторы, как правило, не меняют формат пакетов, поэтому сети с разными форматами пакетов нельзя объединять с их помощью.

Выпускаются также так называемые гибридные (или адаптивные) коммутаторы, которые могут автоматически переключаться из режима Cut-Through в режим SAF и наоборот. При малой нагрузке и при низком уровне ошибок они работают как более быстрые Cut-Through коммутаторы, а при большой нагрузке и при большом количестве ошибок переходят в более медленный, но более качественный режим SAF.

Наконец, еще одно важное достоинство коммутаторов по сравнению с ре-питерными концентраторами состоит в том, что они могут поддерживать режим полнодуплексной связи. Как уже отмечалось, при этом режиме резко упрощается обмен в сети, а скорость передачи в идеале удваивается (20 Мбит/с для Ethernet, 200 Мбит/с для Fast Ethernet).

Остановимся чуть подробнее на достоинствах и недостатках полнодуплексного режима.

Сегменты на витой паре и на оптоволоконном кабеле в любом случае используют две линии связи, одна из которых передает информацию в одну сторону, а другая — в другую. (Это не относится к сегментам 100BASE-T4, в которых есть двунаправленные витые пары, передающие в обе стороны по очереди). Но в стандартном полудуплексном режиме информация не передается по этим линиям связи одновременно. Однако если и адаптер, и коммутатор, связанные этими линиями связи, поддерживают полнодуплексный режим, то одновременная передача информации возможна. Естественно, аппаратура адаптера и коммутатора должна при этом обеспечивать прием приходящего из сети пакета и передачу своего пакета одновременно.

Полнодуплексный режим в принципе исключает любую возможность коллизии и делает ненужным сложный алгоритм управления обменом CSMA/CD. Каждый из абонентов (адаптер и коммутатор) может передавать в данном случае в любой момент без ожидания освобождения сети. В результате сеть нормально функционирует даже при нагрузке, приближающейся к 100% (в полудуплексном режиме — не более 30-40%). Особенно этот режим удобен для высокоскоростных серверов и высокопроизводительных рабочих станций.

Кроме того, отказ от метода CSMA/CD автоматически снимает ограничения на размер сети, связанные с ограничениями на двойное время распространения сигнала. Особенно это важно для Fast Ethernet и Gigabit Ethernet. При полнодуплексном режиме обмена размер любой сети ограничен только затуханием сигнала в среде передачи. Поэтому, например, сети Fast Ethernet и Gigabit Ethernet могут использовать оптоволоконные сегменты длиной 2 км и даже больше. При стандартном полудуплексном режиме, и методе CSMA/CD это было бы в принципе невозможно, так как двойное время распространения

сигнала для Fast Ethernet не должно превышать 5,12 мкс, а для Gigabit Ethernet — 0,512 мкс (а при переходе на минимальную длину пакета в 512 байт — 4,096 мкс).

Полнодуплексный режим можно рассматривать как приближение к топологии классической активной звезды. Как и в активной звезде, здесь не может быть конфликтов, но требования к центру (как по надежности, так и по быстродействию) чрезвычайно велики. Как и при активной звезде, строить сети с большим количеством абонентов затруднительно, необходимо использовать много центров (в нашем случае — коммутаторов). Как и при активной звезде, стоимость оборудования оказывается довольно высокой, так как кроме сетевых адаптеров и соединительных кабелей нужны сложные, быстрые и дорогие коммутаторы. Но, видимо, все это неизбежная плата за повышение скорости обмена. Строго говоря, полнодуплексные сети уже трудно назвать классическими Ethernet и Fast Ethernet, так как в них уже ничего не остается ни от топологии «шина», ни от метода CSMA/CD. Сохраняется только формат пакета и (не всегда) метод кодирования.

Таким образом, в настоящее время коммутирующие концентраторы (коммутаторы) выполняют все больше функций, традиционно относившихся к мостам. Поэтому в пределах одной сети или однотипных сетей с одинаковыми форматами пакетов (Ethernet и Fast Ethernet) коммутаторы все больше и больше вытесняют мосты, так как они более быстрые и более дешевые. На долю мостов остается только соединение разнотипных сетей, что встречается не так уж и часто. Эта тенденция прослеживается и в других областях электроники: узко специализированные быстрые устройства вытесняют универсальные медленные. Универсальные устройства (компьютеры, универсальные контроллеры) сохраняются только там, где без них действительно не обойтись, где нужны очень сложные алгоритмы обработки, которые к тому же могут изменяться в соответствии с требованиями конкретной задачи.

9.4. Мосты и маршрутизаторы Ethernet и Fast Ethernet

Мосты и маршрутизаторы, строго говоря, не совсем правильно относить к специфическому сетевому оборудованию. В большинстве случаев они представляют собой универсальные компьютеры, работающие в сети и выполняющие специфическую функцию соединения двух и более частей сети, хотя существуют мосты и маршрутизаторы, жестко специализированные на работе в сети. В частности, маршрутизаторы выпускаются рядом фирм в виде модулей, устанавливаемых в концентраторы на базе шасси. Понятно, что их стоимость ниже, чем маршрутизаторов на базе компьютеров.

9.4.1. Функции мостов

Мосты до недавнего времени были основными устройствами, применявшимися для разбиения сети на части (для сегментирования сети). Их стоимость меньше, чем маршрутизаторов, а быстродействие выше, к тому же они прозрачны для протоколов второго уровня модели OSI. Абоненты сети могут не знать о наличии в сети мостов, и все их пакеты доходят до нужного адресата по всей сети без всяких проблем.

Мост, как правило, представляет собой компьютер, в который установлено от двух до четырех сетевых адаптеров. Каждый из этих адаптеров соединен с одним из сегментов сети. Конфигурация сети с мостами может быть довольно сложной (рис. 9.8), но в ней не должно быть замкнутых маршрутов (петель), альтернативных путей доставки пакетов (рис. 9.9). В противном случае в результате многократного прохождения Широковещательных пакетов по замкнутому маршруту возникают перегрузки сети (так называемые широковещательные штормы) и ряд других проблем. Чтобы этого не происходило, в мостах предусматривается алгоритм ос-товного дерева (spanning tree), который позволяет в результате диалога между всеми мостами отключать порты, участвующие в создании петель (например, оба порта моста 2 на рис. 9.9).

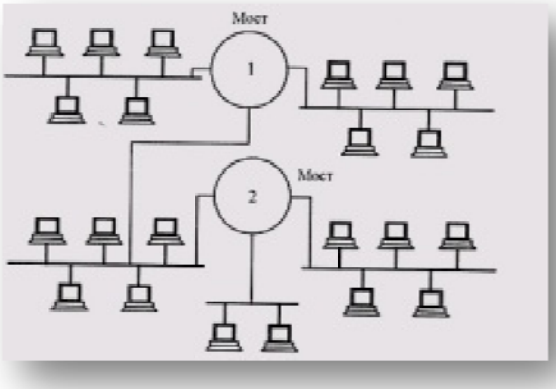


Рис.9.8
Сеть с мостами

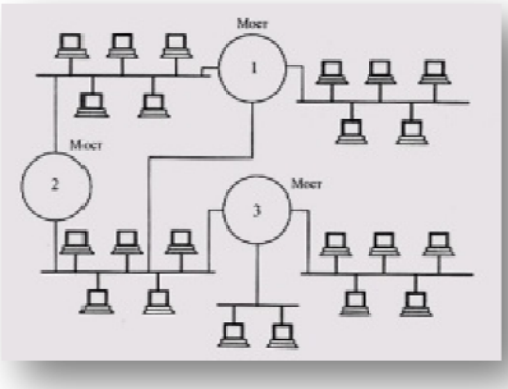


Рис. 9.9
Петля в сети с мостами

Благодаря этому можно специально дублировать соединение сегментов посредством мостов (создавать петли) для того, чтобы при отказе одной из линий связи автоматически восстанавливать целостность сети по альтернативному маршруту. Кстати, этот же алгоритм остовного дерева поддерживают и некоторые коммутаторы, которые тоже не способны работать в сети с петлями.

Мосты, как и коммутаторы, разделяют зону конфликта (область коллизии), но не разделяют широковещательную область (broadcast domain), то есть часть сети, в которой свободно проходят широковещательные пакеты. В результате нагрузка на каждый сегмент уменьшается, а ограничения на размер сети преодолеваются.

Одновременно мост может обрабатывать (ретранслировать) только один пакет, а не несколько, как коммутатор. Любой пакет, приходящий на один из портов, обрабатывается следующим образом:

1. Мост выделяет адрес источника (отправителя) пакета и ищет его в таблице адресов абонентов, относящейся к данному порту. Если этого адреса в таблицу нет, то он туда добавляется. Таким образом, автоматически формируется таблица адресов всех абонентов каждого сегмента из подключенных к портам моста.
2. Мост выделяет адрес приемника (получателя) пакета и ищет его в таблицах адресов, относящихся ко всем портам. Если пакет адресован в тот же сегмент, из которого он пришел, то он не ретранслируется (отфильтровывается). Если пакет широковещательный или многопунктовый (групповой), то он ретранслируется во все порты, кроме принявшего. Если пакет однопунктовый (адресован одному абоненту), то он ретранслируется только в тот порт, к которому присоединен сегмент с этим абонентом. Наконец, если адрес приемника не обнаружен ни в одной из таблиц адресов, то пакет посылается во все порты, кроме принявшего (как широковещательный).

Таблицы адресов абонентов имеют ограниченный размер, поэтому они формируются так, чтобы иметь возможность автоматического обновления их содержимого. Адреса тех абонентов, которые долго не присылают пакеты, через заданное время (обычно 5 минут) стираются из таблицы. Это гарантирует, что адрес абонента, отключенного от сети или перенесенного в другой сегмент, не будет занимать лишнего места в таблице.

Так как мост, как и коммутатор, анализирует информацию внутри кадра (физические адреса, MAC-адреса), часто говорят, что он ретранслирует кадры, а не пакеты (в отличие от репитера или репитерного концентратора).

Как и в случае коммутаторов, для эффективной работы моста необходимо выполнять упоминавшееся «правило 80/20», то есть большинство передач (не менее 80%) должно быть внутрисегментными, а не межсегментными.

Традиционно мосты подразделяются на внутренние и внешние.

Внутренние мосты выполняются на основе компьютера-сервера, в который устанавливают сетевые адаптеры (обычно до четырех), подключенные к разным сегментам сети. Строго говоря, именно эти сетевые адаптеры и соответствующие программные средства и называются внутренним мостом.

Внешний мост представляет собой рабочую станцию, в которую установлены два сетевых адаптера. В этом случае, в отличие от внутреннего моста, сегменты могут быть только однотипными (например, Ethernet-Ethernet).

Внешний мост может быть выделенным (dedicated) или невыделенным (non-dedicated) в зависимости от того, выполняет ли компьютер рабочей станции еще какие-нибудь функции, кроме сетевых. Термин «внешний» употребляется в этом случае по отношению к серверу, как основному компьютеру сети. В любой сети может присутствовать одновременно как внешний, так и внутренний мост или несколько мостов.

Как и коммутаторы Store-and-Forward, мосты могут поддерживать обмен между сегментами с разной скоростью передачи (Ethernet и Fast Ethernet), а также обеспечивать сопряжение полудуплексных и полнодуплексных сегментов. Полный прием пакетов в буферную память моста и их последующая передача легко решают подобные проблемы. Но мосты могут также сопрягать сети Ethernet и Fast Ethernet с сетями любых других типов, например, FDDI или Token-Ring, что не по силам большинству коммутаторов.

9.4.2. Функции маршрутизаторов

Вытесняя мосты, коммутаторы сильно потеснили и маршрутизаторы. Но маршрутизаторы работают на более высоком, третьем уровне модели OSI (мосты и коммутаторы — на втором), они имеют дело с протоколами более высоких уровней. Поэтому им, скорее всего, не грозит полное исчезновение.

Маршрутизаторы, как и мосты и коммутаторы, ретранслируют пакеты из одной части сети в другую (из одного сегмента в другой). Изначально маршрутизатор от моста отличался только тем, что на компьютере, соединяющем две или более части сети, было установлено другое программное обеспечение. Но между маршрутизатором и мостом существуют и принципиальные отличия.

Маршрутизаторы работают не с физическими адресами пакетов (MAC-адресами), а с логическими сетевыми адресами (IP-адресами).

Маршрутизаторы ретранслируют не всю приходящую информацию, а только ту информацию, которая адресована им лично, и отбрасывают широковещательные пакеты, разделяя тем самым широковещательную область сети. (Все абоненты должны знать о существовании в сети маршрутизатора.)

Самое главное — маршрутизаторы поддерживают сети с множеством возможных маршрутов, путей передачи информации, так называемые ячеистые сети (meshed networks). Пример такой сети показан на рис. 9.10. Мосты же требуют, чтобы в сети не было петель, чтобы путь распространения информации между двумя любыми абонентами был единственным.

Маршрутизаторы сложнее мостов и коммутаторов и, следовательно, дороже (например, стоимость коммутации примерно в 10 раз ниже стоимости маршрутизации). Маршрутизаторами сложнее управлять, они почти всегда значительно медленнее коммутаторов. Зато они обеспечивают самое глубокое разделение сети на части. Если репитерные концентраторы всего лишь повторяют все поступившие на них пакеты (уровень 1 модели OSI), а коммутаторы и мосты ретранслируют только межсегментные и широковещательные пакеты (уровень 2 модели OSI), то маршрутизаторы соединяют практически самостоятельные, не влияющие друг от друга сети, сохраняя при этом возможность передачи информации между ними (уровень 3 модели OSI).

Размер сети с маршрутизаторами практически ничем не ограничен: ни допустимыми размерами зоны конфликтов, ни допустимым количеством широковещательных пакетов (которые могут просто не оставлять места для обычных, однопунктовых пакетов), ни возможными для коммутаторов и мостов разнообразными перегрузками. При этом легко обеспечиваются альтернативные, дублирующие пути распространения информации для увеличения надежности связи.

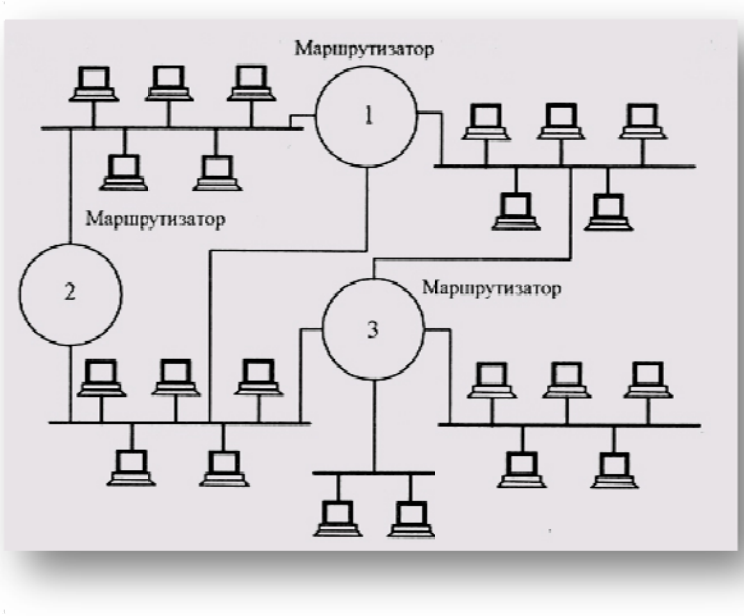


Рис. 9.10
Ячеистая сеть с маршрутизаторами

Именно маршрутизаторы чаще всего используются для связи локальных сетей с глобальными, в частности с сетью Internet, которая может рассматриваться как полностью маршрутизируемая сеть. Преобразовать протоколы локальных сетей в протоколы глобальных сетей для маршрутизатора вполне по силам.

Маршрутизаторы часто применяются для объединения опорной (стержневой) сетью типа FDDI множества локальных сетей (рис. 9.11) или для связи локальных сетей разных типов. Преобразование формата пакетов, требуемое в данной ситуации, для маршрутизатора не представляет никакой сложности. Например, большие пакеты сети FDDI могут разбиваться (фрагментироваться) на несколько меньших пакетов Ethernet.

Маршрутизаторы также легко преобразуют скорости передачи, связывая, например, между собой сети Ethernet, Fast Ethernet и Gigabit Ethernet. Не пропуская широковещательных пакетов, они лучше справляются с этой задачей, чем мосты или коммутаторы, так как защищают медленные сегменты от перегрузок со стороны быстрых сегментов.

Маршрутизаторы иногда объединяют между собой. Множество соединенных друг с другом маршрутизаторов могут образовывать так называемое облако (cloud), представляющее собой, по сути, один гигантский маршрутизатор. Такое соединение обеспечивает исключительно гибкую и

надежную связь между всеми подключенными к нему локальными сетями (рис. 9.12).

Рис. 9.11
Маршрутизируемая сеть на основе FDDI

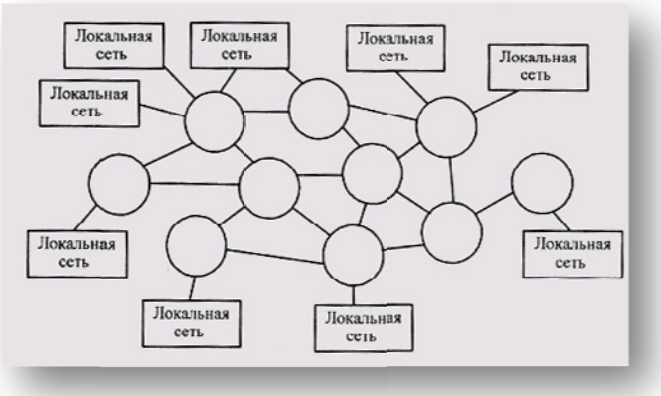


Рис. 9.12
Маршрутизируемое облако

Как уже отмечалось, можно считать, что репитерные концентраторы работают с пакетами, а мосты и коммутаторы — с кадрами. Маршрутизаторы обрабатывают адресную информацию, относящуюся к структуре дейтаграммы IP (IPX), которая вложена в область данных кадра, в свою очередь вложенного в пакет (см. рис. 3.3). Поэтому говорят, что они работают с дейтаграммами, ретранслируют дейтаграммы.

В дейтаграмму входят сетевые адреса, которые определяют абонентов (передающего и принимающего) в маршрутизованной сети, состоящей из множества обычных сетей. Например, сетевой адрес дейтаграммы IPX состоит из 10 байт (рис. 9.13) и включает в себя поле номера сети (4 байта), а также поле идентификатора абонента (6 байт), повторяющее физический адрес (MAC-адрес) абонента. Маршрутизатор обрабатывает именно поле номера сети из сетевого адреса принимающего абонента. Под сетью в данном случае понимается широковещательная область. То есть сеть, разделенная только мостами, коммутаторами и репитерными концентраторами, считается единой сетью с одним номером сети.

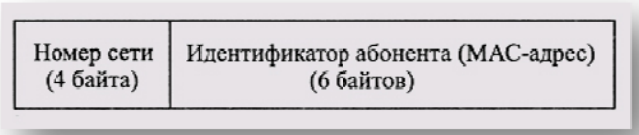


Рис. 9.13
Формат сетевого адреса IPX

Каждый абонент (узел), прежде чем послать пакет, определяет, может ли он послать его непосредственно получателю или же ему надо воспользоваться услугами маршрутизатора. Если номер собственной сети передающего абонента совпадает с номером сети абонента, которому должен передаваться пакет, то пакет передается непосредственно, без маршрутизации. Если же адресат находится в другой сети, то передаваемая дейтаграмма должна быть отправлена маршрутизатору, который затем переправит ее в нужную сеть. При этом получается, что пакет в целом адресован маршрутизатору (как одному из абонентов собственной сети), а заключенная в нем дейтаграмма адресована абоненту из другой сети, которому она, собственно, и предназначена. В поле сетевого адреса передатчика абонент в любом случае помещает номер своей собственной сети (4 байта) и свой MAC-адрес (6 байт).

Глава 10. Выбор конфигурации сетей Ethernet и Fast Ethernet

Содержание десятой главы:

10.1. Выбор конфигурации Ethernet

При выборе конфигурации сети Ethernet, состоящей из сегментов различных типов, возникает много вопросов, связанных прежде всего с максимально допустимым размером (диаметром)4сети и максимально возможным числом различных элементов. Сеть будет работоспособной только в том случае, если максимальная задержка распространения сигнала в ней не превысит предельной величины. Эта величина определяется выбранным методом управления обменом CSMA/CD, основанным на обнаружении и разрешении коллизий.

Прежде всего отметим, что для получения сложных конфигураций Ethernet из отдельных сегментов применяются концентраторы двух уже упоминавшихся основных типов:

репитерные концентраторы, которые представляют собой набор репитеров и никак логически не разделяют сегменты, подключенные к ним;

коммутирующие (switching) концентраторы или коммутаторы, которые передают информацию между сегментами, но не передают конфликты с сегмента на сегмент.

В случае более сложных коммутирующих концентраторов конфликты в отдельных сегментах решаются на месте, в самих сегментах, и не распространяются по сети, как в случае более простых репитерных

концентраторов. Это имеет принципиальное значение для выбора топологии сети Ethernet, так как используемый в ней метод доступа CSMA/ CD предполагает наличие конфликтов и их разрешение, причем общая длина сети как раз и определяется размером зоны конфликта, области коллизии (collision domain). Таким образом, применение репитерного концентратора не разделяет зону конфликта, в то время как каждый коммутирующий концентратор делит зону конфликта на части. В случае коммутатора оценивать работоспособность надо для каждой части сети отдельно, а в случае репитерных концентраторов надо оценивать работоспособность всей сети в целом.

На практике репитерные концентраторы применяются гораздо чаще, так как они проще и дешевле. Поэтому мы будем в основном говорить в дальнейшем именно о них.

При выборе и оценке конфигурации Ethernet используются две основные модели. Остановимся кратко на их особенностях.

10.1.1. Правила модели 1

Первая модель формулирует набор простых правил, которые необходимо соблюдать проектировщику сети при соединении отдельных компьютеров и сегментов.

1. Репитер или концентратор, подключенный к сегменту, снижает на единицу максимально допустимое число абонентов, подключаемых к сегменту.

2. Полный путь между двумя любыми абонентами должен включать в себя не более пяти сегментов, четырех концентраторов (репитеров) и двух трансиверов (MAU) для сегментов 10 BASES.

3.Если путь между абонентами состоит из пяти сегментов и четырех концентраторов (репитеров), то количество сегментов, к которым подключены компьютеры, не должно превышать трех, а остальные сегменты должны просто связывать между собой концентраторы (репитеры). Это так называемое «правило 5-4-3».

4. Если путь между абонентами состоит из четырех сегментов и трех концентраторов (репитеров), то должны выполняться следующие условия:

- максимальная длина оптоволоконного кабеля сегмента 10BASE-FL, соединяющего между собой концентраторы (репитеры), не должна превышать 1000 м;
- максимальная длина оптоволоконного кабеля сегмента 10BASE-FL, соединяющего концентраторы (репитеры) с компьютерами, не должна превышать 400 м;
- ко всем сегментам могут подключаться компьютеры.

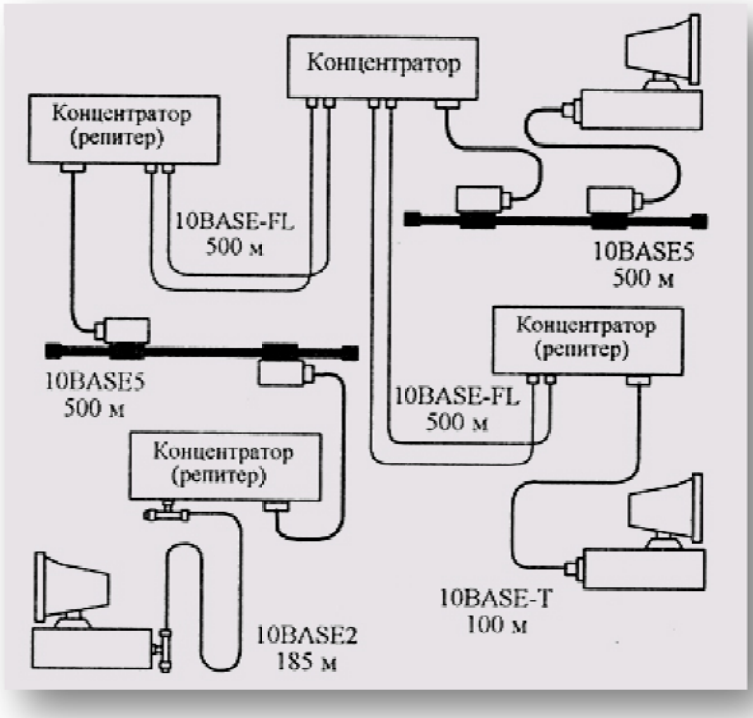


Рис. 10.1
Пример максимальной конфигурации в соответствии с первой моделью

При выполнении этих правил можно быть уверенным, что сеть будет работоспособной. Никаких дополнительных расчетов в данном случае не требуется. Считается, что соблюдение данных правил гарантирует допустимую величину задержки сигнала в сети.

На рис. 10.1 показан пример максимальной конфигурации, удовлетворяющей этим правилам. Здесь максимально возможный путь (диаметр сети) проходит между двумя нижними по рисунку абонентами: он включает в себя пять сегментов (10BASE2, 10BASE5, 10BASE-FL, 10BASE-FL и 10BASE-T), четыре концентратора (репитера) и два трансивера MAU.

10.1.2. Расчет по модели 2

Вторая модель, применяемая для оценки конфигурации Ethernet, основана на точном расчете временных характеристик выбранной конфигурации сети. Она иногда позволяет выйти за пределы жестких ограничений модели 1. Применение модели 2 совершенно необходимо в том случае, когда размер проектируемой сети близок к максимально допустимому.

В модели 2 используются две системы расчетов:

- первая система предполагает вычисление двойного (кругового) времени прохождения сигнала по сети и сравнение его с максимально допустимой величиной;
- вторая система проверяет допустимость величины получаемого межкадрового временного интервала, межпакетной щели (IPG — InterPacket Gap) в сети.

При этом вычисления в обеих системах расчетов ведутся для наихудшего случая, для пути максимальной длины, то есть для такого пути передаваемого по сети пакета, который требует для своего прохождения максимального времени. При первой системе расчетов выделяются три типа сегментов:

- начальный сегмент — это сегмент, соответствующий началу пути максимальной длины;
- конечный сегмент — это сегмент, расположенный в конце пути максимальной длины;
- промежуточный сегмент — это сегмент, входящий в путь максимальной длины, но не являющийся ни начальным, ни конечным.

Табл. 10.1. Величины задержек для расчета двойного времени прохождения сигнала (задержки даны в битовых интервалах)

Тип сегмента Ethernet	Макс, длина м	Начальный сегмент		Промежуточный сегмент	Конечный сегмет tm		Задержка на метр длины,
10BASE5	500	11, 8	55,0	46,5 89,8	169,5	212,8	0,087
10BASE2	185	11, 8	30,8	46,5 65,5	169,5	188,5	0,103
10BASE-T	100	15, 3	26,6	42,0 53,3	165,0	176,3	0,113
10BASE-FL	2000	12, 3	212,3	33,5 233,5	156,5	356,5	0,100
FOIRL	1000	7,8	107,8	29,0 129,0	152,0	252,0	0,100
AUI	50	0	5,1	0 5,1	0	5,1	0,103

Промежуточных сегментов в выбранном пути может быть несколько, а начальный и конечный сегменты при разных расчетах могут меняться местами друг с другом. Выделение трех типов сегментов позволяет автоматически учитывать задержки сигнала на всех концентраторах, входящих в путь максимальной длины, а также в приемопередающих узлах адаптеров.

Для расчетов используются величины задержек, представленные в таблице 10.1. Методика расчета сводится к следующему.

1. В сети выделяется путь максимальной длины. Все дальнейшие расчеты ведутся для него. Если этот путь не очевиден, то расчеты ведутся для всех возможных путей, и на основании этих расчетов выбирается путь максимальной длины.

2. Если длина сегмента, входящего в выбранный путь, не максимальна, то рассчитывается двойное (круговое) время прохождения в каждом сегменте выделенного пути по формуле: ts = LtL + to, где L — длина сегмента в метрах (при этом надо учитывать тип сегмента: начальный, промежуточный или конечный).

3. Если длина сегмента равна максимально допустимой, то из таблицы для него берется величина максимальной задержт ки t .

4. Суммарная величина задержек всех сегментов выделенного пути не должна превышать предельной величины 512 битовых интервалов (51,2 мкс).

5. Выполняются те же действия для обратного направления выбранного пути (то есть конечный сегмент считается начальным, и наоборот). Из-за разных задержек передающих и принимающих узлов концентраторов величины задержек в разных направлениях могут отличаться (правда, не слишком сильно).

6. Если задержки в обоих случаях не превышают величины 512 битовых интервалов, то сеть считается работоспособной.

Например, для конфигурации, показанной на рис. 10.1, путь наибольшей длины — это путь между двумя нижними по рисунку компьютерами. В данном случае это довольно очевидно. Этот путь включает в себя пять сегментов (слева направо): 10BASE2,10BASE5,10BASE-FL (два сегмента) и 10BASE-T.

Произведем расчет, считая начальным сегментом 10BASE2, а конечным -10BASE-T.

1. Начальный сегмент 10BASE2 имеет максимально допустимую длину (185 м), следовательно, для него берем из таблицы величину задержки 30,8.

2. Промежуточный сегмент 1 OBASE5 также имеет максимально допустимую длину (500 м), поэтому для него берем из таблицы величину задержки 89,8.

3. Оба промежуточных сегмента 10BASE-FL имеют длину 500 м, следовательно, задержка каждого из них будет вычисляться по формуле:

500 • 0,100 + 33,5 = 83,5.

1. Конечный сегмент 10BASE-T имеет максимально допустимую длину (100 м), поэтому из таблицы берем для него величину задержки 176,3.

2. В путь наибольшей длины входят также шесть АШ-кабе-лей: два из них (в сегменте 10BASE5) показаны на рисунке, а четыре (в двух сегментах 10BASE-FL) не показаны, но в реальности вполне могут присутствовать. Будем считать, что суммарная длина всех этих кабелей равна 200 м, то есть четырем максимальным длинам. Тогда задержка на всех АШ-кабелях будет равна

4 • 5,1 = 20,4.

1. В результате суммарная задержка для всех пяти сегментов составит:

30,8 + 89,8 + 83,5 + 83,5 + 176,3 + 20,4 = 484,3,

что меньше, чем предельно допустимая величина 512, то есть сеть работоспособна.

произведем теперь расчет суммарной задержки для того же пути, но в)братном направлении. При этом начальным сегментом будет 10BASE-T, і конечным — 10BASE2. В конечной сумме изменятся только два слагаемых (промежуточные сегменты остаются промежуточными). Для началь-гого сегмента 10BASE-T

максимальной длины задержка составит 26,6 >итовых интервалов, а для конечного сегмента 10BASE2 максимальной (лины задержка составит 188,5 битовых интервалов. Суммарная задер-кка будет равняться

26,6 + 83,5 + 83,5 + 89,8 + 188,5 + 20,4 = 492,3, то опять же меньше 512.

Работоспособность сети подтверждена.

Однако расчета двойного времени прохождения, в соответствии со стандартом, еще не достаточно, чтобы сделать окончательный вывод о работоспособности сети.

Второй расчет, применяемый в модели 2, проверяет соответствие стандарту величины межкадрового интервала (IPG). Эта величина изначально не должна быть меньше, чем 96 битовых интервалов (9,6 икс), то есть только через 9,6 мкс после освобождения сети абоненты могут начать свою передачу. Однако при прохождении пакетов (кадров) через репитеры и концентраторы межкадровый интервал может сокращаться, вследствие чего два пакета могут в конце концов восприниматься абонентами как один. Допустимое сокращение IPG определено стандартом в 49 битовых интервалов (4,9 мкс).

Табл. 10.2. Величины сокращения межкадрового интервала (IPG) для разных сегментов Ethernet

Сегмент	Начальный	Промежуточный
10BASE2	16	11
10BASE5	16	11
10BASE-T	16	11
10BASE-FL	11	8

Для вычислений здесь так же, как и в предыдущем случае, используются понятия начального сегмента и промежуточного сегмента. Конечный сегмент не вносит вклада в сокращение межкадрового интервала, так как пакет доходит по нему до принимающего компьютера без прохождения репитеров и концентраторов.

Вычисления здесь очень простые. Для них используются данные табл. 10.2.

Для получения полной величины сокращения IPG надо просуммировать величины из таблицы для сегментов, входящих в путь максимальной длины, и сравнить сумму с предельной величиной 49 битовых интервалов. Если сумма меньше 49, мы можем сделать вывод о работоспособности сети. Для гарантии расчет производится в обоих направлениях выбранного пути.

Для примера обратимся все к той же конфигурации, показанной на рис. 10.1. Максимальный путь здесь — между двумя нижними по рисунку компьютерами. Берем в качестве начального сегмента 10BASE2. Для него сокращение межкадрового интервала равно 16. Далее следуют промежуточные сегменты: 10BASE5 (величина сокращения составит 11) и два сегмента 10BASE-FL (каждый из них внесет свой вклад по 8 битовых интервалов). В результате суммарное сокращение межкадрового интервала составит:

16 + 11+8 + 8 = 43,

что меньше предельной величины 49. Следовательно, данная конфигурация и по этому показателю будет работоспособна.

Вычисления для обратного направления по этому же пути дадут в данном случае тот же результат, так как начальный сегмент 10BASE-T даст ту же величину, что и начальный сегмент 10BASE2 (16 битовых интервалов), а все промежуточные сегменты опять же останутся промежуточными.

Попробуем теперь с помощью второй модели расчетов оценить, каков может быть максимальный размер сети Ethernet. Теоретически возможный размер сети составляет 6,5 км — в предположении, что вся сеть выполнена на одном сегменте. Однако в реальности это невозможно, ведь предельная длина сегмента не превышает 2 км (для 10BASE-FL). Поэтому присутствие репитеров или концентраторов в сети максимального размера обязательно, а они внесут свой вклад в задержку прохождения сигнала по сети.

Возьмем простейшую конфигурацию сети из двух сегментов 10BASE-FL, соединенных концентратором (рис. 10.2).

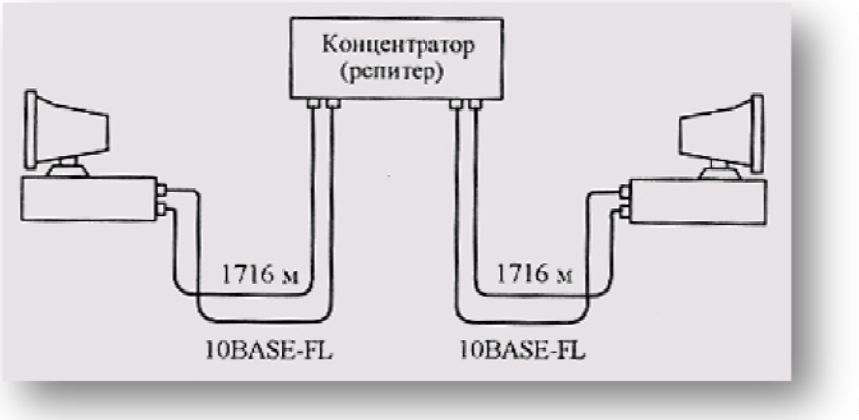


Рис. 10.2
Сеть Ethernet максимально возможной длины

Из таблицы 10.1 видно, что при выборе максимальной длины обоих сегментов по 2000 метров (один из них будет начальным, а другой — конечным) суммарная двойная задержка распространения составит:

212,3 + 356,5 = 568,8,

сто значительно больше допустимой величины 512. То есть реальная длина :ети будет даже меньше, чем 4 км. Элементарный расчет показывает, что три двух одинаковых сегментах 10BASE-FL длина каждого из них не дол

жна превышать 1716 м. Двойная задержка распространения при этом будет вычисляться так (табл. 10.1):

12,3 + 1716 • 0,1+ 156,5 + 1716 • 0,1 = 512.

И общая длина сети будет при этом составлять 3432 м, что значительно меньше теоретически возможной длины в 6500 м. Отметим, что сегменты в конфигурации на рис. 10.2 могут быть и разной длины, но их общая длина не должна превышать все тех же 3432 м. При этом стоит еще учитывать, что мы не включали в расчет задержки трансиверных кабелей. Если используются внешние трансиверы, то необходимо еще уменьшить длину оптоволоконных кабелей.

Попробуем теперь оценить максимально возможный размер сети при использовании только электрического кабеля, например, наиболее популярной сейчас витой пары.

Допустим, мы имеем конфигурацию из пяти сегментов 10BASE-T предельно допустимой длины (100 м), соединенных между собой четырьмя концентраторами. Задержка начального сегмента составит (из табл. 10.1) 26,6 битовых интервалов. Задержка конечного сегмента будет равна 176,3 битовых интервалов. Задержка трех промежуточных сегментов будет 53,3 битовых интервала на каждый сегмент. Итого суммарная задержка равняется:

26,6 + 176,3 + 3 • 53,3 = 362,8, что меньше предельной величины 512.

Мы можем добавить еще два промежуточных 100-метровых сегмента, которые дадут еще 106,6, увеличив количество сегментов до 7, а количество концентраторов до 6. И еще останется запас в 42,6 битовых интервалов. Всего получаем, что сегментов может быть даже 8 при семи концентраторах, а общая длина всех кабелей может достигать 705,3 м. Это значительно превышает ограничения модели 1.

Но подсчитаем, какая величина сокращения межкадрового интервала получается при такой конфигурации. Один начальный сегмент даст 16 битовых интервалов (см. табл. 10.2). Шесть промежуточных сегментов дадут 77 битовых интервалов. В сумме получится 93 битовых интервала, что значительно превышает разрешенные 49 битовых интервалов. Поэтому в данном случае предельная длина сети будет ограничена пятью сегментами, которые сократят межкадровый интервал на величину 16+11 • 3 = 49 битовых интервалов.

В результате сеть максимального размера на витой паре будет состоять из пяти сегментов по 100 м (рис. 10.3), что совпадает с требованиями модели 1. Полная длина сети составит 500 м.

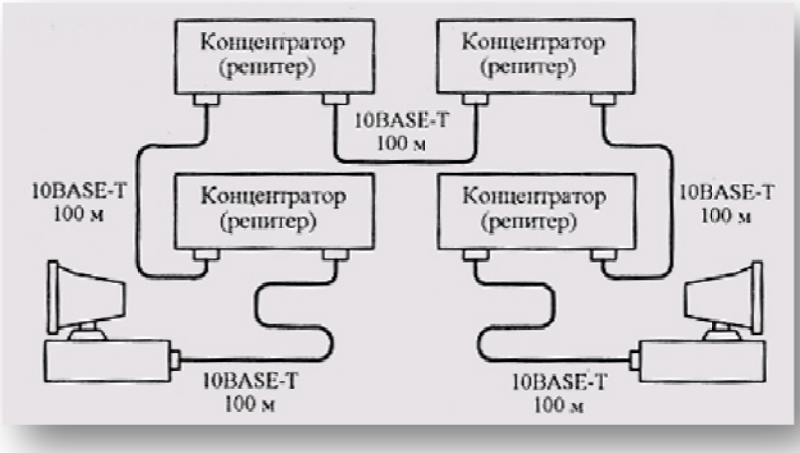


Рис. 10.3
Сеть Ethernet максимального размера на витой паре

Интересно, что пути максимальной длины для расчета круговой задержки и для расчета IPG могут быть различными. Вполне возможна ситуация, когда максимальную задержку прохождения дает один путь в сети, а максимальное сокращение IPG дает другой путь. Например, если один путь состоит из пяти коротких сегментов (электрических и оптоволоконных) и четырех концентраторов, а другой путь имеет всего два оптоволоконных сегмента, но зато с суммарной длиной, близкой к максимально возможной, то первый даст максимальное сокращение IPG, а второй — максимальную задержку прохождения сигнала.

Значит, в идеале необходимо рассчитывать как круговую задержку, так и сокращение IPG для каждого из возможных путей в данной топологии сети. А условие работоспособности сети будет состоять в том, что все задержки всех путей должны быть меньше 512 битовых интервалов, а все величины сокращения IPG для всех путей должны быть меньше 49 битовых интервалов. Правда, неоднозначность пути максимальной длины надо учитывать только в том случае, когда в сети присутствует больше четырех концентраторов, так как четыре концентратора (пять сегментов) в принципе не могут уменьшить APG больше, чем на 49 битовых интервалов при выборе любых возможных сегментов (см. табл. 10.2).

Таким образом, для оценки работоспособности той или иной конфигурации можно использовать обе модели (модель 1 и модель 2), хотя для сложных топологий и предельно длинных сегментов предпочтительнее вторая (числовая) модель, позволяющая количественно оценить временные характеристики сети. В случае же более простых топологий вполне достаточно проверить выполнение элементарных правил первой модели, что не требует никаких расчетов.

10.2. Выбор конфигурации Fast Ethernet

Точно так же, как и в случае Ethernet, для определения работоспособности сети Fast Ethernet стандарт IEEE 802.3 предлагает две модели, называемые Transmission System Model 1 и Transmission System Model 2. При этом первая модель основана на нескольких несложных правилах, а вторая использует систему точных расчетов. Первая модель исходит из того, что все компоненты сети (в частности, кабели) имеют наихудшие из возможных временные характеристики, поэтому она всегда дает результат со значительным запасом. Во второй модели можно использовать реальные временные характеристики кабелей, поэтому ее применение позволяет иногда преодолеть жесткие ограничения модели 1.

10.2.1. Правила модели 1

В соответствии с первой моделью, при выборе конфигурации в любом случае надо руководствоваться следующими принципами:

Сегменты, выполненные на электрических кабелях (витых парах) не должны быть длиннее 100 м. Это относится к кабелям всех возможных категорий — 3, 4 и 5, к сегментам 100BASE-T4 и 100BASE-TX.

Сегменты, выполненные на оптоволоконных кабелях, не должны быть длиннее 412м.

Если используются адаптеры с внешними (выносными) трансиверами, то трансиверные кабели (МП) не должны быть длиннее 50 см.

Рис. 10.4
Двухточечное соединение без концентратора

Модель 1 выделяет три возможных конфигурации сети Fast Ethernet:

1. Соединение двух абонентов (узлов) сети напрямую, без репитера или концентратора (рис. 10.4). Абонентами при этом могут выступать не только компьютеры, но и сетевой принтер, порт коммутатора, моста или маршрутизатора. Это соединение называется соединением DTE—DTE или двухточечным.

2. Соединение двух абонентов сети с помощью одного репитер-ного концентратора класса I или класса II (рис. 10.5).

3. Соединение двух абонентов сети с помощью двух репитер-ных концентраторов класса II (рис. 10.6). При этом предполагается, что для связи концентраторов всегда используется электрический кабель длиной не более 5 м. Концентраторы класса II имеют меньшую задержку, поэтому их может быть два. Использование трех концентраторов не допускается в соответствии с моделью 1 ни в коем случае.

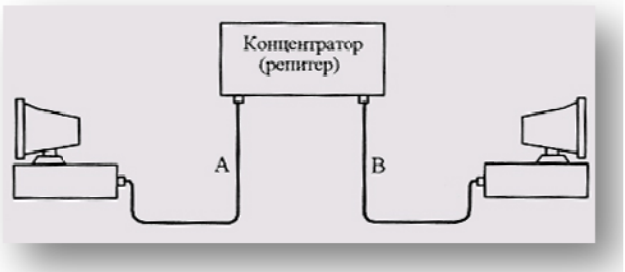


Рис. 10.5
Соединение с одним концентратором

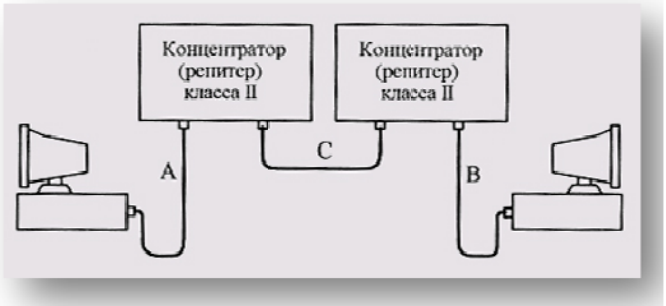


Рис. 10.6
Соединение сдвумя концентраторами

В случае первой конфигурации правила модели 1 предельно простые: электрический кабель не должен быть длиннее 100 м, полудуплексный оптоволоконный не должен быть длиннее 412м, полнодуплексный оптоволоконный — 2000 м (при этом задержка сигнала в кабеле уже не имеет значения, так как метод CSMA/CD не работает).

В случае применения конфигурации с одним концентратором надо ограничивать длину кабелей сети в соответствии с таблицей 10.3.

В случае выбора конфигурации с двумя концентраторами надо ограничивать длину кабелей A и B в соответствии с таблицей 10.4 (по умолчанию предполагается, что кабель C имеет длину 5 м).

Табл. 10.3. Максимальная длина кабелей в конфигурации с одним концентратором

Вид кабеля A	Вид кабеля B	Класс концентратора	Макс, длина кабеля A	Макс, длина кабеля B	Макс, размер сети, м
TX, T4	TX.T4	I или II	100	100	200
тх	FX	I	100	160,8	260,8
T4	FX	I	100	131	231
FX	FX	I	136	136	272
TX	FX	II	100	208,8	308,8
T4	FX	II	100	204	304
FX	FX	II	160	160	320

Табл. 10.4. Максимальная длина кабелей в конфигурации с двумя концентраторами

Вид кабеля A	Вид кабеля B	Макс,	длина	Макс,	длина	Макс,

		кабеля A, м	кабеля B, м	размер сети
TX,T4	TX,T4	100	100	205
TX	FX	100	116,2	221,2
T4	FX	100	136,3	241,3
FX	FX	114	114	233

В обеих конфигурациях с концентраторами при использовании одновременно электрического и оптоволоконного кабелей можно за счет уменьшения длины электрического кабеля увеличить длину оптоволоконного кабеля. Причем уменьшению длины электрического кабеля на 1 м соответствует увеличение длины оптоволоконного кабеля на 1,19 м. Например, уменьшив кабель TX на 10 м, можно увеличить кабель FX на 11,9 м, и его предельная длина составит при двух концентраторах 128,1 м. Немного увеличится и предельный размер сети (в нашем примере на 1,9 м).

В случае использования двух оптоволоконных кабелей можно уменьшать один из кабелей за счет увеличения другого. При уменьшении одного кабеля на 10 м можно увеличить другой тоже на 10м. Если же используется два электрических кабеля, то увеличивать один из них за счет уменьшения другого нельзя, так как их длина в принципе не может превышать 100 м из-за затухания сигнала в кабеле.

Отметим, что концентратор класса II в принципе не может одновременно поддерживать сегменты с разными методами кодирования TX/FX и T4. Поэтому варианты, соответствующие вторым снизу строкам обеих таблиц 10.3 и 10.4 никогда не реализуются на практике, но стандарт почему-то дает цифры и для них.

Во всех перечисленных случаях под размером сети понимается размер зоны конфликта (области коллизии, collision domain). При этом надо учитывать, что включение в сеть одного коммутатора позволяет увеличить полный размер сети вдвое.

Пример сети максимальной конфигурации в соответствии с первой моделью для витой пары показан на рис. 10.7.

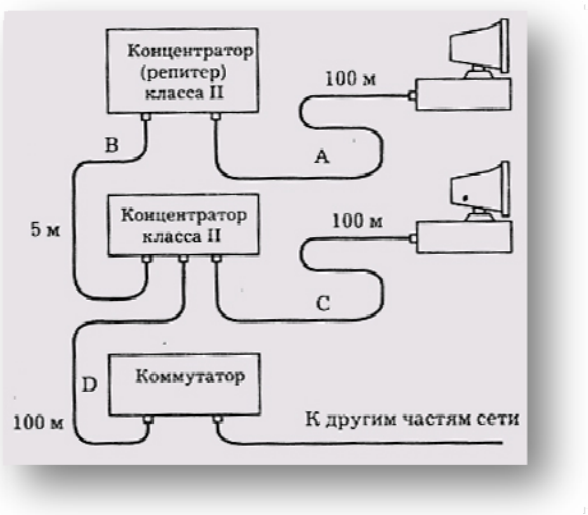


Рис. 10.7
Пример максимальной конфигурации сети Fast Ethernet

Здесь максимальный размер зоны конфликта складывается из сегментов A, B и C, то есть составляет:

100 + 5 + 100 = 205 метров,

что удовлетворяет условию работоспособности сети (табл. 10.4, верхняя строчка). Отметим, что сегмент D также входит в зону конфликта, так как коммутатор тоже является полноправным передатчиком пакетов сети. Поэтому длина сегмента D также не может превышать в нашем случае 100 м, чтобы суммарная длина сегментов A, B и D не превысила все тех же 205 м. Сегменты, отделенные от рассматриваемой зоны конфликта коммутатором, никак не влияют на ее работоспособность.

10.2.2. Расчет по модели 2

Вторая модель для сети Fast Ethernet, как и в случае Ethernet, основана на вычислении суммарного двойного времени прохождения сигнала по сети. В отличие от второй модели, используемой для оценки конфигурации Ethernet, здесь не проводится расчетов величины сокращения межкадрового интервала (межпакетной щели, IPG). Это связано с тем, что даже максимальное количество репитеров и концентраторов, допустимых в Fast Ethernet, в принципе не может вызвать недопустимого сокращения межкадрового интервала.

Табл. 10.5. Двойные задержки компонентов сети Fast Ethernet (величины задержек даны в битовых интервалах)

Тип сегмента	Задержка на метр	Макс, задержка
Два абонента TX/FX	—	100
Два абонента T4	—	138
Один абонент T4 и один TX/FX	—	127
Сегмент на кабеле категории 3	1,14	114 (100м)
Сегмент на кабеле категории 4	1,14	114 (100м)
Сегмент на кабеле категории 5	1,112	111,2 (100м)
Экранированная витая пара	1,112	111, 2 (100м)
Оптоволоконный кабель	1,0	412 (412м)
Репитер (концентратор) класса I	—	140
Репитер (концентратор) класса II с портами TX/FX	—	92
Репитер (концентратор) класса II с портами T4	—	67

Для расчетов в соответствии со второй моделью сначала надо выделить в сети путь с максимальным двойным временем прохождения и максимальным числом репитеров (концентраторов) между компьютерами, то есть путь максимальной длины. Если таких путей несколько, то расчет должен производиться для каждого из них.

Расчет в данном случае ведется на основании таблицы 10.5.

Для вычисления полного двойного (кругового) времени прохождения для сегмента сети необходимо умножить длину сегмента на величину задержки на метр, взятую из второго столбца таблицы. Если сегмент имеет максимально возможную длину, то можно сразу взять величину максимальной задержки для данного сегмента из третьего столбца таблицы. Затем задержки сегментов, входящих в путь максимальной длины, надо просуммировать и прибавить к этой сумме величину задержки для приемопередающих узлов двух абонентов (это три верхние строчки таблицы) и величины задержек для всех репитеров (концентраторов), входящих в данный путь (это три нижние строки таблицы). Суммарная задержка должна быть меньше, чем 512 битовых интервалов. При этом надо помнить, что стандарт IEEE 802.3u рекомендует оставлять запас в пределах 1-4 битовых интервалов для учета кабелей внутри соединительных шкафов и погрешностей измерения, то есть лучше сравнивать суммарную задержку с величиной 508 битовых интервалов, а не 512 битовых интервалов.

Все задержки, приведенные в таблице, даны для наихудшего случая. Если известны временные характеристики конкретных кабелей, концентраторов и адаптеров, то практически всегда лучше использовать именно их. В ряде случаев это может дать заметную прибавку к допустимому размеру сети.

Рассмотрим пример расчета по второй модели для сети, показанной на рис. 10.7. Здесь существуют два максимальных пути: между компьютерами (сегменты A, B и C) и между верхним (по рисунку) компьютером и коммутатором (сегменты A, B и D). Оба эти пути включают в себя два 100-метровых сегмента и один 5-метровый. Предположим, что все сегменты представляют собой 100BASE-TX и выполнены на кабеле категории 5. Произведем расчет работоспособности сети.

1. Для двух 100-метровых сегментов (максимальной длины) из таблицы берем величину задержки 111,2 битовых интервалов.

2. Для 5-метрового сегмента высчитываем задержку, умножая 1,112 (задержка на метр) на длину кабеля (5 метров): 1,112 • 5 = 5,56 битовых интервалов.

3. Берем из таблицы задержку для двух абонентов TX — 100 битовых интервалов.

4. Берем из таблицы величины задержек для двух репитеров класса II — по 92 битовых интервала.

5.Суммируем все перечисленные задержки и получаем: 111,2 + 111,2 + 5,56 + 100 + 92 + 92 = 511,96, что меньше 512, следовательно, данная сеть будет работоспособна, хотя и на пределе, что, вообще говоря, не рекомендуется.

Для гарантии лучше несколько уменьшить длину кабелей или взять кабели, имеющие меньшую задержку (см. табл. 2.3). Например, при использовании кабеля AT&T 1061 (NVP = 0,7, t3= 0,477) мы получим следующие величины задержек для 100-метровых сегментов: (0,477 • 2) • 100 = 95,4 битовых интервалов (умножение на два необходимо, чтобы получить двойное время прохождения), а для 5-метрового сегмента — 4,77 битовых интервалов. Суммарная задержка при этом составит:

95,4 + 95,4 + 4,77 + 100 + 92 + 92 = 483,57,

то есть гораздо меньше 512 и даже 508, что означает полностью работоспособную сеть.

Пользуясь моделью 2, можно обойти некоторые ограничения модели 1, так как модель 1 рассчитывается для наихудшего случая. Например, в сети может присутствовать больше двух концентраторов класса II или больше одного концентратора класса I, а кабель, соединяющий концентраторы, может быть длиннее 5 м.

Для примера на рис. 10.8 показана сеть, содержащая три концентратора класса II, соединенных между собой отрезками кабеля длиной по 10 м. Компьютеры присоединены к концентраторам сегментами 100BASE-TX длиной по 50 м. Произведем расчет двойного времени прохождения для этого случая.

1. Каждый из трех концентраторов класса II с портами TX даст задержку 92 битовых интервала. Суммарная задержка концентраторов будет равна 276 битовым интервалам.

2. Для двух соединительных кабелей между концентраторами задержка равна 2 • 1,112 • 10 = 2,24 битовых интервала.

3. Для двух сегментов TX по 50 метров задержка составит 2 • 1,112 • 50 = 111,2 битовых интервала.

4. Для двух абонентов TX задержка будет равна 100 битовым интервалам.

5. Итого суммарная задержка будет составлять:

276 + 22,24+ 111,2 + 100 = 509,44 битовых интервала. Данная сеть работоспособна, но при этом надо учитывать, что каждый дополнительный концентратор класса II уменьшает общую допустимую длину кабеля на величину 92/1,112 = 82,7 м. Сеть с четырьмя концентраторами уже не будет иметь смысла, так как на задержку в кабеле уже не остается почти никакого запаса (четыре концентратора дадут суммарную задержку в 92 • 4 = 368 битовых интервалов).

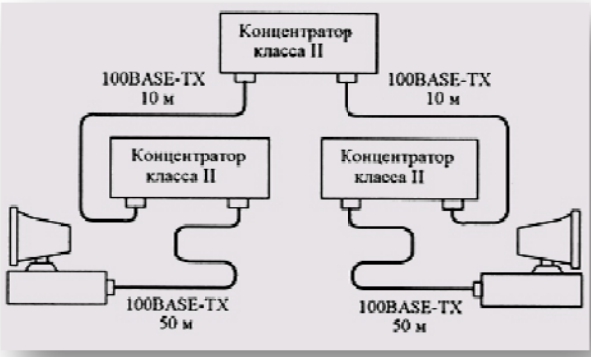


Рис. 10.8
Пример работоспособной конфигурации сети, нарушающей правила модели 1

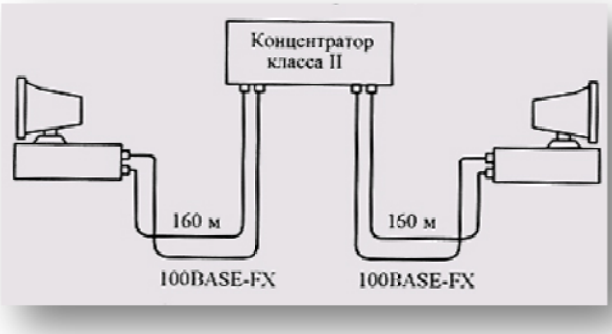


Рис. 10.9
Сеть Fast Ethernet максимальной длины

А теперь посмотрим, какова может быть максимальная величина сети Fast Ethernet. Для этого надо взять сеть с одним концентратором класса II и два сегмента 100BASE-FX. Элементарный расчет показывает, что при одинаковых сегментах длина каждого из них может достигать 160 метров (рис. 10.9), а общая длина сети составит 320 метров. Расчет двойного времени прохождения для этого случая будет выглядеть так:

92 + 100 + 2 • 1,0 • 160 = 512.

Получается, что сеть работоспособна, хотя и на пределе. Естественно, в данном случае важна только суммарная длина обоих кабелей. При уменьшении длины какого-нибудь из сегментов можно без потери работоспособности увеличить на точно такую же величину длину другого сегмента.

Если в приведенной на рис. 10.9 конфигурации используется концентратор класса I, а не концентратор класса II, то допустимая суммарная длина сегментов сокращается с 320 м до 272 м (расчет для этого случая очевиден). А с учетом рекомендуемого стандартом запаса лучше еще уменьшить суммарную длину кабеля на 1-4 м, что даст снижение круговой задержки на 1-4 битовых интервала.

В заключение отметим, что модель 2 целесообразно применять в основном при наличии в сети оптоволоконных сегментов. На электрическом кабеле даже при большом желании довольно трудно создать сеть слишком большого размера.

Глава 11. Проектирование сети Ethernet и Fast Ethernet

Содержание одинадцатой главы:

11.1. Выбор размера сети и ее структуры

Любое проектирование, как известно, представляет собой сильно упрощенное моделирование еще не наступившей действительности. Именно поэтому предусмотреть все возможные факторы, учесть все потребности, которые могут возникнуть в будущем, практически невозможно, и все самые подробные руководства по проектированию чего бы то ни было имеют не слишком большую ценность.

Однако самые общие подходы к проектированию локальных компьютерных сетей все-таки могут быть сформулированы, некоторые полезные принципы такого проектирования могут быть предложены и с успехом использованы. Не стоит только воспринимать их как пригодные для любых практических случаев и достаточные для всех возможных ситуаций.

При создании новой сети для какого-нибудь предприятия желательно учитывать следующие факторы.

Требуемый размер сети (в ближайшем будущем и по прогнозу на перспективу).

Требуемая структура, иерархия и основные части сети (по подразделениям предприятия, а также по комнатам, этажам и зданиям предприятия).

Основные направления и интенсивность информационных потоков (в ближайшем будущем и в дальней перспективе).

Технические характеристики оборудования (компьютеров, адаптеров, кабелей, репитеров, концентраторов, коммутаторов) и его стоимость.

Возможности прокладки кабельной системы в помещениях и между ними, а также меры обеспечения целостности кабеля.

Обеспечение обслуживания сети и контроля за ее безотказностью и безопасностью.

Требования к программным средствам по допустимому размеру сети, скорости, гибкости, разграничению прав доступа, стоимости, возможностям контроля за обменом информацией, и т.д.

Необходимость подключения к глобальным сетям или к другим локальным сетям.

Вполне возможно, что после изучения всех перечисленных и не перечисленных факторов выяснится, что вполне можно обойтись вообще без сети, избежав тем самым довольно больших затрат на аппаратуру и программное обеспечение, на установку и эксплуатацию сети, на зарплату обслуживающему персоналу, на поддержку и ремонт и т.д.. Например, если имеется всего несколько пользователей, которые работают на своих компьютерах автономно и только иногда обмениваются файлами, то сеть вполне может заменить обычная дискета (это и дешевле, и гораздо менее хлопотно).

Сеть порождает множество дополнительных проблем по сравнению с автономными компьютерами: от простейших механических (компьютеры, подключенные к сети, сложнее переносить с места на место) до сложных информационных (необходимость контролировать совместно используемые ресурсы, предотвращать заражение сети вирусами). К тому же пользователи сети уже не так независимы, как пользователи автономных компьютеров, им надо придерживаться определенных правил, подчиняться установленным требованиям, которым их необходимо научить.

Наконец, сеть остро ставит вопрос о безопасности информации, защиты от несанкционированного доступа, ведь с любого компьютера сети можно считать данные с общих сетевых дисков. Защитить один компьютер или даже несколько одиночных компьютеров в любом случае гораздо проще, чем целую сеть. Поэтому приступать к установке сети целесообразно только тогда, когда без сети работа становится попросту невозможной, непроизводительной, когда отсутствие межкомпьютерной связи тормозит работу и сдерживает развитие дела.

Первым этапом проектирования сети должен стать анализ существующей ситуации и задач, которые будет решать сеть. Должен быть определен (хотя бы приблизительно) размер сети и ее структура.

Под размером сети в данном случае понимается как количество объединяемых в сеть компьютеров, так и расстояния между ними. Надо четко представлять себе, сколько компьютеров (минимально и максимально) нуждается в подключении к сети. В любом случае надо оставлять возможность для дальнейшего роста количества компьютеров в сети, хотя бы процентов на 20-50. Кстати, совсем не обязательно раз и навсегда включать в сеть все компьютеры предприятия. Может быть, имеет смысл оставить некоторые из них автономными, например, из соображений безопасности информации на их дисках. Количество подключенных к сети компьютеров сильно влияет как на ее производительность, так и на

сложность ее обслуживания. Оно также определяет стоимость требуемых программных средств. Поэтому ошибки в данном случае могут иметь довольно серьезные последствия.

Требуемая длина линий связи сети играет не меньшую, а иногда и большую роль в проектировании сети, чем количество компьютеров. Например, если расстояния очень большие, может понадобиться использование очень дорогого или редкого оборудования. К тому же с увеличением расстояния резко возрастает значимость защиты линий связи от внешних электромагнитных помех. От расстояния зависит и скорость передачи информации по сети (выбор между Ethernet и Fast Ethernet). Целесообразно при выборе расстояний закладывать небольшой запас (хотя бы процентов 10) для учета различных непредвиденных обстоятельств. Кстати, преодолеть ограничения по длине иногда можно путем выбора структуры сети, разбиения ее на отдельные части.

Под структурой сети понимается способ разделения сети на части (сегменты), а также способ соединения этих сегментов между собой. Сеть предприятия может включать в себя рабочие группы компьютеров, сети подразделений, опорные сети, средства связи с другими сетями. Для объединения частей сети могут использоваться репитеры, репитерные концентраторы, коммутаторы, мосты и маршрутизаторы. Причем в ряде случаев стоимость этого объединительного оборудования может даже превысить стоимость компьютеров, сетевых адаптеров и кабеля. Поэтому выбор структуры сети исключительно важен.

В идеале структура сети должна соответствовать структуре здания или комплекса зданий предприятия. Рабочие места группы сотрудников, занимающихся одной задачей (например, бухгалтерия, отдел продаж, инженерная группа) должны располагаться в одной комнате или в рядом расположенных комнатах. Тогда можно все компьютеры этих сотрудников объединить в один сегмент, в одну рабочую группу и установить вблизи их комнат сервер, с которым они будут работать, а также концентратор или коммутатор, связывающий их компьютеры. Точно так же рабочие места сотрудников подразделения, занимающихся комплексом близких задач, лучше расположить на одном этаже здания, что существенно упростит их объединение в единый сегмент и дальнейшее администрирование этого сегмента. На этом же этаже удобно расположить коммутаторы, маршрутизаторы и серверы, с которыми работает данное подразделение.

Как и в других случаях, при выборе структуры целесообразно оставлять возможности для дальнейшего развития сети. Например, лучше приобретать коммутаторы или маршрутизаторы с количеством портов, несколько большим необходимого в настоящий момент (хотя бы на 10-20 процентов). Это позволит при необходимости легко включить в сеть новый сегмент или несколько сегментов. Ведь любое предприятие всегда стремится к росту), и этот рост не должен приводить к необходимости проектировать сеть предприятия заново.

Рассмотрим простейший пример для небольшого предприятия.

Пусть предприятие занимает три этажа, на каждом из которых по пять комнат, и включает в себя три подразделения, в каждом из которых по три группы. В этом случае можно построить сеть таким образом (рис. 11.1):

Рабочие группы занимают по 1~3 комнаты, их компьютеры объединены между собой репитерными концентраторами. Концентратор может использоваться один на комнату, один на группу или один на весь этаж. Под концентратор лучше выделить одну из комнат (небольшую).

Подразделения занимают отдельный этаж. Все три сети рабочих групп каждого подразделения объединяются коммутатором, а для связи с сетями других подразделений используется маршрутизатор. Коммутатор вместе с одним из концентраторов лучше расположить в отдельной комнате.

Общая сеть предприятия, включающая три сегмента сетей подразделений, объединенных маршрутизатором. Этот же маршрутизатор может использоваться для подключения к глобальной сети.

Серверы рабочих групп располагаются в комнатах рабочих групп, серверы подразделений — на этажах подразделений.

В рассмотренной ситуации области коллизий (зоны конфликта) сети будут включать в себя сегменты, расположенные в комнатах каждой рабочей группы, плюс сегмент, связывающий концентратор рабочей группы с коммутатором подразделения. Всего таких областей коллизий будет девять. Именно для них необходимо проводить расчеты работоспособности сети в соответствии с предыдущей главой. Широковещательные области будут включать в себя все сегменты сети каждого подразделения плюс сегмент, связывающий коммутатор подразделения с маршрутизатором предприятия. Таких широковещательных областей будет всего три.

Сели предполагаемая интенсивность обмена по проектируемой сети не лишком велика, если компьютеров не слишком много, если размеры зда-[ия позволяют, то, вполне возможно, удастся обойтись без маршрутиза-'оров — довольно сложных и дорогих устройств. Тогда сети подразделе-:ий будут объединяться концентраторами, а между собой будут оединяться коммутаторами (рис. 11.2). Области коллизий будут в дан-:ом случае включать в себя все сегменты сети каждого из подразделений :люс сегмент, соединяющий концентратор подразделения и коммутатор редприятия. Таких областей коллизий будет всего три. Для них надо про-одить расчет работоспособности сети, как описано в предыдущей главе. Единственная широковещательная область будет в данном случае вклю-ать в себя всю сеть предприятия.

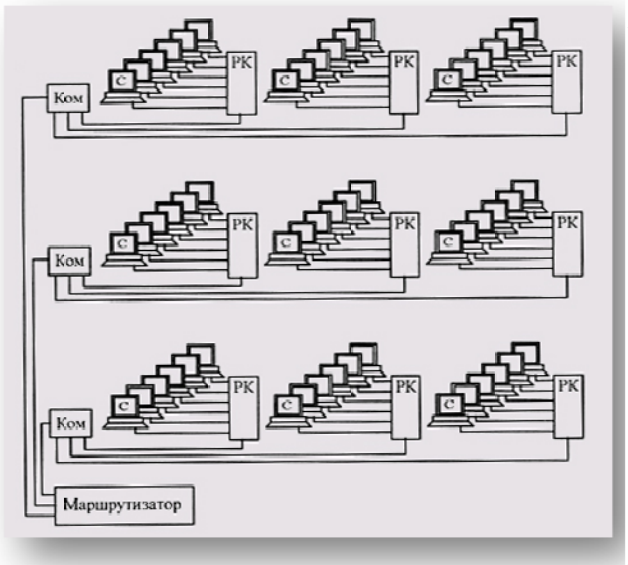


Рис. 11.1
Структура сети предприятия (С — серверы рабочих групп, РК — репитер-ные концентраторы. Ком — коммутаторы)

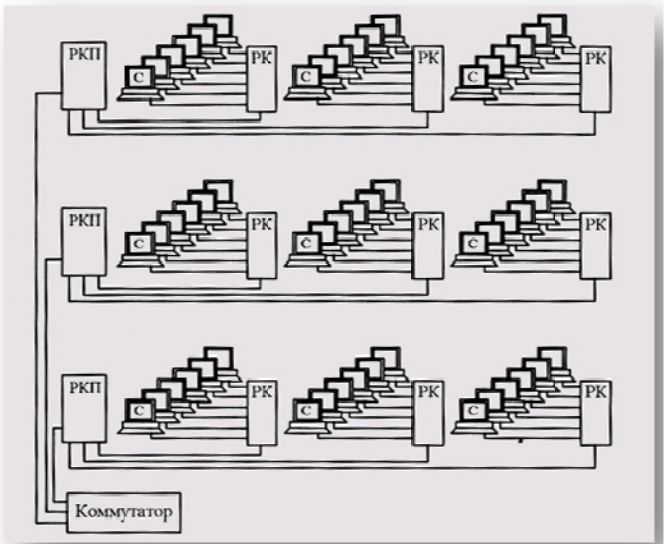


Рис. 11.2
Структура сети предприятия (С — серверы рабочих групп, РК — репитер-!ые концентраторы, РКП — концентраторы подразделений)

В ситуации, когда компьютеров на предприятии немного (до 50), вполне озможно, что имеет смысл отказаться не только от маршрутизаторов, но от коммутаторов, оставив только репитерные концентраторы. Более того, ри такой малой сети и низкой интенсивности обмена вполне может оказаться подходящей сеть Ethernet на тонком коаксиальном кабеле (сегменты 10BASE2) вообще без концентраторов или с 1-2 простейшими репитерами. Правда, в последнем случае, возможно, придется все компьютеры каждого сегмента разместить на одном этаже из-за ограничений на длину кабеля сегмента 10BASE2.

Конечно, такая идиллическая картина наблюдается далеко не всегда. В реальности все обычно бывает гораздо сложнее. Например, структура подразделений может вообще не соответствовать структуре комнат и этажей. Предприятие может занимать два далеко разнесенных помещения в одном здании или даже три—четыре далеко разнесенных здания. Тогда может понадобиться применение оптоволоконных сегментов (возможно, и полнодуплексных, которые обеспечивают максимально возможную длину кабеля). А структура сети при этом может быть чрезвычайно сложной, с множеством областей коллизий и широковещательных областей.

11.2. Выбор оборудования

При выборе сетевого оборудования надо учитывать множество факторов, в том числе:

- уровень стандартизации оборудования и его совместимость с наиболее распространенными программными средствами;
- скорость передачи информации и возможность ее дальнейшего увеличения;
- возможные топологии сети и их комбинации (шина, пассивная звезда, пассивное дерево);
- метод управления обменом в сети (CSMA/CD, полный дуплекс или маркерный метод);
- разрешенные типы кабеля сети, его максимальную длину, защищенность от помех;
- стоимость и технические характеристики конкретных аппаратных средств (сетевых адаптеров, трансиверов, репитеров, концентраторов, коммутаторов).

Всем этим часто пренебрегают, а зря: заменить программное обеспечение сравнительно просто, а вот замена аппаратуры, особенно прокладка кабеля, обходится порой очень дорого, а иногда и просто невозможна. Можно посоветовать в первую очередь проанализировать применимость для рассматриваемого случая сети Ethernet, как наиболее популярной, недорогой и допускающей развитие (Fast Ethernet и Gigabit Ethernet).

При выборе кабеля надо учитывать в первую очередь требуемую длину, а также защищенность от внешних помех и уровень собственных излучений. При большой длине сети и необходимости обеспечить секретность передаваемых данных или высоком уровне помех в помещении незаменим оптоволоконный кабель. Отметим, что применение оптоволоконных кабелей вместо электрических кабелей даже при

достаточно комфортных условиях позволяет существенно (на 10-50 процентов) поднять производительность сети за счет снижения доли искаженных информационных пакетов.

Большой уровень помех может быть вызван наличием в помещении предприятия мощного электрического оборудования (например, металлообрабатывающих станков, физических установок). Он может быть также связан с близким расположением (до 100-200 метров) высоковольтных линий электропередачи, и мощных радиопередатчиков (радиостанций, ретрансляционных антенн сотовой телефонии). Иногда высокий уровень помех вызван всего лишь неправильным размещением кабеля сети. Например, при прокладке кабеля вдоль силовых проводов 220 вольт или вдоль рядов светильников с лампами дневного света количество ошибок передачи резко возрастает (кстати, последнее решение кажется многим очень удобным, так как кабель никому не мешает).

Для прокладки кабелей сети лучше всего использовать специальные подвесные кабельные короба, настенные кабелепроводы или фальшполы. В этом случае кабели надежно защищены от механических воздействий. Замое дорогое решение — это фальшпол, представляющий собой металлические панели, установленные на подставках, и покрывающие весь пол юмещения. Зато фальшпол позволяет легко и безопасно проложить ог-эомное количество проводов, что особенно ценно в научных лаборатори-IX, где помимо кабелей локальной сети существует множество других проводов.

Для прокладки кабеля между комнатами или между этажами обычно пробиваются отверстия в стенах или перекрытиях. По сравнению с прокладкой кабеля через двери комнат и стены коридоров это позволяет существенно сократить общую длину кабелей. Однако надо учитывать, что акое решение усложняет любые дальнейшие изменения в кабельной истеме (замену кабелей, прокладку дополнительных кабелей, измене-ие расположения компьютеров сети и т.д.).

Кабели ни в коем случае не должны самостоятельно удерживать свой вес, ак как со временем это может вызвать их обрыв. Их следует подвеши-ать на стальных тросах, причем для эксплуатации на открытом воздухе еобходимы специально предназначенные для этого кабели с оболочкой, устойчивой к атмосферным воздействиям. По возможности надо использовать для соединения далеко разнесенных зданий подземные коллекторы. Но при этом необходимо предпринимать меры по защите кабелей от воздействия влаги.

Следует также избегать чрезмерно малых радиусов изгиба кабелей (особенно это важно в случае коаксиальных и оптоволоконных кабелей), чтобы не вызвать разрушения изоляции или обрыва центральной жилы. По этой же причине крепежные элементы не должны чересчур пережимать кабель. Известны случаи, когда подобные нарушения вызывали полное прекращение связи через недели или даже месяцы после начала эксплуатации сети.

Для объединения концов всех кабелей часто используются специальные распределительные шкафы, доступ к которым должен быть ограничен. Конечно, их применение оправдано только в том случае, если кабелей очень много (несколько десятков). Располагать распределительные шкафы целесообразно рядом с концентраторами, коммутаторами или маршрутизаторами.

Еще одна важная задача — это выбор компьютеров. Если для рабочих станций или невыделенных серверов обычно используют те компьютеры, которые уже имеются на предприятии, то выделенный сервер лучше приобретать специально для сети. Лучше, если это будет быстродействующий специализированный компьютер-сервер, спроектированный с учетом специфических нужд сети (такие серверы выпускаются всеми крупнейшими производителями компьютеров).

Требования к серверу следующие:

Максимально быстрый процессор (или даже несколько процессоров).

Большой объем оперативной памяти (никак не меньше 64—128 Мб). Это даже важнее быстродействия процессора, так как позволяет эффективно использовать кэширование дисковой информации, храня в памяти копии тех областей диска, с которыми производится наиболее интенсивный обмен.

Быстрые жесткие диски большого объема. Сейчас рекомендуется не менее 200 Мб на каждую рабочую станцию, подключенную к серверу, хотя во многих случаях можно обойтись и меньшим объемом дискового пространства. Дисководы должны быть совместимы с сетевой операционной системой (то есть их драйверы обязательно должны входить в набор драйверов, поставляемый с ОС).

Видеомониторы, клавиатуры и мыши не являются обязательными принадлежностями сервера, так как сервер, как правило, никогда не работает в режиме обычного компьютера.

Если есть возможность выбора компьютеров для рабочих станций, то стоит проанализировать целесообразность применения бездисковых рабочих станций (с загрузкой операционной системы через сеть). Это сразу снизит стоимость сети в целом или позволит при тех же затратах купить более качественные компьютеры: с быстрыми процессорами, с хорошими мониторами, с большой оперативной памятью. Правда, в настоящее время ориентация на бездисковые компьютеры считается не самым лучшим решением. Ведь в этом случае всю информацию компьютер получает через сеть и всю информацию передает в сеть, что может вызвать чрезмерную загрузку сети. Бездисковые рабочие станции допустимы только при очень малых сетях (не более 10-20 компьютеров). В идеале большая часть всех информационных потоков (не менее 80%)

должна оставаться внутри компьютера, а к сетевым ресурсам обращения должны быть только в случае действительной необходимости, то есть упоминавшееся «правило 80/20» работает и в этом случае.

При отказе от использования гибких дисков на каждом компьютере сети можно существенно повысить устойчивость сети как к вирусам, так и к несанкционированному доступу к данным. Дисковод гибкого диска вполне может быть только на одной рабочей станции сегмента или даже всей сети. Причем эта рабочая станция должна контролироваться администратором сети. Она может быть расположена в комнате с концентраторами, коммутаторами, маршрутизаторами.

Для любой сети крайне критична ситуация перебоев в системе электропитания. Несмотря на то, что многие сетевые программные средства применяют специальные меры против этого, как и против других отказов аппаратуры (например, дублирование дисков), проблема очень серьезная. Иногда отключение питания может полностью и надолго вывести сеть из строя.

В идеале защищенными от отключения питания должны быть все серверы сети (желательно, чтобы и рабочие станции тоже). Проще всего этого добиться, если сервер в сети всего один. Источник бесперебойного питания при сбое питания переходит на питание подключенного компьютера от аккумулятора и подает специальный сигнал компьютеру, который за короткое время завершает все текущие операции и сохраняет данные на диске. При выборе источника бесперебойного питания надо прежде всего обращать внимание на максимальную мощность, которую он обеспечивает, и на время поддержания им номинального уровня напряжения (это время бывает от нескольких минут до нескольких часов). Устройство это довольно дорогое (до нескольких тысяч долларов). Поэтому целесообразно один источник бесперебойного питания применять для двух-трех серверов. Маломощные UPS стоят значительно дешевле, мощностью 300-600 Вт — менее 100 долларов, и вполне пригодны для рабочих станций.

Наиболее устойчивы к отказам питания портативные компьютеры (ноутбуки). Встроенный аккумулятор и низкое потребление энергии обеспечивают их нормальную работу без внешнего питания в течение одного-двух часов и даже более. Если еще учесть низкий уровень излучений и высокое качества изображения мониторов этих компьютеров, то стоит всерьез рассмотреть возможность использования ноутбуков в качестве рабочих станций, а возможно, и не слишком мощного, невыделенного сервера, тем более что многие ноутбуки имеют встроенные сетевые адаптеры очень неплохого качества. Особенно удобно применение ноутбуков в одноранговых сетях со множеством серверов. Применение источников бесперебойного питания в подобных случаях становится чересчур дорогим удовольствием.

Кроме перечисленных проблем проектировщику сети приходится решать и проблемы, связанные с выбором сетевых адаптеров, репитеров, концентраторов, коммутаторов и маршрутизаторов, но об этом уже достаточно сказано в предыдущих главах. Стоит только отметить, что производительность сети и ее надежность определяются самым низкокачественным ее компонентом. Поэтому, покупая дорогие концентраторы или коммутаторы, не стоит экономить на сетевых адаптерах. Верно и обратное. В любом случае лучше, когда все компоненты оборудования максимально полно соответствуют друг другу.

11.3. Выбор сетевых программных средств

К сожалению, в процессе проектирования сети совершенно невозможно выделить те проблемы, которые должны быть решены в самом начале, и те, которые можно отложить на самый конец. Выбор программных средств не стоит считать чем-то второстепенным, совершенно не влияющим ни на размер и структуру сети, ни на характеристики требуемого оборудования. Поэтому принимать решение о том, какие программные средства надо использовать или хотя бы к какому классу они должны принадлежать, необходимо в самом начале проектирования.

При выборе сетевого программного обеспечения надо в первую очередь учитывать следующие факторы:

- какую сеть оно поддерживает: одноранговую сеть, сеть на основе сервера или оба этих типа;
- какое максимальное количество пользователей допускается (лучше брать с запасом не менее 20%);
- какое количество серверов можно включить и какие типы серверов возможны;
- какова совместимость с разными операционными системами и разными компьютерами, а также с другими сетевыми средствами;
- каков уровень производительности программных средств в различных режимах работы;
- какова степень надежности работы, каковы разрешенные режимы доступа и степень защиты данных;
- и, возможно, главное — какова стоимость программного обеспечения.

Никогда не стоит гнаться за самым совершенным продуктом просто по-гому, что он популярен, так как с ним, как правило, сложнее обращаться, ца и стоит он гораздо дороже. Вполне вероятно, для ваших

задач подой-цет простая одноранговая сеть, не требующая специального администрирования и покупки дорогого сервера.

Ваконец, еще до установки сети необходимо решить вопрос об управлении сетью. Даже в случае одноранговой сети лучше выделить для этого отдельного специалиста (администратора), который будет иметь всю ин-рормацию о конфигурации сети и распределении ресурсов и следить sa корректным использованием сети всеми пользователями. Если сеть юльшая, то одним сетевым администратором уже не обойтись, нужна делая группа администраторов, возглавляемая системным администратором. После установки и запуска сети решать все эти вопросы, как пра-шло, слишком поздно.

Голько после всего перечисленного можно переходить к установке выб-эанного программного обеспечения, если, конечно, такая установка тре->уется. Заметим, что в большинстве случаев непосредственно установ-сой программных средств занимаются работники специализированных компьютерных фирм. Но принимать решение, о том, что нужно конкрет-юму предприятию, должны все-таки те, кто будет с этой сетью работать ! дальнейшем.

После установки сети необходимо провести ее конфигурирование, то есть задать логическую конфигурацию сети, настроить ее на работу в конкретных условиях. Это входит в обязанности системного администратора сети, который затем осуществляет и контроль за работой сети и управление ее работой:

- создание пользователей и групп пользователей различного назначения;
- определение прав доступа пользователей;
- обучение новых пользователей и оперативная помощь пользователям в случае необходимости;
- контроль за дисковым пространством всех серверов данной сети;
- защита и резервное копирование данных, борьба с компьютерными вирусами;
- модернизация программного обеспечения и сетевой аппаратуры;
- настройка сети для получения максимальной производительности.

Системный администратор, как правило, получает максимальные права по доступу ко всем сетевым ресурсам и ко всем служебным программам сети. Все остальные пользователи сети в идеале не должны замечать сети: просто у них должны появиться новые диски, расположенные на файл-серверах, новые принтеры, сканеры, модемы, новые программы, специально ориентированные на сеть, например, электронная почта.

Создаваемые группы пользователей должны по возможности совпадать с реальными группами сотрудников предприятия, занимающимися одной проблемой или близкими проблемами. Каждой группе системный администратор может установить свои права доступа к сетевым ресурсам. Гораздо удобнее создать группу с определенными правами, а затем включить в нее нужных пользователей, чем определять права каждому пользователю в отдельности. В этом случае при необходимости изменения прав пользователя достаточно перевести его в другую группу. Желательно, чтобы каждой группой управлял свой сетевой администратор (если, конечно, группы достаточно большие). Для примера, сетевая ОС Windows NT позволяет создавать четыре типа групп:

- локальные группы, то есть те, которые регистрируются на локальном компьютере;
- глобальные группы, то есть те, которые регистрируются на главном контроллере домена (PDC);
- специальные группы (обычно используются для внутрисистемных нужд);
- встроенные группы, которые делятся на три категории: администраторы, операторы и другие пользователи.

Свои права доступа можно установить и каждому пользователю в отдельности. В идеале каждый пользователь должен иметь столько прав доступа, сколько ему действительно нужно, не больше и не меньше. Если прав меньше, чем нужно, это мешает работе пользователя, требует постоянного вмешательства сетевого администратора. Если же прав больше, чем необходимо, то пользователь может вольно или невольно уничтожить ценную информацию, с которой он не работает, или исказить ее.

Каждая сетевая операционная система или оболочка имеет свой набор разрешенных прав доступа к каталогам и файлам. Это характеризует ее гибкость, надежность, возможность развития сети. Например, сетевая ОС Novell NetWare обеспечивает права, перечисленные, в табл. 11.1. Сетевая ОС Windows NT Server обеспечивает права, перечисленные в табл. 11.2. Набор прав доступа, предоставляемых операционной системой Windows 95, меньше, чем для других сетевых средств (табл. 11.3).

Табл. 11.1. Виды доступа к каталогам и файлам в ОС NetWare

Вид доступа	Обозначение	Что разрешено
Access Control	A	Изменение прав доступа к каталогу или файлу

File Scan	F	Просмотр каталога
Create	C	Создание каталогов и файлов в данном каталоге
Erase	E	Удаление каталогов и файлов в данном каталоге
Modify	M	Изменение содержимого файлов (перезапись)
Supervisory	S	Любые операции над файлами каталога (права супервизора)
Write	w	Запись в файл

Время от времени рекомендуется делать копии всех дисков сервера, например, на магнитную ленту или на сменные магнитные или оптические диски. Это позволит в случае аварии восстановить недавнее состояние сети, потеряв не слишком много информации. При этом системный администратор должен сохранить на диске рабочей станции информацию о пользователях и их правах доступа, чтобы при восстановлении сети не пришлось все это задавать заново. Целесообразно иметь две копии дисков серверов, одна из которых обновляется довольно редко (например, раз в месяц), а другая — чаще (например, раз в неделю).

Табл. 11.2. Виды доступа к каталогам и файлам в ОС Windows NT Server

Вид доступа	Что разрешено
Read	Чтение и копирование файлов из каталога
Execute	Запуск на выполнение программ из каталога
Write	Создание новых файлов в каталоге
Delete	Удаление файлов в каталоге
No Access	Запрещение любого доступа

Табл. 11.3. Виды доступа к каталогам и файлам в ОС Windows 95

Вид доступа	Что разрешено
Только чтение	Чтение и копирование файлов из каталога
Полный	Чтение, запись в каталог и удаление файлов из каталога
По паролю	Определяется паролем (по паролю «для чтения» — доступ только для чтения, по паролю «для полного доступа» — полный доступ)

Для контроля за функционированием сети системным администратором имеются специальные программные средства. Например, ОС Windows NT Server имеет специальную программу-утилиту Performance Monitor, которая позволяет наблюдать в реальном времени за деятельностью процессоров, за работой дисков, за использованием памяти, за использованием сети. Имеются и отдельные программные пакеты, например, Network Monitor или LANalyzer. Анализируя параметры реального обмена в сети, администратор может установить такие режимы, которые обеспечивают наибольшую эффективность обмена. Выявив тенденции развития сети, он может вовремя принять решение о необходимости модернизации программных или аппаратных средств.

Конечно, всегда надо учитывать, что производительность любой сети зависит не только от установленной аппаратуры и программных продуктов, но и от характера решаемых задач. Одна и та же сеть может прекрасно справляться, например, с задачами доступа к базе данных, но очень плохо работать с передачей динамических трехмерных полноцветных изображений. Так что при проектировании сети с самого начала желательно знать, какого характера информационные потоки предполагается обслуживать с ее помощью.

Впрочем, учесть все факторы в любом случае невозможно, можно только приближаться к оптимальному соответствию возможностей и потребностей.

Глава 12. Подключение к глобальным сетям с помощью модемов

Содержание двенадцатой главы:

12.1. Формулы Шеннона для непрерывного и дискретного каналов

Как уже отмечалось, локальные сети в настоящее время практически всегда имеют выход в какую-то глобальную сеть. Как правило, для подключения к глобальной сети используются модемы.

Модем (сокращение от «модулятор-демодулятор») — это устройство, преобразующее цифровые данные от компьютера в аналоговые сигналы перед их передачей по последовательной линии и, после передачи, производящее обратное преобразование. Основная цель преобразования состоит в согласовании полосы частот, занимаемой сигналами, с полосой пропускания линии передачи. Сигналы могут занимать всю полосу пропускания линии передачи либо ее часть (при частотном разделении каналов, например, в случае организации полностью дуплексного обмена). Кроме того, модемы должны обеспечивать необходимую амплитуду и мощность сигналов для достижения большого отношения сигнал/шум и, как следствие обоих перечисленных факторов (полосы частот и отношения сигнал/шум), возможно большей скорости передачи.

Модемы наиболее часто используются для подключения отдельных компьютеров либо локальных сетей к телефонной линии и, через нее, к другим компьютерам и сетям, в том числе и к глобальной сети Internet. Возможно, однако, использование достаточно экзотичных (по крайней мере, в настоящее время) линий передачи (типа силовой линии электропитания или системы кабельного телевидения) и не менее экзотичных модемов для связи компьютеров (и не только компьютеров), подключенных к той же самой линии связи. Все эти вскользь упомянутые темы, а также принципы работы и внутреннее устройство модемов (в упрощенном виде) рассматриваются в данной главе.

Внимание к характеристикам, внутреннему устройству модемов и принципам их работы вызвано отнюдь не абстрактным соображением о пользе знаний вообще и даже не только чисто прагматическим взглядом на проблему выбора конкретного типа модема, исходя из анализа доступных (часто не полных) сведений и цен. Дело в том, что модемы, используемые для передачи уязвимых по отношению к помехам цифровых данных по отнюдь неидеальным также и в других отношениях линиям передачи, являются хорошим примером «торжества человеческой мысли», воплощенном в достаточно компактном и зачастую интеллектуальном техническом устройстве. Весьма наглядно это проявляется на примере все тех же модемов для подключения к телефонным линиям, которые, как известно, имеют весьма ограниченную полосу пропускания (стандартное значение 3100 Гц) и прочие неприятные и не всегда предсказуемые особенности (временные перерывы в связи, искажения вплоть до полной неузнаваемости формы сигналов после передачи и др.). Для модемов, работающих на аналоговых телефонных линиях, в настоящее время достигнут теоретический предел, определяемый теоремами Шеннона. Работа на пределе возможностей приводит, как всегда, к наукоемким и оригинальным в техническом отношении решениям, которые могут быть полезны широкому кругу специалистов, занимающихся собственными разработками.

Формулы Шеннона представляют собой математические записи теорем кодирования Шеннона для дискретных и непрерывных сообщений, передаваемых по каналам с ограниченной пропускной способностью на фоне шумов и помех.

Каналы связи принято делить на дискретные, непрерывные и смешанные в зависимости от типов сигналов на входе и выходе. В общей структурной схеме канала передачи (рис. 12.1) дискретными являются каналы от входа модулятора до выхода демодулятора и от входа кодера до выхода декодера. Непрерывный (аналоговый) канал — это собственно последовательная линия передачи (телефонная линия, скрученная пара проводов, коаксиальный кабель и др.). Дискретные каналы не являются независимыми рт-аналогового канала, который часто образует наиболее «узкое место» при передаче и из-за собственной ограниченной полосы пропускания и внешних шумов и помех определяет общую достижимую скорость передачи (при заданном допустимом уровне ошибок при приеме).

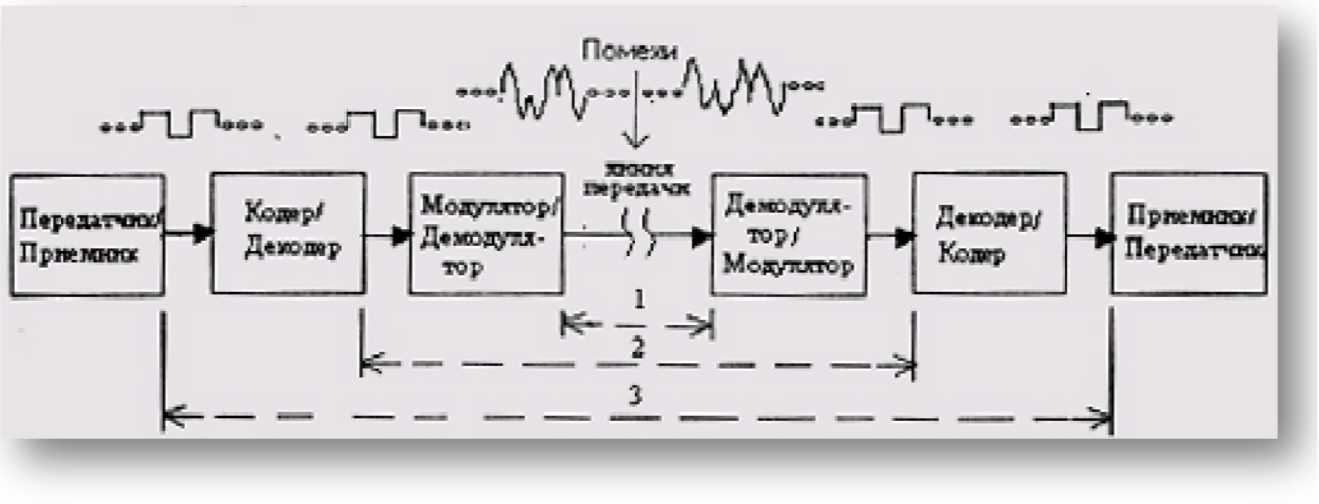


Рис. 12.1
Общая структурная схема канала передачи: 1 — непрерывный (аналоговый) канал; 2,3- дискретные каналы

Прежде чем рассматривать формулы Шеннона, целесообразно обратиться еще раз к рис. 12.1 и пояснить функции отдельных устройств, так как это пригодится при дальнейшем изложении.

Кодер/декодер в конкретной системе может совмещать, на первый взгляд, прямо противоположные функции.

Во-первых, кодер может быть использован для внесения избыточности в передаваемую информацию с целью обнаружения влияния шумов и помех на приемном конце (там этим занимается соответствующий декодер). Избыточность проявляется в добавлении к передаваемой полезной информации так называемых проверочных разрядов, формируемых, как правило, чисто аппаратурными средствами из информационной части сообщения. Известно много различных помехоустойчивых кодов, причем самый простой однобитовый код (бит четности/нечетности) далеко не всегда удовлетворительно работает на практике. Вместо него в локальных сетях используются контрольная сумма или, что еще лучше, циклический код (CRC — Cyclic Redundancy Check), занимающий в формате передаваемого сообщения 2 или 4 байта, независимо от длины в байтах информационной части сообщения.

Во-вторых, при больших объемах передаваемой информации целесообразно ее сжать до передачи, если есть такая возможность. В этом случае говорят уже о статистическом кодировании. Здесь уместна аналогия с обычными программами архивации файлов (типа arj, rar, pkzip и др.), которые широко используются при организации обмена в сети Internet. Волее того, если проблема с большими объемами информации и после такого обратимого сжатия до конца не решается, можно рассмотреть возможность необратимого сжатия информации с частичной ее потерей («огрублением»). Конечно, здесь не может быть и речи об отбрасывании части чисто цифровых данных, но по отношению к изображениям иногда можно пойти на снижение разрешения (числа пикселей) без искажения общего вида «картинки». Здесь можно упомянуть алгоритмы сжатия JPEG для изображений и MPEG для видео- и аудиопотоков, допускающие значительные степени компресии без уменьшения разрешения и с минимальными потерями.

Понятно, что оба типа кодирования (помехоустойчивое избыточное кодирование и статистическое кодирование) служат, в конечном счете, решению одной задачи — повышению качества передачи как в смысле отсутствия или минимального допустимого уровня ошибок в принятом сообщении, так и в смысле максимального использования пропускной способности канала передачи. Поэтому в высокоскоростных модемах нередко реализуются оба типа кодирования. Что касается функций модулятора/демодулятора на рис. 12.1, то они, как уже было сказано, включают согласование полосы частот, занимаемой сигналами, с полосой пропускания линии передачи. Кроме того, выходные каскады передатчиков (после модуляторов) реализуют усиление сигналов по мощности и амплитуде, что является наиболее очевидным средством увеличения отношения сигнал/шум. Действительно, ничто (кроме, пожалуй, техники безопасности...) не заставляет разработчиков придерживаться в аналоговом канале столь жестких ограничений сигналов по амплитуде, как в дискретных (цифровых) каналах (от 0 до + 5В при использовании аппаратуры в стандарте ТТЛ). Например, для распространенного стандарта последовательного порта компьютера RS-232C предусмотрена «вилка» амплитуд от -(3...12)В до +(3...12)В. Конечно, в обоих случаях речь идет об амплитудах вблизи передатчика, в то время как вблизи приемника амплитуда сигналов может быть существенно ослаблена.

Формула Шеннона для непрерывного (аналогового) канала связи достаточна проста:

$$V_{макс} = \Delta f \cdot \log_2(1 + S/N), (1)$$

где VMaKc — максимальная скорость передачи (бит/сек), Af — полоса пропускания линии передачи и, одновременно, полоса частот, занимаемая сигналами (если не используется частотное разделение

каналов), S/N — отношение сигнал/шум по мощности. График этой зависимости приведен на рис. 12.2 (формуле Шеннона соответствует кривая под названием «теоретический предел»).

Под шумом понимается любой нежелательный сигнал, в том числе внешние помехи или сигнал, вернувшийся к передающему устройству — может быть, и модему — в результате отражения от противоположного конца линии. Сами по себе сосредоточенные помехи не столь существенно ограничивают пропускную способность аналогового канала, как непредсказуемый в каждый момент времени белый гауссовский шум. «Умные» высокоскоростные модемы умеют, как будет отмечено в дальнейшем, определять уровень и задержку «своих» отраженных сигналов и компенсировать их влияние.

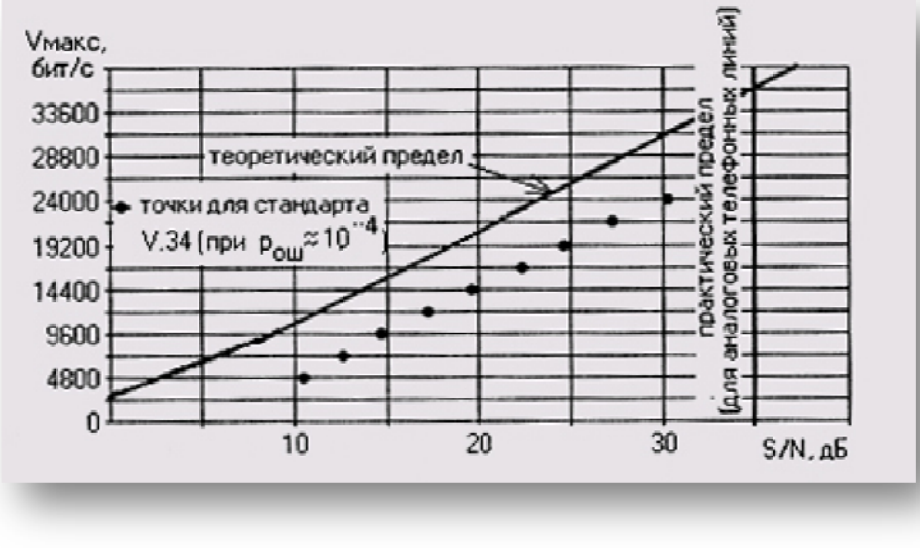


Рис. 12.2
Зависимость максимальной скорости передачи VU3KCдля аналоговой линии от отношения сигнал-шум по мощности S/N

Формула Шеннона для многопозиционного дискретного канала, построенного на базе предыдущего непрерывного канала, в отсутствие ошибок при приеме, имеет следующий вид:

$$V_{макс} = 2 \cdot \Delta f \cdot \log_2 n \quad (2)$$

Здесь п — общее число вариантов дискретного (цифрового) сигнала (алфавит). Если за время одной посылки (длительность элементарного аналогового сигнала типа отрезка синусоиды) передается информация о k двоичных разрядах, то n = 2k. Практически расширение алфавита для дискретных сигналов приводит к появлению все менее различимых элементарных посылок, так что величина п ограничивается сверху все тем же отношением сигнал/шум S/N в аналоговом канале.

При учете ошибок при приеме формула Шеннона для многопозиционного дискретного канала, построенного на базе непрерывного канала, имеет следующий вид:

Здесь рош — отношение числа бит, принятых с ошибками, к общему числу переданных бит за время наблюдения, теоретически стремящееся к бесконечности, а практически достаточное для набора статистики.

Согласно стандарта МККТТ (CCITT, новое название той же организации -ITU-T), для телефонных сообщений должно выполняться условие рош. < 3 • 10~5, а для цифровых данных рош. < 10~6 (в отдельных случаях для критичных данных этот порог уменьшают до 10~9). При выполнении требований стандартов влиянием ошибок при приеме на максимально-допустимую скорость передачи можно полностью пренебречь и от соотношения (3) перейти к более простому соотношению (2). В частном случае бинарного канала (k = 1, n = 2) при Рош= 1/2 из соотношения (3) следует, что V — 0, а при р —> 0 и при р —> 1 V —> 2 • Af. Физический смысл такой зависимости состоит в том, что при рош— 1/2 принятый сигнал не содержит полезной информации (каждый из принятых битов может оказаться ошибочным). При рош (гипотетический случай, имеющий чисто теоретический интерес) каждый бит с большой вероятностью инвертируется, и доля полезной информации снова возрастает.

$$V_{макс} = 2 \cdot \Delta f \cdot [\log_2 n + p_{ош} \cdot \log_2 (p_{ош} / (n-1)) + \; + (1 - p_{ош}) \cdot \log_2 (1 - p_{ош})]$$

Формулы Шеннона показывают, что наиболее эффективный способ увеличения максимальной скорости передачи Умакс состоит в увеличении полосы пропускания линии передачи Af (VMaKc ~ Af). Логарифмическая зависимость VMaKc от отношения сигнал/шум S/N делает этот путь повышения Умакс

гораздо менее перспективным и более трудоемким. Однако на практике редко возможен свободный выбор линии передачи, который с точки зрения реализации максимальной скорости передачи однозначно сводится к использованию оптоволоконной линии связи (ВОЛС). Суровая действительность часто состоит в том, что имеется телефонная линия, по которой и нужно организовать передачу с использованием модемов.

Как уже говорилось, телефонная линия (точнее, тракт передачи, функционирующий на этой линии, с учетом фильтров) имеет фиксированную полосу пропускания Af = 3400 — 300 = 3100 Гц, поэтому приходится бороться именно за повышение отношения сигнал/шум. Да и то хороший результат сам по себе не гарантирован, так как речь идет о реализации возможностей, близких к теоретическому пределу. Практический предел отношения сигнал/ шум в аналоговой телефонной линии составляет примерно 35 дБ (более 3000 раз по мощности или более 56 раз по амплитуде), что соответствует максимальной скорости VMBKC« 34822 бит/сек (стандартное значение, реализуемое на практике, 33600 бит/сек). Популярные в настоящее время 56К—модемы реализуют заявленную скорость только в одну сторону — от провайдера (из сети) до пользователя и только при условии работы провайдера непосредственно на цифровой, несколько более широкополосной, линии передачи (чудес не бывает!).

12.2. Типы линий передачи, использующих модемы

Прокладывание по всем правилам структурированных кабельных систем (СКС) для вновь создаваемых или реорганизуемых компьютерных сетей-- безусловно, полезное, но, одновременно, и дорогостоящее мероприятие, требующее больших первоначальных затрат на проведение капитальных работ. По этой причине производители аппаратных сетевых средств осваивают уже существующие или создаваемые линии передачи, которые не предназначены изначально для соединения компьютеров в сети. Для работы на таких линиях обычно требуются специфические модемы. В сравнении с обычными телефонными модемами эти модемы, как правило, более дорогие не в последнюю очередь из-за ограниченного объема их выпуска. В то же время они по-прежнему служат для переноса спектра передаваемых сигналов в полосу рабочих частот линии передачи, выделенную для организации обмена по сети. Ниже представлен краткий обзор линий передачи, в которых используется модемная связь, и приводятся достигнутые в настоящее время технические характеристики соответствующих модемов (в первую очередь — скорость передачи).

Однопроводная линия — самая простая из возможных линий последовательной передачи данных (см. рис. 12.3). Из-за большого территориального удаления передатчика от приемника в сети (до нескольких сотен метров или даже свыше километра) возникает заметная разница потенциалов между точками заземления аппаратуры и возрастает влияние ничем не скомпенсированных помех. Поэтому на практике такие линии передачи в сетях не используются.

Обычная линия силового электропитания на 220 В (электропроводка) в последнее время успешно используется для организации двунаправленной системы домашней автоматики, связывающей различные бытовые приборы (осветительные приборы, стиральную машину, телевизор и др.) и датчики (датчики температуры, потребляемой мощности и др.). Цель состоит как в управлении этими приборами, так и в сигнализации об опасных ситуациях (пожар, утечка газа и т.д.). «Побочное» использование электропроводки для организации домашней локальной сети напрашивается само собой, однако при этом надо иметь в виду далеко не идеальные характеристики такой линии. Измерения на реальных линиях электропроводки в диапазоне частот 100...150 кГц, наиболее перспективном для передачи данных, показали существенный разброс модуля импеданса линии (1,5...80 Ом), затухания (2...40 дБ) и уровня шума (до -15 дБ). Эти характеристики существенно зависят от количества одновременно включенных в сеть бытовых приборов.

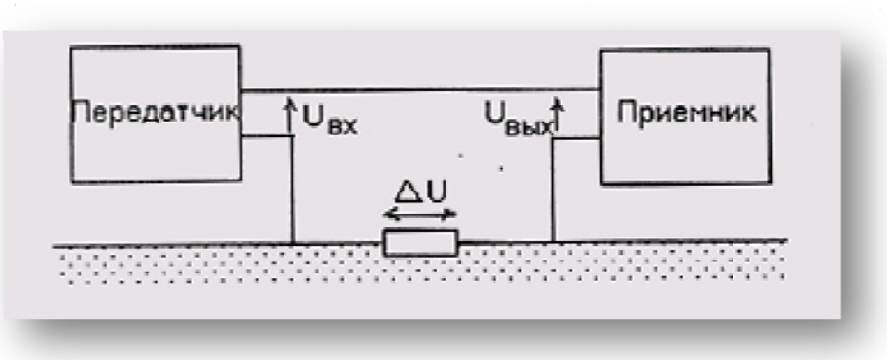


Рис. 12.3
Однопроводная линия передачи
(при симплексном режиме обмена данными)

Для организации домашней локальной сети, использующей линию электропроводки, необходимы специальные модемы (power line modems). Модемы типа CD8000 (фирма Compu Mech) работают на центральной частоте 125 кГц, используют частотную модуляцию и допускают объединение до 15 устройств (с дополнительным модулем адресации — до 255 устройств) при скорости передачи 300бит/с...19,2 Кбит/с. Таким образом, устройства обмениваются данными примерно с такими же скоростями, сак если бы это происходило в сети Internet, хотя и находятся в соседних томещениях. Это не столь важно при обмене чисто цифровыми данными, еднако может создавать проблемы при передаче оцифрованной речи и изображений (особенно динамических).

Двухпроводная телефонная линия в пределах отдельных зданий пред-:тавляет собой простой двухжильный провод, но и это уже прогресс по :равнению с рассмотренной ранее однопроводной линией, так как отсчет гринятого сигнала ведется не от потенциала «земли», а от второго прово-la. в линии. В таких линиях просто организуется симплексный и полугуплексный режим обмена данными, в то время как дуплексный обмен юзможен только ценою снижения скорости передачи (при частотном или феменном разделении «прямого» и «обратного» каналов). Если учесть, (то в лучшем случае скорость передачи по аналоговой телефонной линии !е превышает 33600 Кбит/с (см. предыдущий раздел), то делить в общем-'о и нечего... Правда, иногда требуется передавать в одном из направлений чисто служебную информацию (сообщение о состоянии удаленного юдема, его режимах работы и др.), для которой скорость передачи не-:ритична. Тогда параллельный канал может быть организован практи-[ески без потери скорости по основному каналу.

Четырехпроводная телефонная линия преодолевает недостаток обычной двухпроводной линии, так как позволяет организовать дуплексный обмен без потери скорости в обоих направлениях.

Многопарный телефонный кабель используется в магистральной части телефонной линии (для внешних соединений) и отличается от «внутренних» телефонных линий большей полосой пропускания, которая необходима для уплотнения множества телефонных каналов.

Линии на основе коаксиального кабеля, используемые в системах кабельного телевидения, подобны соединениям во многих локальных сетях. В этих линиях используется еще один тип специализированных модемов, «заслуживших» собственное название: cable modems. Обычный телевизионный сигнал и цифровые данные при передаче по кабелю должны быть разнесены по разным частотным диапазонам Поэтому увеличение скорости не такое заметное, как в локальных сетях, монопольно использующих высокочастотные кабели (100 Мбит/с в сетях типа Fast Ethernet и др.). Компромиссное решение для локальных сетей, основанных на системах кабельного телевидения, состоит в выборе неравных скоростей при передаче запросов от пользователя в сеть (0,512...10 Мбит/с) и при получении информации в обратном направлении (10...40 Мбит/с). Понятно, что вторая скорость важнее.

Беспроводные (радио-) линии привлекательны для тех пользователей, которые не имеют фиксированного рабочего места (учащиеся институтов и университетов, инженеры на производстве и т.д.). Обычно в локальной сети стационарные проводные участки (сегменты) сочетаются с удаленными пользователями или сегментами, обслуживаемыми с помощью радиомодемов (radio modems). Высокая частота несущей (2000...2500 МГц) выбирается из условия малого влияния на передаваемую информацию погодных условий. Однако полоса используемых частот, которая определяет достижимую скорость передачи, ограничена как из-за влияния помех, так и из-за общей занятости радиодиапазонов. В результате максимальная скорость передачи по беспроводным линиям составляет примерно 50 Мбит/с. Следует заметить, что беспроводная связь устойчиво работает только в условиях прямой видимости абонентов (отсутствия препятствий для радиоволн) на расстоянии до 50 км.

Линии передачи с использованием искусственных спутников Земли в качестве ретрансляторов сигналов в глобальных или региональных компьютерных сетях в целом напоминают наземные варианты беспроводных линий. Для передачи в разных направлениях теперь используются две частоты несущей: 6/4 ГГц (другой вариант — 14/12 ГГц). Однако скорость передачи по-гтоежнему обычно не ппевышает 50 Мбит /г Огнгтняя гтоблема в таких линиях связана с заметной временной задержкой сигналов, передаваемых по длинному маршруту. Например, при числе работающих абонентов, равном 100, используемый алгоритм временного разделения каналов (TDMA) приводит к величине временной задержки 1002 (37100 км/300000 км/с) «24 с. Для компенсации этой задержки, создающей дискомфорт при «живом» общении, используются специальные наземные станции-накопители информации SDU (Satellite Delay compensation Unit).

Не все из перечисленных линий передачи нашли в настоящее время широкое применение в качестве основы для построения локальных сетей, хотя роль каких-то из них с течением времени может быстро возрасти. Кроме ограниченной развитости линий (как в случае отечественных телевизионных кабельных сетей), сдерживающими факторами могут быть технические особенности отдельных линий (например, ограничение области действия сети на основе силовой проводки пределами тех помещений, которые питаются от одного силового трансформатора). Как уже отмечалось, стоимость специфических модемов (типа power line modems, cable modems или radio modems) может быть в настоящее время достаточно высока в сравнении со стоимостью обычных телефонных модемов. Наконец, такие глобальные

линии передачи, которые используют искусственные спутники Земли, не всегда доступны рядовому пользователю, хотя неявно их эксплуатируют многие пользователи сети Internet.

Среди наиболее распространенных при модемной связи телефонных линий есть такие их разновидности и такие режимы работы, которые, опять же, не всегда доступны на практике. Ниже в двух колонках представлены: слева — желательные типы и режимы работы телефонных линий, а справа — доступные широкому кругу пользователей (применительно к отечественным условиям).

Четырехпроводные телефонные Двухпроводные телефонные линии линии Выделенные (leased) линии Переключаемые (switched) линии Многоточечные (many-points) Двухточечные (point-to-point) линии.

Линии с тональным набором Линии с импульсным набором номеномера (tone dial) ра (pulse dial) В современных стандартах для модемов (например, в стандарте V.34) предусматривается возможность работы на двухпроводных переключаемых двухточечных линиях, как широко распространенных во всем мире.

При работе на выделенных линиях, аренда которых из-за высоких цен считается оправданной только при достаточно высокой и постоянной во времени загрузке (трафике), а также при использовании широко распространенных (но не у нас) линий с тональным набором номера существенно снижается уровень помех и более полно реализуются собственные скоростные возможности модемов. Многоточечные линии обеспечивают дополнительный сервис — возможность одновременного подключения к линии нескольких пользователей для проведения чего-то вроде «селекторных совещаний», в то время как случающееся иногда многоточечное соединение в обычной линии с прослушиванием абсолютно посторонних абонентов никому из участников не нужно и всех раздражает.

В отношении качества отечественных телефонных линий высказываются обоснованные претензии, связанные с возможными искажениями сигналов из-за множества факторов.

Значительную долю искажений вносят абонентские линии:

- затухание (уменьшение мощности) полезного сигнала;
- изменение амплитудно-частотной характеристики по сравнению со стандартными требованиями (изменение мощности сигнала в зависимости от частоты), причем высокочастотные сигналы затухают более сильно;
- импеданс линии при нормативе 600 Ом ± 20% в реальных линиях может лежать в диапазоне от 400 до 1800 Ом. Это означает, что в российских условиях преимущество имеют модемы с перестраиваемым выходным сопротивлением;
- постоянное напряжение смещения (то самое, благодаря которому работают микрофоны) может иметь значительные отклонения от номинала.

При междугородней связи наибольшее влияние оказывают участки переприема, в которых происходит преобразование сигналов из высокочастотных, передаваемых по магистральным линиям с использованием частотного уплотнения каналов, в сигналы звукового диапазона 300..3400 Гц и наоборот. Общее число таких участков может доходить до 8....11. Вносимые искажения во многом зависят от качества настройки полосовых фильтров на телефонных станциях. Основные искажения при этом следующие:

- фазочастотные искажения (отклонение группового времени прохождения относительно его значения на частоте 1900Гц);
- дополнительные амплитудно-частотные искажения (затухание на краях полосы пропускания);
- смещение несущей частоты (спектр сигнала равномерно смещается на несколько герц);
- джиттер фазы (дрожание фазы по периодическому или случайному закону);
- скачки фазы (случайный поток скачкообразных изменений начальной фазы сигнала).

Существует еще целый ряд искажений, которые могут возникнуть на всем пути сигнала: шумы, импульсные помехи, замирание сигнала — временное уменьшение его мощности до уровня ниже распознавания модемом, колебания амплитуды и др.

«Ответ» модема на все эти искажения, независимо от их природы и места возникновения, один и тот же — снижение реальной скорости передачи, вплоть до временного прекращения связи в процессе автоматической адаптации модема к характеристикам линии (см. следующие пункты данного раздела). Так, если рассматривать влияние на скорость передачи только отношения сигнал-шум по мощности S/N, то, как следует из графика на рис. 12.2, даже для достижения сравнительно «скромной» скорости на уровне 10 Кбит/с в соответствии со стандартом V.34 требуемое отношение сигнал-шум должно быть больше 15 дБ. Измерения на реальных отечественных телефонных линиях, особенно при междугородней связи, показывают возможность снижения отношения сигнал/шум и до меньших величин.

12.3. Структура модема

Одна из возможных структурных схем модема показана на рис. 12.4.

Она содержит типовые функциональные узлы обработки и преобразования сигналов, из числа которых намеренно исключены некоторые второстепенные узлы, предназначенные для организации синхронизации и обработки служебных сигналов. Далее узлы, осуществляющие прямое и обратное преобразования в передающей и приемной части модема, рассматриваются попарно.

Кодер/декодер предназначены для защиты от ошибок и «сжатия» данных. Защита от ошибок предполагает включение в пакеты передаваемых данных избыточного циклического кода (CRC), как и в локальных компьютерных сетях. При этом в качестве стандартных протоколов, более подробно описывающих форматы данных (в том числе число бит в коде CRC — 16 или 32), используются протоколы серии MNP (Microcom Networking Protocol от фирмы Microcom) или V.42 (международный стандарт ITU-T).

Протокол V.42bis представляет собой протокол сжатия данных. Если нельзя увеличить пропускную способность линии передачи из-за ограничения, накладываемого теоремой Шеннона, то можно уменьшить избыточность передаваемой текстовой информации, используя свойство повторяемости цепочек символов в словах. Для этого на передающем и приемном конце линии модемы (точнее, их кодеры и декодеры) организуют и поддерживают идентичные динамические словари в виде структур типа дерева с отдельными символами в качестве узлов (см. рис. 12.5). Достаточно передавать не сами слова, а, фактически, специальным образом описанные (в виде чисел) части словарей (пути в дереве), содержащие требуемые последовательности символов. Так, часть словаря на рис. 12.5 позволяет описать строки символов A, B, BA, BAG, BAR, BI, BIN, C, D, DE, DO и DOG относительно соответствующих корневых узлов.

Рис. 12.4. Структурная схема модема

Скремблер/дескремблер производят такое преобразование передаваемого и принятого сигналов, которое исключает влияние длинных цепочек из логический нулей или единиц, а также коротких повторяющихся последовательностей на надежность синхронизации в приемной части модема. Скремблер при необходимости «прореживает» такие последовательности за счет вставляемых принудительно логических нулей или единиц, делая преобразованные данные псевдослучайными, а дескремблер удаляет лишние биты, восстанавливая исходный вид данных.

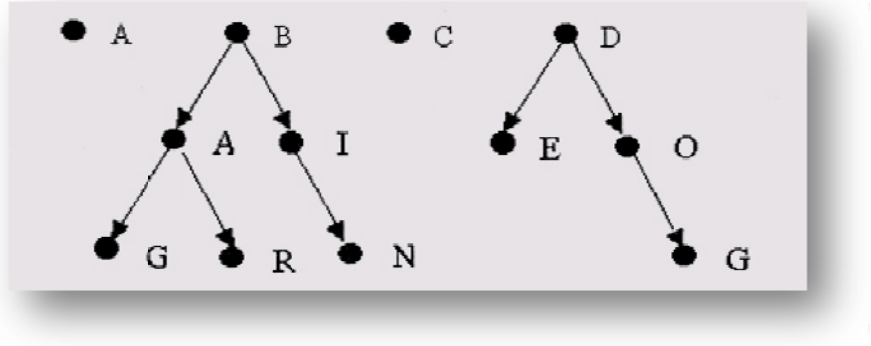


Рис. 12.5
Пример представления части словаря при работе протокола сжатия V.42bis

Описанная проблема (зависимость качества синхронизации от вида передаваемых данных) существенна, конечно, не только при модемной связи, но и при любых видах обменов цифровыми данными по последовательной линии передачи, в которой не предусмотрена посылка отдельного синхросигнала. Такая ситуация характерна для компьютерных сетей, в которых для решения указанной проблемы вместо простых кодов передачи используются самосинхронизирующиеся коды (типа двухуровневых кодов

Манчестер-П или трехуровневых кодов с высокой плотностью единиц — КВП или BNZS в английском варианте названия).

Эквалайзер включается в приемной части модема и служит для компенсации зависимости группового времени запаздывания в линии от частоты. Для улучшения качества передачи речевых сигналов их спектральные составляющие на разных частотах должны приходить к удаленному модему с одинаковой задержкой. Идеальная компенсация показана на рис. 12.6. На практике в высокоскоростных модемах собственное групповое время запаздывания эквалайзера подстраивается автоматически.

В приемной части модемов, работающих в дуплексном режиме на обычной двухпроводной телефонной линии, требуется осуществлять также эхо-компенсацию.

Соответствующий функциональный узел на рис. 12.4 не показан. Проблема состоит в том, что при дуплексном обмене передающий модем может воспринять порожденный им же сигнал, отраженный от другого конца линии, как пришедший от удаленного модема. В стандартах для высокоскоростных модемов (в частности, в стандарте V.34) предусмотрена процедура эхо-компенсации и установлены ограничения на уровень отраженного сигнала (он должен быть меньше полезного сигнала не менее чем на 25...30 дБ) и его максимальную задержку (не более 200...300 мс). Практическая реализация эхо-компенсации в высокоскоростных модемах предусматривает автоматическое определение параметров отраженного сигнала (его амплитуды и задержки) на этапе установления соединения.

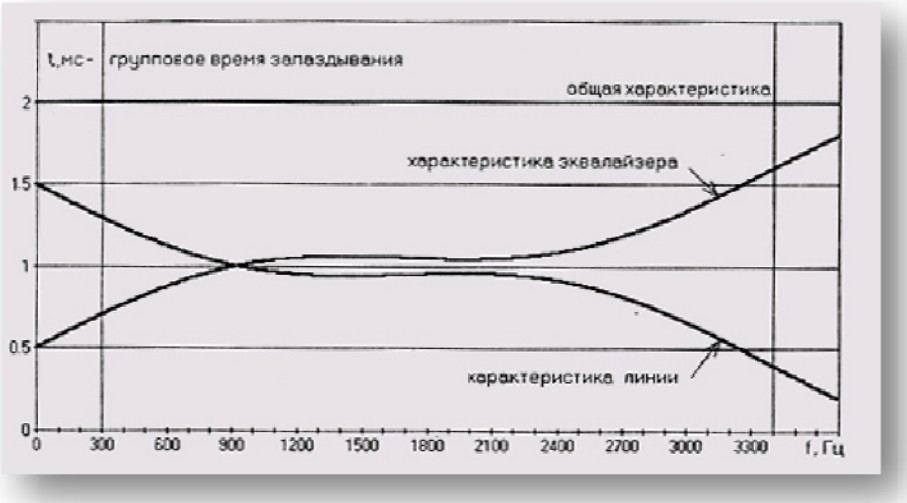


Рис. 12.6
Идеальная компенсация эквалайзером зависимости группового времени запаздывания в линии от частоты

Фильтры и усилители на рис. 12.4 являются традиционными устройствами при обработке сигналов на фоне шумов и помех и не нуждаются в более подробном описании. В то же время модулятор и демодулятор в модемах реализуют специфические и достаточно сложные методы модуляции, которые рассматриваются в разделе 12.4.

В современных модемах большая часть функций выполняется программой, управляющей работой цифрового сигнального процессора (ЦСП). Для исключения эффекта наложения спектров принципиально использование непрерывных аналоговых фильтров. Нужны также аналоговые усилители, АЦП и ЦАП для преобразования аналоговых сигналов в цифровые и обратно.

12.4. Методы модуляции, используемые в высокоскоростных модемах

Известно, что «классические» методы модуляции при прочих равных условиях существенно отличаются между собой по степени устойчивости к помехам. В отношении посылок ограниченных во времени отрезков синусоидальных сигналов, несущих информацию о логических нулях и единицах, возможна следующая простая интерпретация преимущества одних методов модуляции перед другими.

На рис. 12.7 Sj(t) и s2(t) — сигналы, соответствующие логическому нулю и

несет информацию только об одном бите). АМ, ЧМ и ФМ — соответственно амплитудная, частотная и фазовая модуляция. Из графиков видно, что в наибольшей степени отличаются между собой посылки сигналов при фазовой модуляции, в наименьшей — при амплитудной модуляции. Поэтому по степени устойчивости к помехам «классические» методы модуляции должны быть расставлены в том же порядке.

В высокоскоростных модемах для дальнейшего улучшения помехоустойчивости (при неизменном отношении сигнал-шум в линии) используются обычно комбинации из «классических» методов модуляции, в частности, различные варианты амплитудно-фазовой модуляции. Для пояснения преимущества таких

комбинированных методов модуляции над «классическими» методами могут быть использованы так называемые констел-ляционные (constellation — созвездие) или треллис (trellis — решетка) диаграммы. Используется еще и третий вариант названия — квадратурные диаграммы, напрямую связанный со способом изображения на комплексной плоскости гармонических функций при их разложении на синусоидальную («мнимую» — Im) и косинусоидальную («вещественную» — Re) составляющие.

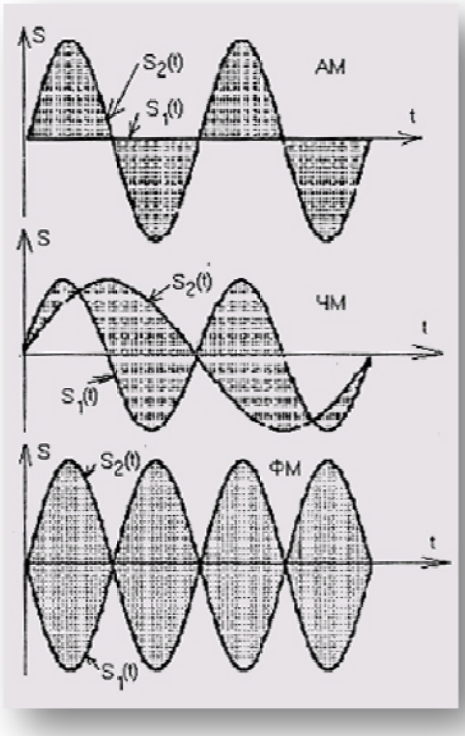


Рис. 12.7
Качественное сравнение «классических» методов модуляции по степени УСТОЙЧИВОСТИ к помрхам

На рис. 12.8 показан фрагмент сигнала для простой бинарной дифференциальной фазовой модуляции (DPSK). При ее использовании передаче логической 1 в исходной цифровой последовательности соответствует сдвиг фазы гармонической посылки на 180°, а логическому 0 — отсутствие такого сдвига. В аналитическом виде этот сигнал описывается соотношением s(t) = cos(wct ± p/2) и на комплексной плоскости представляется в виде двух точек на окружности. В современных высокоскоростных модемах этот вид модуляции не используется, хотя использовался ранее в модемах со скоростью передачи до 4800 бит/с. Причина ограничения скорости передачи связана с неэффективным размещением сигналов в пространстве, при котором минимальное расстояние между ними (а значит, и степень устойчивости к помехам) далеко от теоретического предела.

Для метода DPSK максимальное число бит, информация о которых может быть «закодирована» в одной посылке гармонического сигнала (на одном бодовом интервале), составляет 3, что означает улучшение скорости передачи по сравнению с бинарным кодированием только в 3 раза и общее число гармонических посылок, различающихся по фазе, равное 23 = 8. При попытке дальнейшего «дробления» фаз метод модуляции DPSK становится неконкурентоспособным с точки зрения помехоустойчивости в сравнении с более совершенными комбинированными амплитудно-фазовыми методами модуляции.

Переход от чисто фазовой к амплитудно-фазовой модуляции позволяет увеличить минимальное достижимое расстояние между гармоническими посылками (в смысле расстояния между точками в евклидовом пространстве) при заданном числе этих посылок, как показано на рис. 12.9.

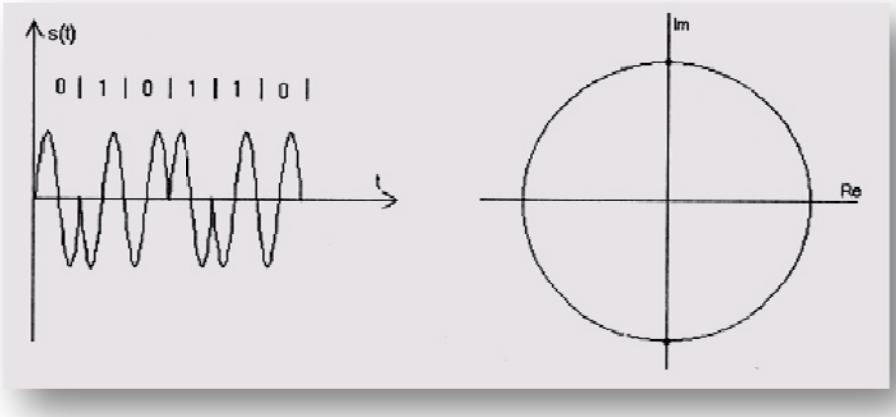


Рис. 12.8
Фрагмент сигнала для простой бинарной дифференциальной фазовой модуляции (2 — DPSK) и его отображение на комплексной плоскости

На этом рисунке сравниваются два метода модуляции (16-DPSK и 16-QAM), причем минимальное расстояние между посылками d, очевидно, больше для второго метода модуляции. Здесь QAM (Quadrature Amplitude Modulation) — многопозиционная амплитудно-фазовая модуляция, при использовании которой достижимое число бит на один бодовый интервал может быть увеличено до 8.

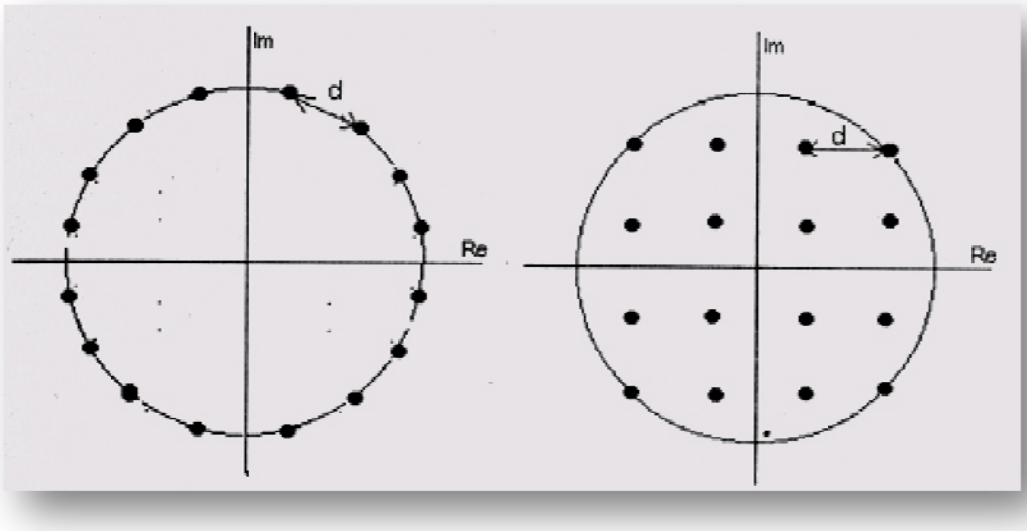


Рис. 12.9
Сравнение двух методов модуляции (16-DPSK и 16-QAM) по величине минимального расстояния между посылками

Существует, однако, еще более совершенный метод модуляции — TCM (Trellis Coded Modulation), модуляция с решетчатым кодированием, или треллис-модуляция. Преимущество метода TCM перед QAM состоит не столько в увеличении числа бит, передаваемых за время посылки (оно может составлять от 1 до 9), сколько в снижении требования к телефонной линии по величине отношения сигнал-шум на 3...6 дБ. Если ограничиться кратким пояснением без привлечения целого ряда дополнительных и необязательных для широкого круга пользователей терминов, то к одним из основных решений, заложенных в метод модуляции TCM, следует отнести введение избыточного бита, полученного с помощью свер-точного кодирования. После этого применяется метод модуляции QAM. Несмотря на то, что введение избыточного бита приводит к увеличению общего числа посылок в два раза, использование при декодировании эффективного алгоритма обработки сигналов на фоне шумов и помех (алгоритма Виттерби) позволяет компенсировать эту избыточность и получить отмеченный выше выигрыш в отношении сигнал-шум. Анализ принятого избыточного бита и учет ранее принятых сигналов позволяют более уверенно выбрать наиболее вероятную точку в пространстве сигналов. Усложнение алгоритмов обработки сигналов и увеличение общего числа возможных посылок ведет, естественно, к увеличению тоебуемой производительности (вычислительной мощности) декодера, однако современный уровень развития цифровых сигнальных процессоров позволяет решить эту задачу.

Модемы со скоростью передачи до 33600 бит/с, предназначенные для работы на аналоговых телефонных линиях и отвечающие рекомендациям стандарта V.34, используют метод модуляции TCM. На

рис. 12.10 в качестве примера представлены проекции сигналов на комплексную плоскость для метода модуляции ТСМ при числе точек, равном 24,128, 256 и 960 (соответствующие скорости передачи в стандарте V.34 — 9600,19200, 24000 и 28800+200 бит/с). В последнем случае за счет временного уплотнения помимо основного канала вводится независимый дополнительный (параллельный) низкоскоростной канал (со скоростью передачи 200 бит/с), который может использоваться для служебных целей. Общий вид проекций сигналов на комплексную плоскость на рис. 12.10 делает понятными ранее упоминаемые варианты названий квадратурных диаграмм: констелляцион-ные или треллис-диаграммы.

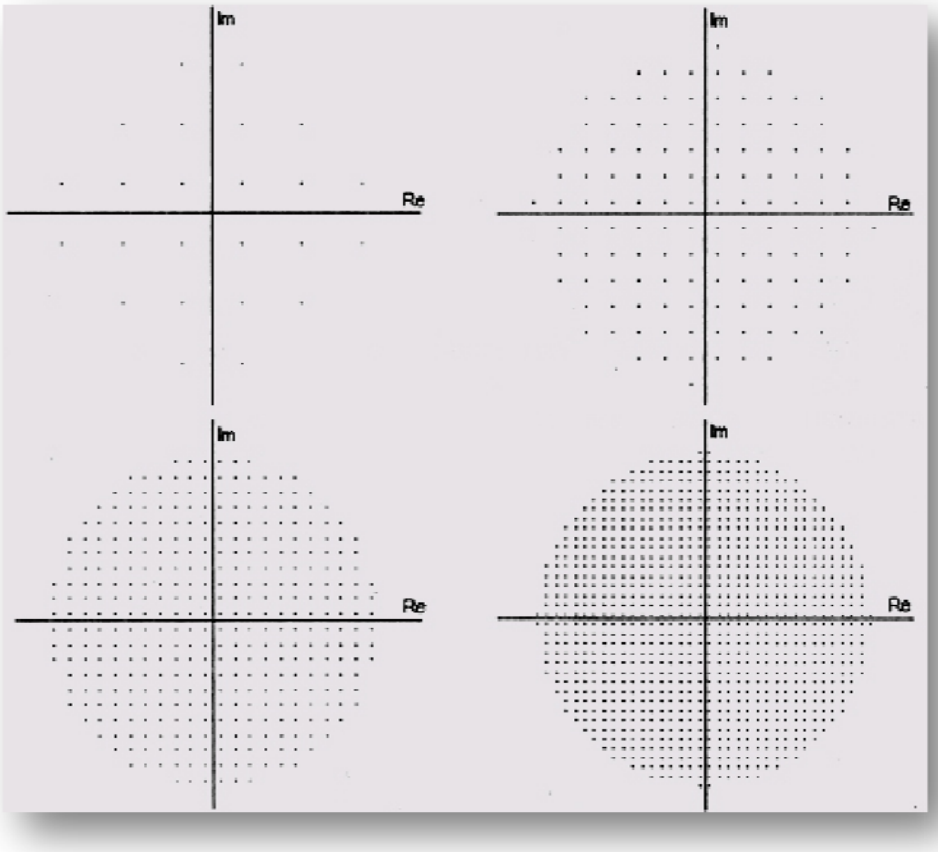


Рис. 12.10. Проекции сигналов на комплексную плоскость для метода модуляции

Стоит сделать замечание относительно двух возможных способов описания скоростей модемов. Скорость в бодах (baudrate) представляет собой физическую частоту смены посылок. Она обычно ограничена полосой пропускания телефонной линии (от 300 до 3400 Гц, т.е. 3100 Гц). Частота несущей выбирается близкой к середине полосы пропускания телефонной линии; для стандарта V.34 предусмотрен ряд возможных частот несущей в диапазоне от 1600 до 2000 Гц («уход» в ту или иную сторону от центра полосы пропускания может несколько улучшить качество связи). Таким образом, бодовый интервал (длительность одной элементарной посылки) может содержать менее одного периода гармонического колебания (в отличие от случая, показанного на рис. 12.8.). Информационная скорость передачи может задаваться либо в бит/с (в англоязычной литературе в bps — bit per second), либо в числе символов в секунду, то есть байт/с (в англоязычной литературе в cps — characters per second). Скорость в бит/с всегда больше или равна скорости в бодах, причем отношение этих скоростей совпадает с числом бит, приходящихся на один бодовый интервал в том или ином методе модуляции. Произведение 3100 (стандартная полоса пропускания телефонной линии в Гц)х9 (максимальное число бит, приходящихся на один бодовый интервал в методе модуляции QAM) все еще меньше 33600 Бит/с. Это означает необходимость использования более широкой полосы пропускания (и большей частоты смены посылок), что и является одной из особенностей стандарта V.34 (см. следующий раздел). Правда, в случае стандарта V.34 вместо скорости в бодах частота смены посылок задается в числе символов/с, что не меняет ее абсолютной величины.

12.5. Особенности стандартов V.34 и V.90

Стандарт V.34 имеет длинное название, перевод которого звучит так: «Модем, обеспечивающий передачу данных со скоростями до 28800 (33600) бит/с для использования на коммутируемой сети общего пользования и на двухточечных двухпроводных выделенных каналах телефонного типа». Таким образом, этот стандарт ориентирован на использование в наиболее распространенных типах телефонных линий. Стандарт V.34 имеет две «версии» или редакции — в первой редакции стандарта от 1994 г.

предусматривалась скорость передачи не выше 28800 бит/с, во второй от 1998 г. этот предел был увеличен до 33600 бит/с. Кроме перечисленных ранее, этот стандарт имеет целый ряд других особенностей, наиболее принципиальные из которых перечислены ниже.

Более полное использование полосы пропускания телефонной линии. Из шести предусмотренных стандартом V.34 символьных скоростей передачи две наибольшие (3200 и 3429 символов/с) требуют ширины полосы пропускания линии, большей стандартного значения 3100 Гц, но достижимой для ряда реальных телефонных линий.

Введение в передаваемый сигнал наряду с линейными нелинейных предискажений для частичной компенсации нелинейных искажений, вносимых аппаратурой с импульсно-кодовой модуляцией (ИКМ), работающей на линии. На комплексной плоскости такие предискажения выглядят в виде неравномерного (отличающегося от строго решетчатого) расположения сигнальных точек.

Развитый сервис, включающий возможность организации асимметричной передачи (разные скорости, несущие частоты, число точек на комплексной плоскости и другие режимы работы для модемов на противоположных концах линии), полудуплексного обмена (эхо-компенсация не используется) и дополнительного канала.

Автоматический адаптивный выбор режимов работы модемов в соответствии с параметрами реальной телефонной линии. Для этого модемы попеременно передают друг другу последовательность из 21 гармонических колебаний с частотами в диапазоне от 150 до 3750 Гц, определяют возможные режимы работы и обмениваются информацией о них. Настройка скорости работы модемов в соответствии с качеством связи (отношением сигнал-шум) означает, что фактически скорость может уменьшаться с шагом 2400 бит/с и в случае отношения сигнал-шум менее 20 дБ (реальная цифра для некоторых отечественных телефонных линий, особенно при междугородней связи) окажется не более 9600 бит/с. Связь ряда достижимых значений скоростей передачи с отношением сигнал/шум для стандарта V.34 показана на рис. 12.2.

Как следует из анализа особенностей стандарта V.34, он практически полностью использует возможности, предоставляемые стандартными аналоговыми телефонными линиями. Дальнейший рост скорости передачи возможен только при использовании линий с большей полосой пропускания, что и предусмотрено в стандарте V.90 для модемов со скоростью передачи до 56 Кбит/с, часто обозначаемых как V.90- или 56К-модемы. Стандарт V.90 на 56К—модемы утвержден ITU-T в сентябре 1998 г. Появление этого станпапта положило конец данного класса K56Flex (в связи с которым упоминаются фирмы 3COM, Rockwell и Lucent Technologies) и X2 (от фирмы US Robotics).

На рис. 12.11 приведена иллюстрация принципа работы обычных (со скоростью передачи до 33600 бит/с на основе стандарта V.34) и 56К (V.90)-модемов в телефонной сети общего пользования.

Хотя большая часть сети цифровая, при работе на обоих концах линии модемы, соответствующие протоколу V.34, используют ее как полностью аналоговую. Это означает необходимость использования аналого-цифровых преобразователей (АЦП) при передаче сигналов в обоих направлениях. В результате дискретизации сигналов по амплитуде АЦП вносят заметный вклад в ухудшение отношения сигнал-шум, и скорость передачи в обоих направлениях одинакова (при самых благоприятных условиях до 33600 бит/с). Однако если на одном из концов линии (у провайдера) использовать специальный цифровой V.OO-модем, подключенный непосредственно к цифровой части телефонной сети, а на другом конце (у клиента) аналоговый У.90-модем, то в направлении от провайдера к пользователю АЦП отсутствует, и скорость может быть увеличена (теоретически) до 56 Кбит/с.

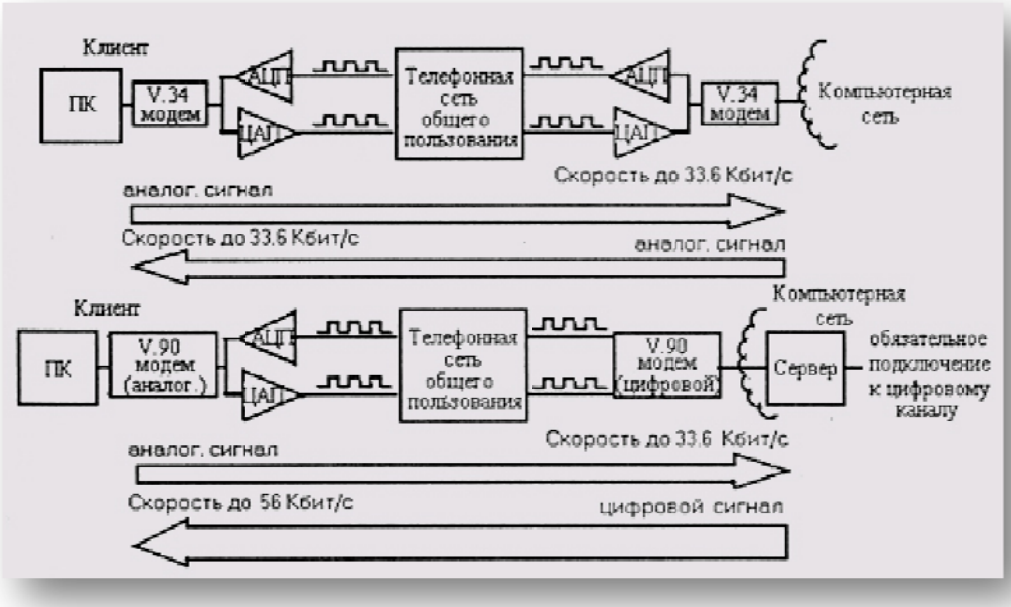


Рис. 12.11. Иллюстрация принципа работы обычных и 56К (\/.90)-модемов

Сама по себе цифровая телефонная сеть имеет скорость передачи 64 Кбит/с, однако наличие дополнительных искажений и шумов от работы ЦАП и АТС, хотя и меньших по уровню, чем шум дискретизации АЦП, ограничивает достижимую скорость передачи. Кроме того, тестирование 56К-модемов показывает возможность достижения скорости в диапазоне 40...50 Кбит/с при связи с местной телефонной станцией и 28...33 Кбит/с при работе на международных линиях.

Таким образом, достижение скорости передачи 33,6 Кбит/с и, тем более, 56 Кбит/с требует выполнения целого ряда условий. В первую очередь сама по себе телефонная линия со всем оборудованием, которое используется для преобразования сигналов и коммутации каналов, должна быть достаточно качественной в смысле малости вносимых искажений сигналов (см. 12.2).

Чтобы работа со скоростью 56 Кбит/с была возможной, необходимо выполнение трех дополнительных условий.

1. Цифровое подключение на одном из концов (со стороны провайдера).

2. Поддержка стандарта V.90 на обоих концах. Стандарт V.90 должен поддерживаться на обоих концах соединения: как аналоговым модемом пользователя, так и сервером удаленного доступа или модемным пулом на стороне хост-компьютера. Переход к стандарту V.90 не означает обязательного приобретения нового модема, т.к. некоторые из них допускают чисто программный «upgrade».

3. Одно аналого-цифровое преобразование. На пути следования сигнала между цифровым модемом V.90 и аналоговым модемом может быть только одно аналого-цифровое преобразование.

Если необходимы подробности, то их можно найти в сети Internet (достаточно в одной из русских поисковых систем указать ключевое слово «V.90»). Однако самый правильный (и неизбежный) шаг состоит в том, чтобы выяснить все у выбранного провайдера и, по возможности, осуществить пробную эксплуатацию 56К-модема (некоторые из провайдеров предоставляют такой вид сервиса).

12.6. Классификация модемов

Выше были упомянуты в достаточно большом количестве разные типы модемов. Однако этот список был бы неполным без упоминания еще ряда названий модемов, используемых на практике. Представлен вариант классификации модемов по следующим трем признакам:

- типы линий передачи, в которых используются модемы;
- виды сервиса и характеристики модемов:
- особенности внутреннего устройства и конструктивного исполнения модемов.

Следует отметить, что модемы относятся к категории массовых и быстро развивающихся телекоммуникационных средств. Их разработкой, изготовлением и продвижением до конечного пользователя занимается множество фирм. С этим связано существование множества неустоявшихся, частично пересекающихся названий модемов. Поэтому краткое название модема может оказаться недостаточным для определения его истинного назначения и особенностей, весьма существенных для

пользователя. Так, существуют два абсолютно несовпадающих типа V-90-модемов — один, аналоговый, для использования у пользователя и другой, чисто цифровой, для поддержки стандарта V.90 со стороны провайдера. Путаница может быть также связана с понятием голосового модема (voice modem) в связи с наличием в некоторых модемах близкой по названию, но совершенно отдельной функции голосовой почты (voice mail).

Приложение 1

Организации, занимающиесястандартизацией сетей

Таблица П.1. Организации, занимающиеся стандартизацией в области компьютерных сетей

Статус орг-ции	Сокр. название	Полное название	
		английское	русское
междун.	CCITT/ МККТТ ITU-T (с 1993 г.)	International Telegraph and Telephone Consultative Committee/ International Telecommunication Union-Telecom	Международный Консультативный Комитет по Телефонии и Телеграфии / Международный телекоммуникационный союз — Телеком
междун.	ISO МОС	International Organization for Standardization	Международная Организация по Стандартизации
междун.	ECMA	European Computer Manufactures Association	Европейская ассоциация изготовителей компьютеров
междун.	ETSI	European Telecommunications Standards Institute	Европейский институт стандартов в области телекоммуникаций
национ. (США)	IEEE	Institute of Electronic and Electrical Engineers	Институт Инженеров по Электротехнике и Радиоэлектронике
национ. (США)	EIA	Electronic Industries Association	Ассоциация электронной промышленности
национ. (США)	ANSI	American National Standards Institute	Американский национальный институт стандартов
национ. (США)	TIA	Telecommunication Industry of America	Телекоммуникационная индустрия Америки

Таблица П.2. Примеры обозначений стандартов С — соответствие может быть неполным)

Организация	Примеры обозначений	Краткое описание содержания стандарта	Соответствующие стандарты
CCITT/ ITU-T	V.34	Модем, обеспечивающий передачу данных со скоростями до 28800 (33600) бит/с для использования на коммутируемой сети общего пользования и на двухточечных двухпроводных выделенных каналах телефонного типа	
	X.25	Интерфейс между оконечным оборудованием данных (ООД) и аппаратурой передачи данных (АПД) для терминалов, работающих в пакетном режиме и подключаемых к сетям передачи данных общего пользования	ECMA-40, ISO 6526
ISO	ISO 646	Набор 7-разрядных символов для обмена данными в системах обработки информации	CCITT V.3; ANSI X3.4
ECMA	ECMA-40	Структура кадра HDLC	CCITT X.25, X.75; ANSI X3.66; ISO 3309
	ECMA-82	Локальные вычислительные сети. Канальный уровень. Передача в основной полосе частот с использованием CSMA/CD	IEEE 802.3
EIA	RS-232C	Интерфейс между оконечным оборудованием данных (ООД) и	CCITT V.24, V.28; ISO 2110

	аппаратурой передачи данных (АПД), использующих последовательный обмен двоичными данными

Для официальных формулировок характерно использование целого ряда дополнительных терминов, которые сами нуждаются в определении. Поэтому имеют право на существование менее строгие формулировки при условии, что они однозначно и правильно понимаются каждым, кто их использует. К примеру, RS-232C часто называют последовательным интерфейсом и это соответствует действительности, а вот название «последовательный порт» вряд ли следует назвать корректным, так как оно слишком далеко отступает от официальной формулировки.

Большинство приведенных в табл. П.2 примеров являются протоколами (кроме ISO 646), правда, относительно простыми.

Иногда используется другая классификация, при которой протоколы делятся на следующие группы:

Novell (от фирмы Novell, известной своими сетевыми ОС NetWare);

SNA (от фирмы IBM);

DECnet (от фирмы DEC);

TCP/IP (большая группа протоколовдля коммуникации в локальной сети или во взаимосвязанном наборе сетей, в том числе широко используемая в сети Internet);

Banyan (от фирмы Banyan Systems);

Apple (от фирмы Apple Computer).

Таким образом, обозначение протоколов — как раз такая область, где действует много стандартов «де факто».

Часть из протоколов упомянута и описана (с разной степенью детализации) в других разделах данной книги.

Приложение 2

Словарь терминов и сокращений

10BASE2 — **стандарт сегмента сети Ethernet на тонком коаксиальном кабеле.**
10BASE5 — **стандарт сегмента сети Ethernet на толстом коаксиальном кабеле.**
10BASE-T — **стандарт сегмента сети Ethernet на витой паре.**
10BASE-FL — **стандарт сегмента сети Ethernet на оптоволоконном кабеле.**
100BASE-T4 — **стандарт сегмента сети Fast Ethernet на счетверенной витой паре.**
100BASE-TX — **стандарт сегмента сети Fast Ethernet на сдвоенной витой паре.**
100BASE-FX — **стандарт сегмента сети Fast Ethernet на оптоволоконном кабеле.**
lOOVG-AnyLAN — **локальная сеть в соответствии со стандартом IEEE 802.12 со скоростью передачи 100 Мбит/с, централизованным управлением обменом, топологией типа звезда, средой передачи витой парой.**
1000BASE-SX — **стандарт сегмента сети Gigabit Ethernet на оптоволоконном кабеле с длиной волны света 0,85 мкм.**
1000BASE-LX — **стандарт сегмента сети Gigabit Ethernet на оптоволоконном кабеле с длиной волны света 1,3 мкм.**
1000BASE-CX — **стандарт сегмента сети Gigabit Ethernet на экранированной витой паре.**
1000BASE-T — **стандарт сегмента сети Gigabit Ethernet на неэкранированной витой паре.**
4B/5B — **самосинхронизирующийся код для передачи данных, применяемый в сети FDDI, в котором 4 бита данных преобразуются в 5 бит, передаваемых в сеть.**
5B6B — **самосинхронизирующийся код передачи данных, применяемый в сети lOOVG-AnyLAN, в котором 5 бит данных преобразуются в 6 бит, передаваемых в сеть.**
8B6T — **код передачи данных, используемый в сегменте сети Fast Ethernet 100BASE-T4, в котором 8 передаваемых бит преобразуются в 6 трехуровневых сигналов.**
8B/10B — **код передачи данных, который будет использоваться в сети Gigabit Ethernet.**
AM (Amplitude Modulation) — **амплитудная модуляция, АМ.**
ANSI (American National Standards Institute) — **Национальный институт стандартов США.**
API (Application Programming Interfaces) — **интерфейсы прикладных программ (относятся к 6 уровню модели OSI).**
Arcnet (ARCnet, Attached Resource Computer Net) — **локальная сеть, разработанная фирмой Datapoint Corporation (скорость передачи — 2,5 Мбит/с, метод доступа — маркерный).**
ARP (Address Resolution Protocol) — **высокоуровневый протокол определения адресов абонентов сети.**
ASCII (American Standard Code for Information Interchange) — **американский стандартный код обмена информацией (8 разрядов).**
ASN.l (Abstract Syntax Notation 1) — **абстрактное описание синтаксиса, формат описания данных в протоколе SNMP.**
ATM (Asynchronous Transfer Mode) — **технология передачи информации, при которой по сети одновременно передаются данные, аудио- и видеосигналы, а также соответствующие технические средства одноименной сети, обеспечивающие обмен информацией на скорости до 6%2 Мбит/с.**
AUI (Access Unit Interface) — **тип разъема и кабеля для подключения сетевого адаптера Ethernet к трансиверу (MAU) толстого коаксиального кабеля.**
Auto-Negotiation — **протокол автодиалога для автоматического согласования скоростей передачи в сети Fast Ethernet.**
Backbone network — **стержневая, базовая, опорная сеть, представляющая собой линию связи или аппаратура с высокой пропускной способностью, соединяющая отдельные части единой локальной сети или несколько локальных сетей.**
Bandwidth — **пропускная способность (вместимость) информационного канала или среды передачи, обычно измеряется в Мбит/с или МГц.**
BFOC/2.5 — **стандарт оптоволоконного байонетного ST-разъема.**
BNC (Bayonet Neill Concelnan) — **разъем байонетного типа, применяющийся, в частности, в сети Ethernet для соединения адаптера с тонким коаксиальным кабелем.**
BPDU (Bridge Protocol Data Units) — **элементы данных протокола мо-:та, применяемого мостами сети для установления структуры сети и уст-эанения петель.**
Broadcast — **широковещательная передача, при которой пакет (сооб-цение) получают все абоненты сети независимо от их сетевого адреса.**

BSC (Binary Synchronous Communications) **-двоичная синхронная пе-эедача данных.**

BT (Bit Time) **— время передачи одного бита в сети.**

CAN (Campus Area Network) **— сеть, объединяющая группу близко рас-юложенных зданий.**

CCITT (Consultative Committee on International Telephony and Telegraphy) **— Международный консультативный комитет по телефонии и телеграфии, МККТТ.**

CD (Collision Detection) **— обнаружение коллизий, столкновений пакетов.**

CDDI (Copper Distributed Data Interface) **— реализация сети FDDI на электрическом (медном) кабеле, то же, что TPFDDI и SDDI.**

Cheapernet **— довольно распространенное название сети или сегмента Ethernet на тонком коаксиальном кабеле (в отличие от сегмента или сети на толстом коаксиальном кабеле).**

Collapse **— крах сети, резкое падение производительности сети из-за перегрузки передаваемым потоком информации.**

Collision domain **— область (зона) конфликта, то есть часть сети (например, Ethernet), на которую распространяется ситуация конфликта (коллизии) передаваемых пакетов.**

CRC (Cyclic Redundancy Check) **— метод контроля правильности передачи с использованием помехоустойчивого циклического кода, а также циклическая контрольная сумма (обычно 16- или 32-разрядная).**

Crosstalk **— взаимное влияние кабелей и проводов друг на друга, перекрестные наводки.**

CSMA/CD (Carrier-Sense Multiple Access/Collision detection) **— децентрализованный метод доступа к сети с контролем несущей (с контролем наличия передачи) и обнаружением конфликтов, применяемый, в частности, в сети Ethernet. Распространенное сокращение — МДКН/ОК.**

Cut-Trough **— тип коммутаторов, в которых не происходит полного приема коммутируемого пакета.**

DAS (Dual-Attachment Stations) **— абоненты (станции) сети FDDI двойного подключения.**

DB9 **— стандартный 9-контактный разъем, используемый в сети Token-Ring.**

DB15 **— стандартный 15-контактный разъем, используемый при подключении трансиверов Ethernet.**

DCE (Data Communications Equipment) **— аппаратура передачи данных, например, модем (АПД).**

DES (Data Encryption Standard) **— стандарт шифрования данных США (с 1976 г.), относящийся к группе методов симметричного шифрования.**

DIX **— объединение фирм DEC (Digital), Intel и Xerox, созданное для поддержки и стандартизации сети Ethernet.**

DMI (Desktop Management Interface) **— интерфейс управления настольными компьютерами.**

DPSK (Differential Phase Shift Keying) **— дифференциальная фазо-разностная модуляция, использовавшаяся в модемах с относительно низкой скоростью передачи (до 4800 бит/с). В настоящее время в высокоскоростных модемах используются более совершенные методы модуляции QAM и TCM.**

DTE (Data Terminal Equipment) **— оконечное оборудование данных (ООД), источник или приемник информации, например, компьютер.**

ECS (Excessive Collision Error) **— множественные коллизии, то есть больше 60 коллизий подряд (ошибка в сети Ethernet).**

ECMA (European Computer Manufacturers Association) **— Европейская Ассоциация производителей компьютеров, международная организация.**

ECTP (Ethernet Configuration Test Protocol) **— протокол тестирования конфигурации сети Ethernet.**

EIA/TIA 568 (Commercial Building Telecommunications Cabling Standard) **— стандарт на кабели для локальных сетей, определяющий их основные характеристики (затухания на различных частотах, отражения, количество витков на метр длины и т.д.).**

Ethernet **— наиболее распространенная в мире локальная сеть, предложенная фирмой Xerox (топология — шина, метод доступа CSMA/CD, скорость передачи — 10 Мбит/с). Удовлетворяет стандарту IEEE 802.3.**

ETR (Early Token Release) **— раннее формирование маркера (в сети Token-Ring).**

Fast Ethernet **— высокоскоростная разновидность сети Ethernet, обеспечивающая скорость передачи 100 Мбит/с. Удовлетворяет доработанному стандарту IEEE 802.3u (стандарт утвержден в 1995 году).**

FCC (Federal Communications Commission) **— Федеральная комиссия по связи**

FCE (False Carrier Event) **—ложная несущая, передача данных без признака начала пакета (ошибка в сети Ethernet).**

FCS (Frame Check Sequence) **— проверочная последовательность кадра, контрольная сумма.**

FDDI (Fiber Distributed Data Interface) **— кольцевая оптоволоконная высокоскоростная локальная сеть (метод доступа — маркерный, скорость передачи — 100 Мбит/с).**

FIRL **— то же, что** FOIRL**.**

FLP (Fast Link Pulse) **— сигналы, передаваемые в промежутках между пакетами в сети Fast Ethernet в режиме автодиалога (автоматического согласования скоростей передачи).**

FM (Frequency Modulation) **— частотная модуляция, ЧМ.**

FOIRL (Fiber Optic Inter-Repeater Link) **— стандарт оптоволоконной связи между двумя репитерами сети Ethernet.**

FOMAU (Fiber Optic MAU) **— оптоволоконные трансиверы сети Ethernet.**

Frame **— кадр, пакет, единица передаваемой по сети информации.**

FTP (File Transfer Protocol) **— протокол передачи файлов, используемый в сети Internet.**

Full duplex **— режим полнодуплексной передачи, при котором передача может идти по линии связи в две стороны одновременно.**

GAN (Global Area Network) **— глобальная сеть.**

Gigabit Ethernet **— разрабатываемая сверхвысокоскоростная версия сети Ethernet, обеспечивающая скорость передачи 1 Гбит/с.**

Half duplex **— режим полудуплексной передачи, при котором передача может идти по линии связи в две стороны, но не одновременно.**

HST (High-Speed Technology) **— технология быстрой передачи данных (один из стандартов модуляции сигналов в модемах).**

HTML (Hypertext Markup Language) **— язык, используемый для создания страниц WWW-серверов, а также сами эти страницы.**

HTTP (Hypertext Transport Protocol) **— протокол передачи по сети страниц WWW-серверов.**

I-connector **— соединитель двух кусков тонкого коаксиального кабеля, оснащенных разъемами BNC на концах.**

IAB (Internet Activities Board) **— Комиссия по деятельности в сети Internet.**

IEC (International Electrotechnical Committee) **— Международный электротехнический комитет (МЭК).**

IEEE (Institute of Electrical and Electronic Engineers) **— Институт инженеров по электронике и радиотехнике (ИИЭР), организация, занимающаяся, в частности, стандартизацией локальных сетей.**

IEEE 802.1 **— стандарт IEEE на объединение сетей.**

IEEE 802.2 **— стандарт IEEE на управление логической связью в сетях.**

IEEE 802.3 **— стандарт IEEE, которому удовлетворяет сеть Ethernet (топология шина, метод доступа** CSMA/CD, среда передачи **— коаксиальный кабель, скорость передачи 10 Мбит/с и т.д.).**

IEEE 802.3u **— стандарт IEEE, которому удовлетворяет сеть Fast Ethernet.**

IEEE 802.3z **— стандарт IEEE, которому удовлетворяет сеть Gigabit Ethernet.**

IEEE 802.4 **— стандарт IEEE, который определяет широкополосную маркерную шину со скоростью передачи 10 Мбит/с, максимальной длиной 1,5 км с числом абонентов до 64.**

IEEE 802.5 **— стандарт IEEE, которому удовлетворяет сеть IBM Token-Ring (топология кольцо, маркерный доступ, среда передачи — витая пара, скорость передачи 4 Мбит/с и т.д.).**

IEEE 802.6 **— стандарт IEEE на городскую сеть (Metropolitan Area Network, MAN).**

IEEE 802.7 **— стандарт IEEE на широковещательную технологию.**

IEEE 802.8 **— стандарт IEEE на оптоволоконную технологию.**

IEEE 802.9 **— стандарт IEEE на интегрированные сети с передачей речи и данных.**

IEEE 802.10 **— стандарт IEEE на безопасность сетей.**

IEEE 802.11 **— стандарт IEEE на беспроводные сети.**

IEEE 802.12 **— стандарт IEEE, которому удовлетворяет сеть 100VG-AnyLAN (скорость передачи 100 Мбит/с, топология звезда, централизованное управление доступом и т.д.).**

IP-address **— цифровой адрес, идентифицирующий пользователей сети [nternet.**

IPG (InterPacket Gap) **— межпакетная щель, межкадровый интервал, минимально допустимый временной промежуток между пакетами Ethernet (96 битовых интервалов).**

IPX (Internet Packet Exchange) **— протокол обмена пакетами в сети без логического соединения.**

IPX/SPX **— набор протоколов низких уровней, используемый в сетях Novell NetWare.**

ISA (Industrial System Architecture) **— наиболее распространенная в настоящее время системная магистраль, персональных компьютеров типа [BM PC. Имеет 16 разрядов данных.**

ISDN (Integrated Services Digital Network) **— цифровая сеть с интеграцией служб передачи телефонных, телевизионных сигналов и данных по одной линии.**

Jabber **— ошибка в сети Ethernet/Fast Ethernet, чрезмерно затянувшаяся передача пакета, то есть передача в течение времени больше 400 мкс (в сети Fast Ethernet) или больше 4000 мкс (в сети Ethernet).**

K56Flex **— стандарт «де-факто» от фирм 3COM, Rockwell и Lucent Technologies для аналоговых модемов со скоростью обмена, достигающей 33,6 Кбит/с (при передаче данных в сеть) и 56 Кбит/с (при приеме данных от цифрового модема провайдера). Широко применялся до появления международного стандарта V.90 в 1998 году.**

LAN (Local Area Network) **— локальная (вычислительная) сеть, ЛВС.**

LAPM (Link Access Procedure for Modems) **— процедура доступа к линии связи для модемов.**

LED (Light Emitted Diode) **— светодиод.**

LLC (Logical Link Control) **— верхний подуровень второго уровня мо-Зели OSI (уровня управления линией передачи), отвечающий за управ-тение логическими связями.**

Login **— процесс подтверждения личности пользователя компьютерной сети, используемый для контроля доступа к сети.**

MAC (Media Access Control) **— нижний подуровень второго уровня модели OSI (уровня управления линией передачи), отвечающий за управление доступом к среде передачи.**

MAC-адрес **— уникальный 48-битный адрес сетевого адаптера, устанавливаемый производителем адаптера. Применяется в сетях Ethernet, Token-Ring, FDDI.**

MAN (Metropolitan Area Network) **— глобальная сеть в масштабах города.**

Manchester-II **— самосинхронизирующийся двухуровневый код передачи данных, применяющийся, в частности, в сети Ethernet.**

MAU (Medium Attachment Unit) **— трансивер сети Ethernet на толстом коаксиальном кабеле, устанавливаемый непосредственно на кабеле. См. также MSAU.**

Mbps (Mb/s, Mbits per second) **— мегабит в секунду (Мбит/с), единица измерения скорости передачи и пропускной способности среды передачи.**

MDI (Medium Dependent Interface) **— интерфейс, зависящий от среды, средства непосредственной связи со средой передачи, например, разъем.**

МШ (Management Information Base) **— база данных управляющей информации, используемая в протоколе SNMP.**

МП (Medium Independent Interface) **— интерфейс, не зависящий от среды передачи, связывающий адаптер или концентратор с трансивером среды.**

MMF (Multimode Fiber-optic cable) **— мультимодовый оптоволоконный кабель.**

MNP (Microcom Networking Protocol) **— стандартный набор протоколов модемной связи, предложенный фирмой Microcom.**

MSAU или MAU (Multistation Access Unit) **— концентраторы сети IBM Token-Ring.**

NDIS (Network Driver Interface Specification) **— спецификация интерфейса сетевого драйвера.**

NE2000 **— популярный тип адаптера сети Ethernet (фирма Novell), ставший одним из фактических стандартов.**

NetBEUI **— расширенный интерфейс** NetBIOS.

NetBIOS (Network Basic Input/Output System) **— сетевое программное обеспечение сеансового уровня модели OSI, разработанное первоначально фирмой IBM и ставшее впоследствии фактическим стандартом.**

NIC (Network Interface Card) **— сетевой адаптер (контроллер), сетевая карта.**

NLP (Normal Link Pulse) **— сигналы, передаваемые в сегментах 10BASE-T между пакетами для контроля целостности линии связи.**

NMS (Network Monitoring Station) **— станция управления сетью, ра-ютающая с протоколом SNMP.**

NOS (Network Operational System**) — сетевая операционная система.**

NVP (Nominal Velocity of Propagation) **— скорость распространения :игнала в кабеле, выражается в долях от скорости света С, например, NVP = 0,7С.**

NRZ (Non-Return to Zero) **— простейший несамосинхронизирующий-:я код передачи данных (без возврата к нулю), применяемый, например, з интерфейсе RS-232C.**

ODI (Open Data link Interface) **— открытый интерфейс канала данных, :пецификация, позволяющая сетевому адаптеру работать с сетями Novell NetWare и совместимыми с ними.**

OSI (Open System Interchange) **— модель взаимодействия открытых систем (ВОС), которая выделяет семь уровней в сетевых функциях: 1 — физический, 2 — канальный, 3 — сетевой, 4 — транспортный, 5 — сеансо-зый, 6 — представительский, 7 — уровень приложений.**

Overload **— перегрузка сети чрезмерно большим потоком передаваемой информации.**

PCI (Peripheral Component Interconnect) **— быстродействующая 32-чли 64-разрядная магистраль, применяющаяся в персональных компь-отерах типа IBM PC.**

PDU (Protocol Data Unit) **— модуль данных протокола, блок данных в дейтаграмме, используемый в протоколе SNMP.**

PDV (Path Delay Value) **— двойное (круговое) время задержки прохождения сигнала по сети. Учитывает суммарную задержку в кабельной :истеме, сетевых адаптерах, репитерах и других сетевых устройствах.**

PGP (Pretty Good Privacy) **— метод шифрования данных, относящий-:я к группе методов несимметричного шифрования. Широко использует-:я в сети Internet для защиты сообщений, передаваемых посредством «лектронной почты.**

PHY **— средства взаимодействия с физической средой передачи в сети входят в первый уровень модели OSI), также приемопередатчик.**

Plenum **— тип кабеля в тефлоновой оболочке, более устойчивый к воз-*ействиям окружающей среды, чем обычный кабель (non-plenum); при 'орении не выделяет токсичных газов.**

Plug and Play (PnP, P&P) **— стандартная технология автоматической гастройки параметров плат, подключаемых к компьютеру, фирм Microsoft, Compaq, Intel и Phoenix Technologies.**

PMD (Physical Medium Dependent) **— нижний подуровень первого (фи-!ического) уровня модели OSI, зависящий от типа среды передачи.**

PMI (Physical Medium Independent) **— верхний подуровень первого физического) уровня модели OSI, независящий от типа среды передачи.**

PPP (Point-to-Point Protocol) **— протокол связи с Internet по телефонному каналу.**

PVC **— поливинилхлоридная оболочка кабеля.**

QAM (Quadrature Amplitude Modulation) **— многопозиционная амплитудно-фазовая модуляция, используемая в высокоскоростных модемах (скорость передачи до 9600 бит/с). Улучшенный вариант — метод TCM.**

RG-11 **— распространенный тип толстого коаксиального кабеля сети Ethernet с волновым сопротивлением 50 Ом.**

RG-58 A/U **— распространенный тип тонкого коаксиального кабеля сети Ethernet с волновым сопротивлением, равным 50 Ом.**

RG-62 A/U **— распространенный тип коаксиального кабеля для сети Arcnet с волновым сопротивлением 93 Ом.**

RJ-11 **— четырехконтактный разъем, используемый для подключения телефонных кабелей.**

RJ-45 **— тип разъема для присоединения кабеля на основе витых пар (8 контактов).**

RMON (Remote Network Monitoring) **— система удаленного мониторинга сети.**

RS-232C **— стандартный интерфейс последовательной передачи данных компьютера.**

RSA (Rivest, Shamir, Adleman) **— метод шифрования данных, относящийся к группе методов несимметричного шифрования.**

Runt frame **— карликовый кадр (пакет), кадр в сети Ethernet, имеющий длину меньше минимальной (512 бит).**

RXC (Received Clock) **— принимаемый синхроимпульс.**

RX, RXD (Received Data) **— принимаемые данные.**

RZ (Return to Zero) **— самосинхронизирующийся трехуровневый код передачи данных.**

SAF **— см.** Store-and-Forward**.**

SAS (Single-Attachment Stations) **— абоненты (станции) сети FDDI одинарного подключения.**

SCS (Structured Cabling System) **— структурированная кабельная система для локальной сети (СКС).**

SDDI (Shielded Distributed Data Interface) **— реализация сети FDDI на экранированной витой паре, то же, что CDDI и TPFDDI.**

SDLC (Synchronous Data Link Control) **— стандарт синхронного управления передачей данных.**

SFD (Start of Frame Delimiter) **— признак начала кадра.**

Simplex **— режим симплексной передачи, при котором передача может идти только в одном направлении: от передатчика к приемнику.**

SLAN (Switched Local Area Network) **— коммутируемая локальная сеть, то есть сеть, содержащая коммутаторы (переключатели).**

Slot time **— максимально допустимое время окна коллизий в сети Ethernet (512 битовых интервалов).**

SMF (Single Mode Fiber-optic cable) **— одномодовый оптоволоконный :абель.**

SMTP (Simple Mail Transfer Protocol) **— протокол передачи сообще-[ий электронной почты, используемый в сети Internet.**

SNA (System Network Architecture) **— архитектура сетевых систем, [редложенная фирмой IBM и ориентированная на объединение компьютеров самых разных типов.**

SNMP (Simple Network Management Protocol) **— протокол обмена для гдаленной управляющей станции в сети Ethernet, служащей для конт-юля за нагрузкой сети и за интенсивностью ошибок в сети, а также для втоматического отключения неисправных сегментов.**

SPD (Simple Propagation Delay) **— простая (не двойная, не круговая) адержка распространения сигнала в сети.**

Store-and-Forward **— тип коммутаторов, в которых производится полый прием (хранение) коммутируемых пакетов.**

STP (Shielded Twisted-Pair cable) **— кабель на основе экранированных итых пар, сами экранированные витые пары.**

SPX (Sequenced Packet Exchange) **— протокол обмена пакетами с ло-ическим соединением.**

T-connector **— Т-образный соединитель, служащий для подключения ;вух кусков тонкого коаксиального**

кабеля к сетевому адаптеру.

TCM (Trellis Coded Modulation) **— модуляция с решетчатым кодиро-анием, многопозиционная амплитудно-фазовая модуляция. Улучшенный ариант метода QAM, использующий его на одном из этапов преобразо-ания сигналов.**

TCP/IP **— набор протоколов нижних уровней для связи в гетерогенной реде, применяемый в сети Internet.**

Terminator **— терминатор, согласующее устройство, выполняющее лектрическое согласование кабеля на обоих его концах. Представляет обой резистор с сопротивлением, равным волновому сопротивлению при-[еняемого кабеля. Присоединяется к кабелю с помощью разъема.**

TIA (Telecommunication Industry Association) **— Ассоциация телеком-;уникационной промышленности.**

Token-Ring **— кольцевая локальная сеть фирмы ЮМ с маркерным ме-одом доступа и скоростью передачи 4 Мбит/с.**

TP (Twisted Pair) **— витая пара.**

TPFDDI (TDDI) **— версия сети FDDI на электрическом кабеле (витой аре) со скоростью передачи данных 100 Мбит/с, то же, что CDDI и SDDI.**

TXC (Transmitted Clock) **— принимаемый синхроимпульс.**

TX, TXD (Transmitted Data) **— передаваемые данные.**

UART (Universal Asynchronous Receiver/Transmitter) **-универсальный асинхронный приемопередатчик (УАПП).**

UTP (Unshielded Twisted-Pair cable) **— кабель на основе неэкранированных витых пар, сами неэкранированные витые пары.**

URL (Uniform Resource Locator) **— адрес ресурсов специального вида, применяемый в сети Internet.**

USART (Universal Synchronous/Asynchronous Receiver/Transmitter) **— универсальный синхронно-асинхронный приемопередатчик (УСАПП).**

V.34 **— стандарт МККТТ (CCITT/ITU-T) для аналоговых модемов, обеспечивающих передачу данных со скоростями до 33,6 Кбит/с для использования на коммутируемой сети общего пользования и на двухточечных двухпроводных выделенных каналах телефонного типа.**

V.90 **— стандарт МККТТ (CCITT/ITU-T) для модемов, обеспечивающих передачу данных со скоростями до 56 Кбит/с. После принятия в 1998 году подвел итог борьбе двух стандартов «де-факто» K56Flex и X2.**

WAN (Wide Area Network) **— глобальная (вычислительная) сеть, ГВС.**

WWW (World Wide Web) **— гипертекстовая мультимедийная служба в сети Internet, содержащая информацию в гипертекстовом виде.**

X2 **— аналог стандарта «де-факто» K56Flex. Принадлежит фирме US Robotics.**

Абонент сети (узел) **— любое устройство, подключенное к сети и общающееся с ней (компьютер, принтер, сканер и т.д.).**

Адаптер сетевой **— электронная плата (карта) для сопряжения компьютера со средой передачи информации в сети.**

Бездисковые компьютеры **— компьютеры без жестких и гибких дисков, начальная загрузка которых производится из сети с помощью загрузочного ПЗУ на плате сетевого адаптера.**

Вероятность ошибки **— допустимое стандартами относительное число ошибочных бит в информации, принятой после передачи по протяженной последовательной линии с помехами. Для цифровых данных может задаваться на уровне 10~6...10~9, что соответствует не более чем одному ошибочному биту из 106... 109 принятых бит.**

Виртуальный канал **— последовательность логических соединений между посылающим и принимающим компьютером, происходящих при передаче информации.**

Витая пара **— среда передачи информации из двух перекрученных между собой электрических проводов, характеризующаяся наибольшей простотой монтажа и низкой стоимостью.**

Время канала (slot time) **— максимально допустимое окно коллизий для сегмента в сетях типа Ethernet и Fast Ethernet, равное 512 • BT, т.е. 51,2 мкс и 5,12 мкс соответственно.**

Время доступа **— временной интервал между возникновением заявки на передачу данного абонента и получением права на передачу.**

Выделенный (dedicated) сервер **— компьютер в сети, работающий исключительно как сервер сети и не способный выполнять другие (не сетевые) задачи.**

Гаммирование **— один из простейших способов шифрования данных, основанный на сложении их цифрового представления с маской конечной или бесконечной длины.**

Группа **— логическое объединение компьютеров сети, решающих общие задачи и имеющих одинаковые права доступа.**

Датаграмма, дейтаграмма **— способ передачи пакетов без подтверждения получения в произвольном порядке; правильный порядок восстанавливается принимающим абонентом.**

Децентрализованное управление обменом **— метод управления обменом в сети, при котором нет**

выделенного центра управления, и все абоненты равноправны (хотя и могут иметь разные приоритеты по захвату сети).

Диаметр сети **— путь максимальной длины в сети Etherne.t, то есть путь между двумя абонентами с максимальной для данной сети задержкой распространения сигнала.**

Домен **— в сетях Microsoft — логическое объединение компьютеров, в отношении которых проводится единая политика безопасности.**

Доменная система имен **— система преобразования имен пользователей сети Internet в IP-адреса, строящаяся по многоуровневому принципу.**

Драйвер адаптера **— программа, осуществляющая взаимодействие аппаратуры драйвера и сетевого программного обеспечения.**

Затухание сигнала **— ослабление передаваемого сигнала при его прохождении по сети, доля мощности сигнала, потерянная при прохождении по кабелю. Измеряется в децибелах (дБ).**

Затянувшаяся передача **— см.** Jabber**.**

Захват сети **— получение абонентом сети права на передачу пакета.**

Звезда (star) **— вид топологии локальной сети, в котором к одному цен- , тральному абоненту (концентратору) подключаются несколько периферийных абонентов; при этом все управление сетью и (или) передачу всей информации в ней осуществляет центральный абонент.**

Зона конфликтов (область коллизий) **— множество абонентов (узлов) сети Ethernet, осуществляющих доступ к сети по методу CSMA/CD. Часть сети, на которую распространяется ситуация конфликта. Может включать в себя всю сеть.**

Источник бесперебойного питания **— устройство, обеспечивающее электроснабжение потребителей (компьютеров, концентраторов, принтеров и т.д.) при сбоях в электросети.**

Кадр **— базовый элемент передаваемых данных в сети. Часто то же самое, что и пакет.**

Клиент **— абонент, не отдающий своего ресурса в сеть, но имеющий доступ к ресурсам сети. Иногда клиенты называются также рабочими станциями в противоположность серверу.**

Коаксиальный кабель **— среда передачи информации, электрический кабель, состоящий из центрального проводника и металлической оплетки, разделенных диэлектриком.**

Кодер/Декодер **— одно из устройств модема, осуществляющее статистическое сжатие/распаковку данных, а также их защиту от помех за счет формирования и анализа помехоустойчивого циклического кода, добавляемого в конец пакета с данными.**

Коллизия **— ситуация, при которой в сеть передаются несколько пакетов одновременно, что вызывает искажение информации. Называется также конфликтом или столкновением.**

Кольцо (ring) **— вид топологии локальной сети, в котором все абоненты последовательно передают информацию друг другу по цепочке, замкнутой в кольцо.**

Концентратор (hub) **— устройство, служащее для объединения нескольких сегментов единой сети и не преобразующее передаваемую информацию.**

Комбинированный маршрутизатор (brouter) **— устройство (компьютер), являющееся комбинацией моста и маршрутизатора.**

Коммутатор, коммутирующий концентратор, переключатель (switching hub, switch) **— концентратор, передающий на другие сегменты только те пакеты, которые адресованы им, с целью снижения нагрузки на сеть.**

Коммутатор Cut-Through **— коммутатор, начинающий ретранслировать пакеты (кадры) до того, как полностью получит их.**

Коммутатор Store-and-Forward **— коммутатор, который получает и хранит полный пакет (кадр) перед тем, как ретранслировать его.**

Конфликт, коллизия (collision) **— ситуация, при которой в сеть передаются несколько пакетов, что вызывает искажение информации.**

Криптография **— преобразование информации с целью исключения доступа к ней со стороны нелегальных пользователей и подмены информации. Включает в себя шифрование и комплекс мер для достижения второй цели (цифровые подписи, имитовставки и хэш-функции).**

Кэширование **— хранение в оперативной памяти копии наиболее часто требуемой информации с целью ускорения доступа к ней.**

Локальная сеть **— компьютеры или другие устройства, соединенные линиями связи для передачи информации между ними, как правило, на сравнительно небольшие расстояния.**

Маркер **— уникальная комбинация битов или пакет специального вида, использующийся для процедуры захвата сети.**

Маркерное кольцо **— детерминированный метод доступа в локальных сетях, альтернативный случайному методу доступа CSMA/CD и обеспечивающий, в отличие от него, отсутствие коллизий и гарантированное сверху время доставки данных в сетях при отсутствии перегрузок. Допускает организацию системы**

приоритетов между абонентами.

Маршрутизатор (router) **— устройство (компьютер), служащее для определения маршрута, по которому наиболее целесообразно пересылать пакет.**

Межкадровый интервал (межпакетная щель, IPG) **— интервал между двумя пакетами (кадрами).**

Метод доступа **— способ определения, какой из абонентов сети может захватить сеть и начать передачу своего пакета.**

Модем (модулятор-демодулятор) **— устройство, преобразующее цифровые данные от компьютера в аналоговые сигналы перед их передачей по последовательной линии и, после передачи, производящее обратное преобразование. Кроме функции согласования полосы частот, занимаемой передаваемыми сигналами, с полосой пропускания реальной линии передачи, выполняют много других функций (сжатие данных, формирование и проверка помехоустойчивого циклического кода, эхо-компенсация и др.).**

Модемы, разновидности по типам линии передачи **— специальные типы модемов для работы в линии электропроводки (power line modems), в системах кабельного телевидения (cable modems) и в беспроводных (радио-) линиях (radio modems).**

Моноканал **— сеть (или среда передачи), в которой используется узкополосная передача.**

Мост (bridge) **— устройство (компьютер), служащее для объединение в единую сеть нескольких сетей разных типов (например, Ethernet и Arcnet), а также для снижения нагрузки в сети.**

Невыделенный сервер **— сервер, который может выполнять помимо функций по обслуживанию сети еще и другие задачи.**

Несимметричное шифрование (в системах с открытыми ключами — public-key systems) **— метод шифрования, при использовании которого каждый пользователь имеет пару ключей — открытый для шифрования и закрытый (секретный) для дешифрования.**

Область коллизий (collision domain) **— см.** зона конфликтов**.**

Оболочка сетевая **— сетевое программное обеспечение, реализующее связь операционной системы компьютера с сетью.**

Одноранговая сеть (peer-to-peer network)**— сеть, в которой нет выделенных серверов и иерархии среди компьютеров. Все компьютеры могут быть серверами и клиентами.**

Окно коллизий **— величина двойной (круговой) задержки в зоне конфликта (области коллизий).**

Оптоволоконный кабель **— среда передачи информации, представляющая собой стеклянное или пластиковое волокно в оболочке, по которому распространяется световой сигнал.**

Отражение сигнала **— возникновение обратной электромагнитной волны при несогласованных концах электрического кабеля, искажающее сигнал в сети.**

Ошибки передачи **— искажения передаваемой информации в сетях вследствие внешних помех, некачественных кабелей, неисправностей сетевого оборудования, неправильного согласования электрических кабелей, отсутствия гальванической развязки, а также вследствие конфликтов (коллизий)передачи.**

Пакет **— единица информации, передаваемой по сети. Могут быть короткими (порядка десятков байт и даже единиц байт), а также длинными (порядка нескольких килобайт). Включают в себя данные (необязательно), адреса и управляющие коды.**

Петля **— замкнутый контур передачи информации в топологии сети.**

Перегрузка (overload) **— ситуация, при которой сеть не может работать при полной нагрузке большую часть времени. В сетях, использующих метод доступа CSMA/CD, перегрузка связана с ростом числа коллизий из-за конкуренции абонентов в сети.**

Переключатель **— то же, что** коммутатор**.**

Перекрестные помехи **— взаимное влияние (наводки) двух расположенных рядом проводов, искажающее сигналы в этих проводах.**

Перестановка **— один из простейших способов шифрования данных, основанный на изменении расположения символов исходного сообщения. Новая последовательность расположения символов определяется выбранным ключом.**

Повторитель**,** репитер **(**repeater**) — устройство для восстановления и усиления сигналов в сети, служащее для увеличения ее длины.**

Подстановка **— один из простейших способов шифрования данных, основанный на использовании альтернативного алфавита (или нескольких алфавитов, при многоэтапной подстановке) вместо исходного алфавита.**

Показатель использования сети **(**network utilization**) — отношение числа байтов данных, фактически переданных по сети в течение заданного времени, к максимально возможному для данной сети числу. В сетях, использующих метод доступа CSMA/CD, этот показатель связан, в том числе, и с количеством коллизий.**

Порождающий полином **— полином, представляющий собой альтернативную запись числа в двоичной**

системе счисления, ненулевые коэффициенты которого определяют структуру кодера и декодера циклического кода (структуру обратных связей в сдвиговом регистре).

Предложенная нагрузка (offered load) **— количество данных или кадров, которое должна передать сеть.**

Пробка **— 32-битная последовательность, передаваемая абонентом сети Ethernet при обнаружении коллизии для усиления конфликта с целью его обнаружения всеми абонентами, участвующими в конфликте.**

Протокол **— набор правил, алгоритм обмена информацией между абонентами сети.**

Рабочая группа **— группа компьютеров сети, совместно использующая какие-нибудь ресурсы.**

Рабочая станция **— другое название абонента сети, клиента сети (в противоположность серверу) или специального компьютера, ориентированного на работу в сети.**

Размножение кадров **— нарушение обмена в сети с топологией шина при наличии в ней петель.**

Редиректор **— программа, обрабатывающая запросы операционной системы и разделяющая их на локальные и удаленные.**

Ретрансляция **— прием и передача информации без ее изменения, но с восстановлением уровней сигналов и их формы.**

Сеанс **— логическое соединение между абонентами сети для обмена информацией; включает в себя передачу нескольких пакетов.**

Сегмент **— часть сети, ограниченная разделяющими устройствами (репитерами, концентраторами, мостами, маршрутизаторами, шлюзами), иногда используется как синоним понятия сети.**

Сервер **— абонент сети, отдающий в сеть свой ресурс и имеющий или не имеющий доступа к ресурсам сети. Также сервером называют специализированный компьютер, предназначенный для работы в сети (имеет быстродействующие диски большого объема, быстрый процессор, большую память).**

Сервер базы данных **— специализированный компьютер, обеспечивающий клиентов сети доступом к базе данных (по сети пересылаются только запросы и запрашиваемая информация).**

Сервер печати **— компьютер, обеспечивающий доступ клиентам сети к совместно используемому принтеру.**

Сетевая операционная система **— программное обеспечение, управляющее работой сети и позволяющее поддерживать связь и совместно использовать ресурсы.**

Сетевой адаптер (он же контроллер, интерфейс, сетевая карта) **— электронная плата, сопрягающая аппаратуру абонента сети и линии связи сети.**

Сеть на основе сервера **— сеть, в которой имеется четкое разделение абонентов на клиентов и серверов, и в которой есть хотя бы один выделенный сервер.**

Симметричное шифрование **— шифрование, при котором один и тот же ключ используется как для шифрования, так и для дешифрования (расшифрования) данных.**

Скремблер/Дескремблер **— одно из устройств модема, служащее для снижения вероятности сбоя синхронизации на приемном конце линии из-за длинной цепочки единиц или нулей в передаваемых данных.**

Среда передачи информации **— электрический кабель (коаксиальный, витая пара), волоконно-оптический кабель, радиоканал, инфракрасный канал, то есть то, что используется в данной сети для связи абонентов; характеризуется стоимостью, удобством подключения, пропускной способностью (то есть предельной скоростью передачи), предельной длиной линии связи (затуханием сигнала с расстоянием на данной частоте), помехоустойчивостью, секретностью передаваемых данных (возможностью подслушивания), требуемой сложностью адаптеров абонентов, а также рядом специфических параметров, менее важных для пользователей сети.**

Топология **— метод соединения, структура связей абонентов сети. Основные топологии — это звезда, шина и кольцо, реже встречаются топологии цепочка и дерево; топологии различаются требуемой длиной соединительного кабеля, удобством соединения, возможностями подключения дополнительных абонентов, отказоустойчивостью, возможностями управления обменом.**

Трансивер (TRANSmitter+reCEI VER) **— приемопередатчик сети, служащий для умощнения сигналов или для преобразования физической природы сигналов (например, электрических сигналов в световые и наоборот).**

Узел **— компьютер или другое устройство, подключенное к сети, то же, что абонент.**

Узкополосная передача (baseband) **— способ передачи данных по кабелю без модуляции (каждый бит кодируется определенным сочетанием уровней сигнала).**

Централизованное управление обменом **— метод управления обменом в сети, при котором один компьютер или одно специальное устройство управляет всем обменом в сети.**

Циклический код (CRC) **— эффективный помехоустойчивый код, позволяющий обнаружить большое число ошибок в принятой информации при малой избыточности и используемый, в частности, в составе передаваемых по сети пакетов.**

Шеннона теорема **— соотношение, связывающее максимально возможную скорость передачи данных по линии связи с ее полосой пропускания и отношением сигнал/шум.**
Шина **(**bus**) — вид топологии локальной сети, в котором все абоненты параллельно подключены к линейному отрезку кабеля, согласованного на концах.**
Широковещательное сообщение **— сообщение, предназначенное для всех пользователей сети и принимаемое всеми абонентами.**
Широковещательная область **(**broadcast domain**) — часть сети (или вся сеть), по которой распространяются широковещательные пакеты (сообщения).**
Широкополосная сеть **— сеть, в которой используется модуляция передаваемых сигналов и несколько частотных каналов передачи информации.**
Шифрование **— способ защиты информации от несанкционированного доступа за счет ее обратимого преобразования с использованием одного или нескольких ключей.**
Шлюз (gateway) **— устройство (компьютер), служащее для объединения сетей с совершенно различными протоколами обмена.**
Шум **— временные или фазовые искажения сигнала в сети, которые могут нарушить обмен.**
Эквалайзер **— одно из устройств модема, служащее для компенсации искажений амплитудно-частотной характеристики линии, в которой используется модем.**
Электронная почта **— система передачи сообщений между пользователями сети.**
Электронные конференции **— система публичного обмена новостями и обсуждения новостей в сети по разнообразным темам.**
Эхо-компенсация **— одна из функций модема, состоящая в подавлении собственного сигнала модема, отраженного от противоположного конца линии, при дуплексном обмене.**
Ячеистая сеть **— сеть, имеющая множество маршрутизированных соединений между составляющими ее локальными сетями.**