

# Локальные сети

## Введение

Локальные сети в последнее время из модного дополнения к компьютерам все более превращаются в обязательную принадлежность любой компании, имеющей больше одного компьютера. Совершенствование аппаратуры и программных средств достигло такого уровня, когда установить и эксплуатировать простейшую сеть может практически любой более или менее грамотный пользователь, тем более что на рынке имеется множество книг, подробно описывающих процесс установки и обслуживания, а последние версии наиболее распространенной операционной системы Windows содержат в себе довольно развитые сетевые средства, так что даже покупать специальное сетевое программное обеспечение совсем не обязательно. То, что раньше было доступно только посвященным, только специально обученным профессионалам, теперь легко может сделать каждый.

## 1. Определение локальных сетей и их топология

### 1.1. Место и роль локальных сетей

Передача информации между компьютерами существует, наверное, с самого 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 обеспечивают 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 администратором 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).

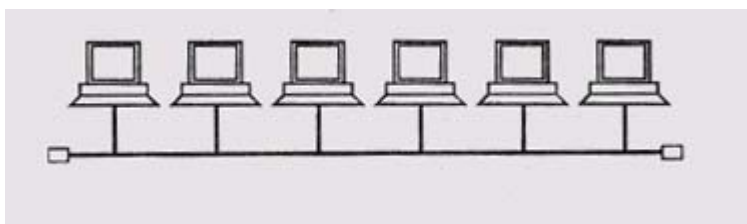


Рис. 1.1. Сетевая топология «шина»

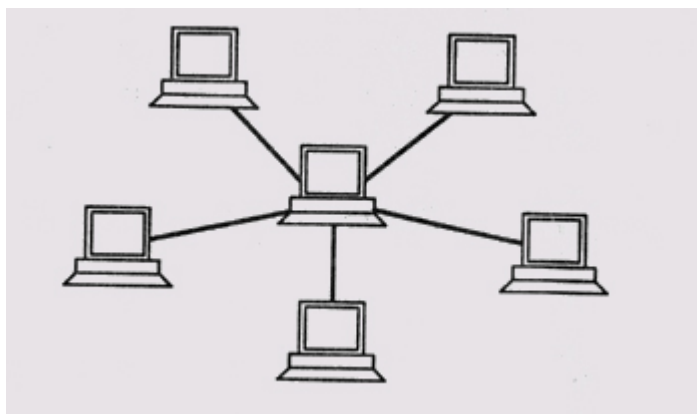


Рис. 1.2. Сетевая топология «звезда»

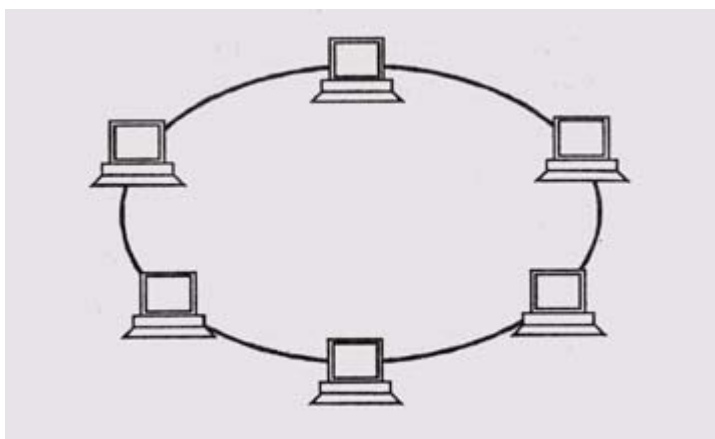


Рис. 1.3. Сетевая топология «кольцо»

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. 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.

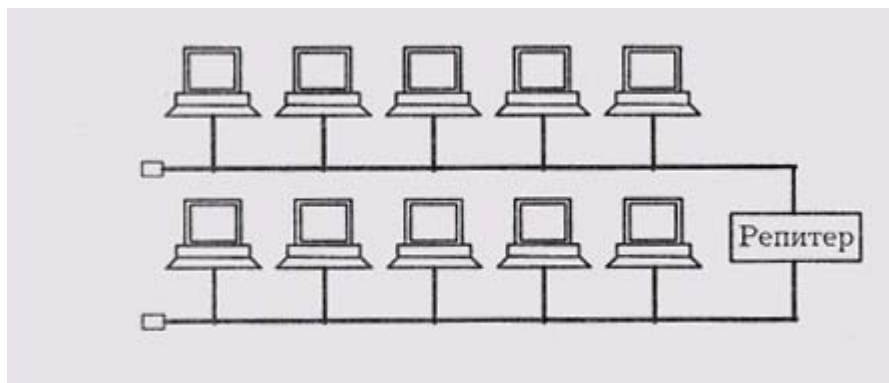


Рис. 1.4. Соединение сегментов сети типа «шина» с помощью репитера

При прохождении по линии связи сети с топологией «шина» информационные сигналы ослабевают 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.

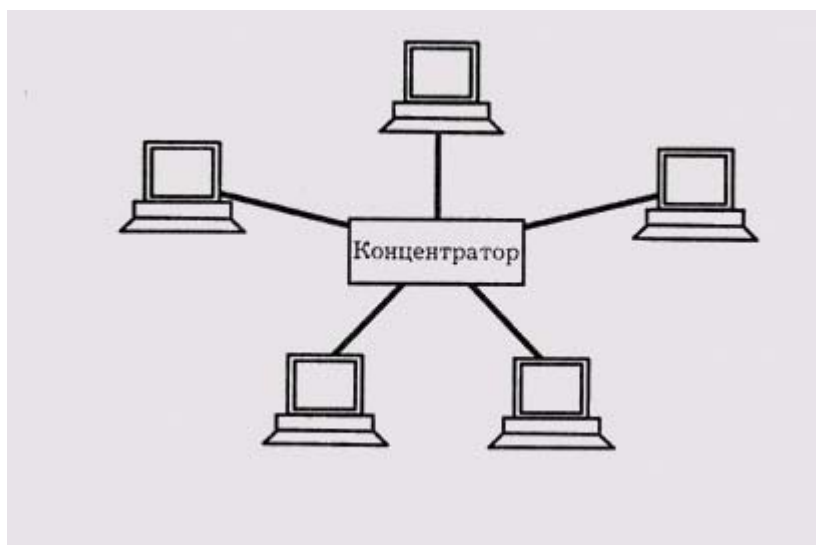


Рис. 1.5. Топология «пассивная звезда»

В центре сети с данной топологией помещается не компьютер, а концентратор, или хаб (hub), выполняющий ту же функцию, что и репитер. Он восстанавливает входящие 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) входящий 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).

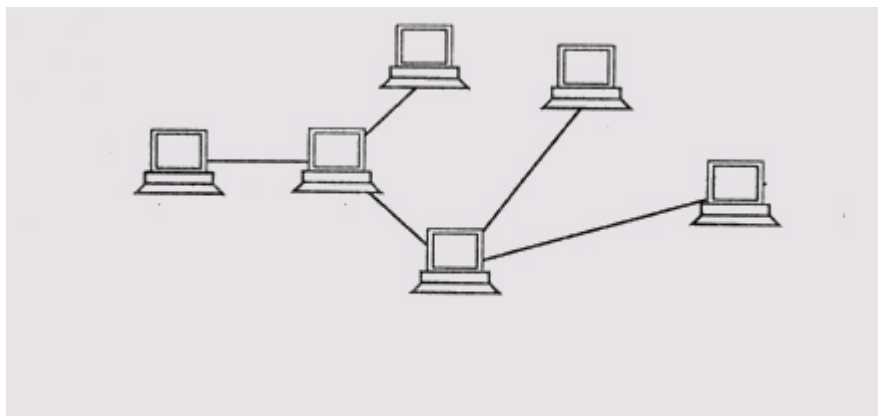


Рис. 1.6. Топология «активное дерево»

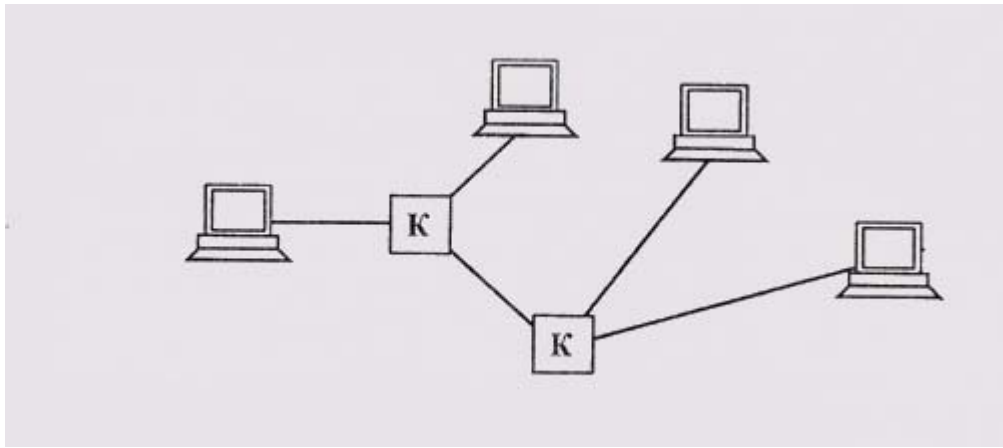


Рис. 1.7. Топология «пассивное дерево». К – концентраторы

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

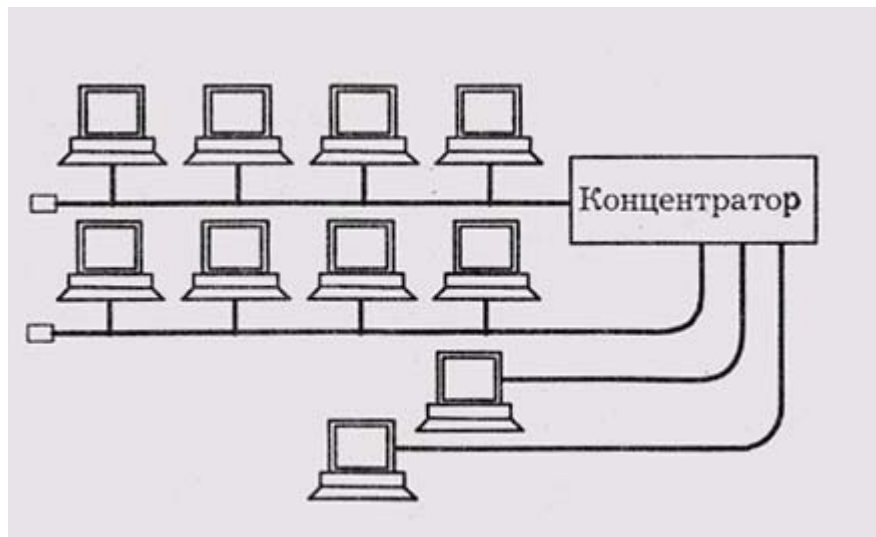


Рис. 1.8. Пример звездно-шинной топологии

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.

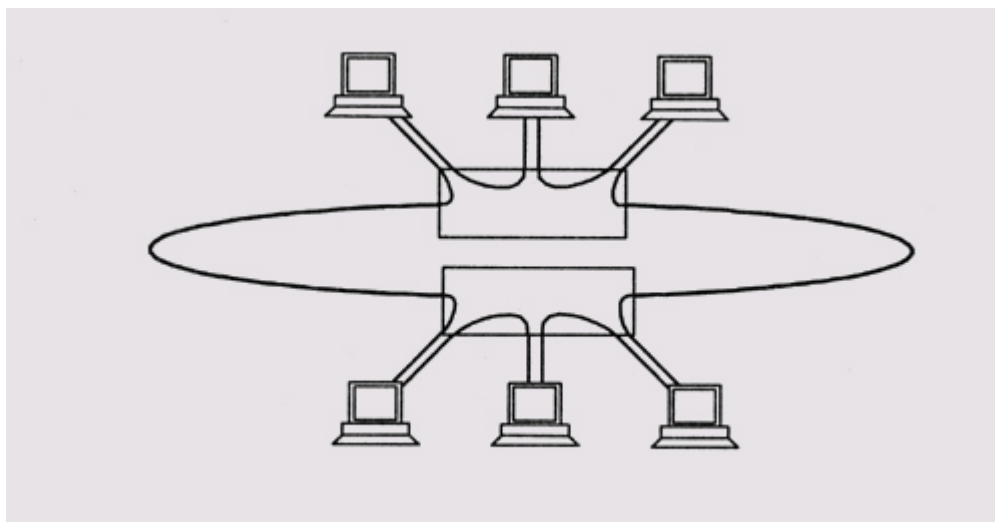


Рис. 1.9. Пример звездно-кольцевой топологии

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.

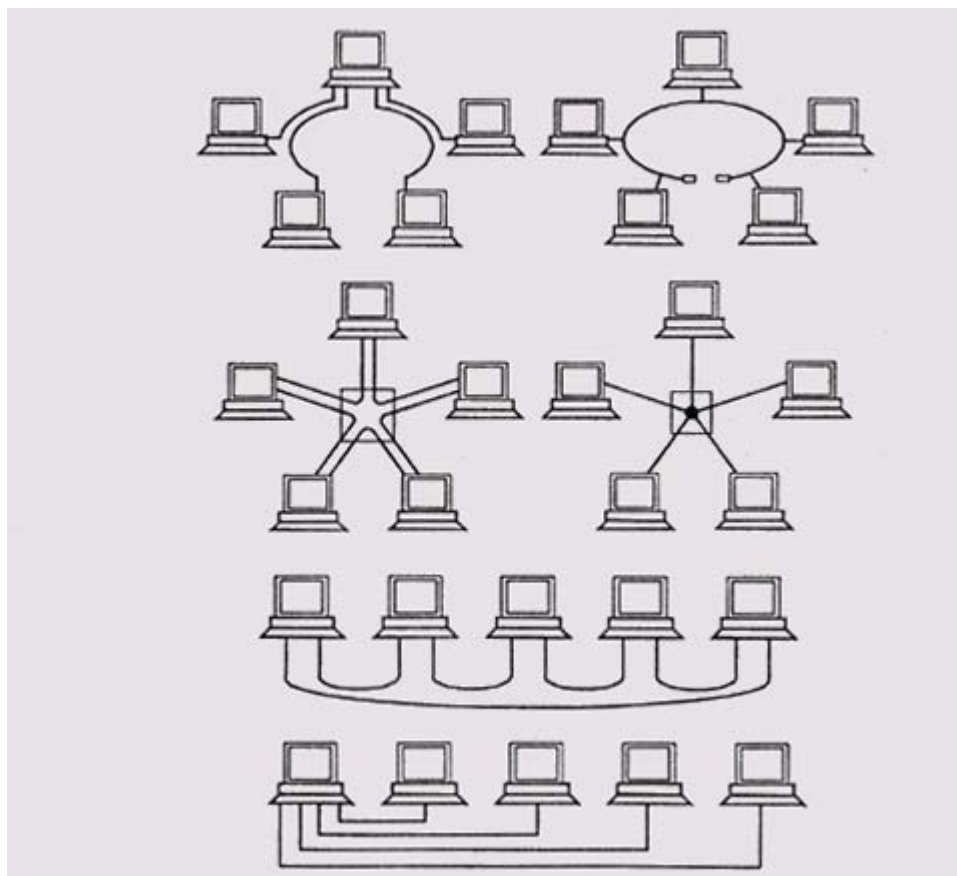


Рис. 1.10. Примеры использования разных топологий

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-единственного 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.

## 2. Среды передачи информации

### 2.1. Кабели на основе витых пар

Средой передачи информации называются те линии связи (или каналы связи), по которым производится обмен информацией между компьютерами. В подавляющем большинстве компьютерных сетей (особенно локальных) используются проводные или кабельные каналы связи, хотя существуют и беспроводные сети.

Информация в локальных сетях чаще всего передается в последовательном коде, то есть бит за битом. Понятно, что такая передача медленнее и сложнее, чем при использовании параллельного кода. Однако надо учитывать то, что при более быстрой параллельной передаче увеличивается количество соединительных кабелей в число раз, равное количеству разрядов параллельного кода (например, в 8 раз при 8-разрядном коде). Это совсем не мелочь, как может показаться на первый взгляд. При значительных расстояниях между абонентами сети стоимость кабеля может быть вполне сравнима со стоимостью компьютеров и даже превосходить ее. К тому же проложить один кабель (реже два разнонаправленных) гораздо проще, чем 8,16 или 32. Значительно дешевле обойдется также поиск повреждений и ремонт кабеля.

Но это еще не все. Передача на большие расстояния при любом типе кабеля требует сложной передающей и приемной аппаратуры: для этого надо формировать мощный сигнал на передающем конце и детектировать слабый сигнал на приемном конце. При последовательной передаче для этого требуется всего один передатчик и один приемник. При параллельной же передаче количество передатчиков и приемников возрастает пропорционально разрядности используемого параллельного кода. Поэтому даже при разработке сети незначительной длины (порядка десятка метров) чаще всего все равно выбирают последовательную передачу.

К тому же при параллельной передаче чрезвычайно важно, чтобы длины отдельных кабелей были точно равны друг другу, иначе в результате прохождения по кабелям разной длины между сигналами на приемном конце образуется временной сдвиг, который может привести к сбоям в работе или даже к полной неработоспособности сети. Например, при скорости передачи 100 Мбит/с и длительности бита 10 нс этот временной сдвиг не должен превышать 5-10 нс. Такую величину сдвига дает разница в длинах кабелей в 1-2 метра. При длине кабеля 1000 метров это составляет 0,1-0,2%.

Правда, в некоторых высокоскоростных локальных сетях все-таки используют параллельную передачу по 2-4 кабелям, что позволяет при заданной скорости передачи применять более дешевые кабели с меньшей полосой пропускания, но допустимая длина кабелей при этом не превышает сотни метров. Примером может служить сегмент 100BASE-T4 сети Fast Ethernet.

Промышленностью выпускается огромное количество типов кабелей, например, крупнейшая кабельная фирма Belden предлагает более 2000 их наименований. Все выпускаемые кабели можно разделить на три большие группы:

- кабели на основе витых пар проводов (twisted pair), которые делятся на экранированные (shielded twisted pair, STP) и неэкранированные (unshielded twisted pair, UTP);
- коаксиальные кабели (coaxial cable);
- оптоволоконные кабели (fiber optic).

Каждый тип кабеля имеет свои преимущества и недостатки, так что при выборе типа кабеля надо учитывать как особенности решаемой задачи, так и особенности конкретной сети, в том числе и используемую топологию. В настоящее время действует стандарт на кабели EIA/TIA 568 (Commercial Building Telecommunications Cabling Standard), принятый в 1995 году и заменивший все действовавшие ранее фирменные стандарты.

Витые пары проводов используются в самых дешевых и на сегодняшний день, пожалуй, самых популярных кабелях. Кабель на основе витых пар представляет собой несколько пар скрученных изолированных медных проводов в единой диэлектрической (пластиковой) оболочке. Он довольно гибкий и удобный для прокладки.

Обычно в кабель входит две витые пары (рис. 2.1) или четыре витые пары.

Неэкранированные витые пары характеризуются слабой защищенностью от внешних электромагнитных помех, а также слабой защищенностью от подслушивания с целью, например, промышленного шпионажа. Перехват передаваемой информации возможен как с помощью контактного метода (посредством двух иголок, воткнутых в кабель), так и с помощью бесконтактного метода, сводящегося к радиоперехвату излучаемых кабелем электромагнитных полей. Для устранения этих недостатков применяется экранирование.

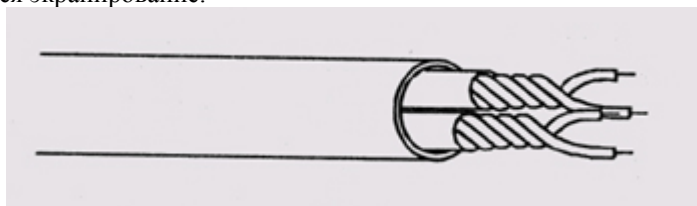


Рис. 2.1. Кабель с витыми парами

В случае экранированной витой пары STP каждая из витых пар помещается в металлическую оплетку-экран для уменьшения излучений кабеля, защиты от внешних электромагнитных помех и снижения взаимного влияния пар проводов друг на друга (crosstalk - перекрестные наводки). Естественно, экранированная витая пара гораздо дороже, чем неэкранированная, а при ее использовании необходимо применять и специальные экранированные разъемы, поэтому встречается она значительно реже, чем неэкранированная витая пара.

Основные достоинства неэкранированных витых пар - простота монтажа разъемов на концах кабеля, а также простота ремонта любых повреждений по сравнению с другими типами кабеля. Все остальные характеристики у них хуже, чем у других кабелей. Например, при заданной скорости передачи затухание сигнала (уменьшение его уровня по мере прохождения по кабелю) у них больше, чем у коаксиальных кабелей. Если учесть еще низкую помехозащищенность, то становится понятным, почему линии связи на основе витых пар, как правило, довольно короткие (обычно в пределах 100 метров). В настоящее время витая пара используется для передачи информации на скоростях до 100 Мбит/с и ведутся работы по повышению скорости передачи до 1000 Мбит/с.

Согласно стандарту EIA/TIA 568, существуют пять категорий кабелей на основе неэкранированной витой пары (UTP):

Кабель категории 1 — это обычный телефонный кабель (пары проводов не витые), по которому можно передавать только речь, но не данные. Данный тип кабеля имеет большой разброс параметров (волнового сопротивления, полосы пропускания, перекрестных наводок).

Кабель категории 2 - это кабель из витых пар для передачи данных в полосе частот до 1 МГц. Кабель не тестируется на уровень перекрестных наводок. В настоящее время он используется очень редко. Стандарт EIA/TIA 568 не различает кабели категорий 1 и 2.

Кабель категории 3 — это кабель для передачи данных в полосе частот до 16 МГц, состоящий из витых пар с девятью витками проводов на метр длины. Кабель тестируется на все параметры и имеет волновое сопротивление 100 Ом. Это самый простой тип кабелей, рекомендованный стандартом для локальных сетей. Сейчас он имеет наибольшее распространение.

Кабель категории 4 - это кабель, передающий данные в полосе частот до 20 МГц. Используется редко, так как не слишком заметно отличается от категории 3. Стандартом рекомендуется вместо кабеля категории 3 переходить сразу на кабель категории 5. Кабель категории 4 тестируется на все параметры и имеет волновое сопротивление 100 Ом. Кабель был разработан для работы в сетях по стандарту IEEE 802.5.

Кабель категории 5 - самый совершенный кабель в настоящее время, рассчитанный на передачу данных в полосе частот до 100 МГц. Состоит из витых пар, имеющих не менее 27 витков на метр длины (8 витков на фут). Кабель тестируется на все параметры и имеет волновое сопротивление 100 Ом. Рекомендуется применять его в современных высокоскоростных сетях типа Fast Ethernet и TPFDDI. Кабель категории 5 примерно на 30-50% дороже, чем кабель категории 3.

Кабель категории 6 - перспективный тип кабеля для передачи данных в полосе частот до 200 МГц.

Кабель категории 7 - перспективный тип кабеля для передачи данных в полосе частот до 600 МГц.

Для присоединения витых пар используются разъемы (коннекторы) типа 5, похожие на всем известные разъемы, используемые в телефонах (RJ-11), но несколько большие по размеру (поэтому они не входят в телефонную розетку). Разъемы RJ-45 имеют восемь контактов вместо четырех в случае RJ-11. Присоединяются разъемы к кабелю с помощью специальных обжимных инструментов. При этом золоченые игольчатые контакты разъема прокалывают изоляцию каждого провода, входят между его жилами и обеспечивают надежное и качественное соединение. Надо учитывать, что при установке разъемов стандартом допускается расплетение витой пары кабеля на длину не более одного сантиметра.

Чаще всего витые пары используются для передачи данных в одном направлении, то есть в топологиях типа «звезда» или «кольцо». Топология «шина» обычно ориентируется на коаксиальный кабель. Поэтому внешние терминаторы, согласующие неподключенные концы кабеля, для витых пар практически никогда не применяются.

Кабели выпускаются с двумя типами внешних оболочек:

кабель в поливинилхлоридной (ПВХ, PVC) оболочке дешевле и предназначен для работы кабеля в сравнительно комфортных условиях эксплуатации;

кабель в тефлоновой оболочке дороже и предназначен для более жестких условий эксплуатации.

Кабель в ПВХ-оболочке называется еще pop-plenum, а кабель в тефлоновой оболочке - plenum. Термин plenum обозначает здесь не собрание руководства какой-то партии, а пространство под фальшполом и над подвесным потолком, где очень удобно размещать кабели сети. Для прокладки в этих скрытых от глаз пространствах как раз удобнее кабель в тефлоновой оболочке, который, в частности, горит гораздо хуже, чем ПВХ-кабель, и не выделяет при горении так много ядовитых газов.

Стоит также отметить, что каждый из проводов, входящих в кабель на витых парах, как правило, имеет свой цвет изоляции, что существенно упрощает монтаж разъемов, особенно в том случае, когда концы кабеля находятся в разных комнатах, и контроль с помощью приборов затруднен.

## 2.2. 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).

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 подключить 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.



Рис. 2.2. Коаксиальный кабель

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. Терминаторы должны быть обязательно согласованы с кабелем, то есть их сопротивление должно быть равно волновому 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, тефлоновый 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.

### 2.3. 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).

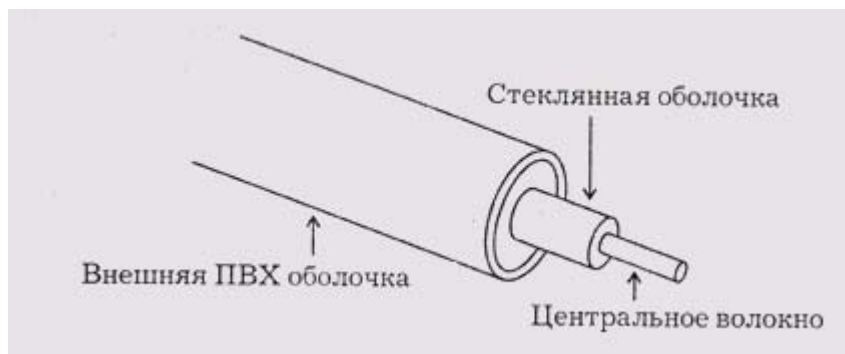


Рис. 2.3. Структура оптоволоконного кабеля

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 10<sup>12</sup> 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 разьеме). 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 время 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 сырьё 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 режимом 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 одномодового 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.

## 2.4. Бескабельные каналы связи

Кроме кабельных, в компьютерных сетях иногда используются также бескабельные каналы. Их главное преимущество состоит в том, что не требуется никакой прокладки проводов (не надо делать отверстий в стенах, не надо закреплять кабель в трубах и желобах, прокладывать его по фальшполам, над подвесными потолками или в вентиляционных шахтах, 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 он 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 м<sup>2</sup>. 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 и в случае 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 являясь передается одновременно всем абонентам. Но в принципе при организации узконаправленной передачи можно реализовать любые ТОР (кольцо, звезда, комбинированные топологии) как на радиоканале, так и на инфракрасном канале.

### **3. Пакеты, протоколы и методы управления обменом**

#### **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 уравнивать в правах всех абонентов, а также примерно уравнивать 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 вероятностью ошибки из-за помех и сбоев. Например, при характерной для локальных сетей величине вероятности одиночной ошибки в 10<sup>-8</sup> пакет длиной 10 Кбит будет искажен с вероятностью 10<sup>-4</sup>, а массив длиной 10 Мбит - с вероятностью 10<sup>-1</sup>. 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 неоправданно 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 аппаратными 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):

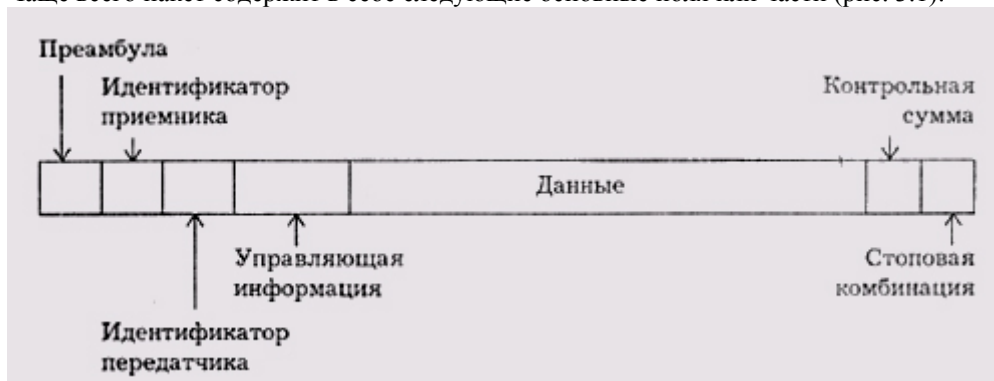


Рис. 3.1. Типичная структура пакета

Стартовая комбинация, или препамбула, 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.

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."

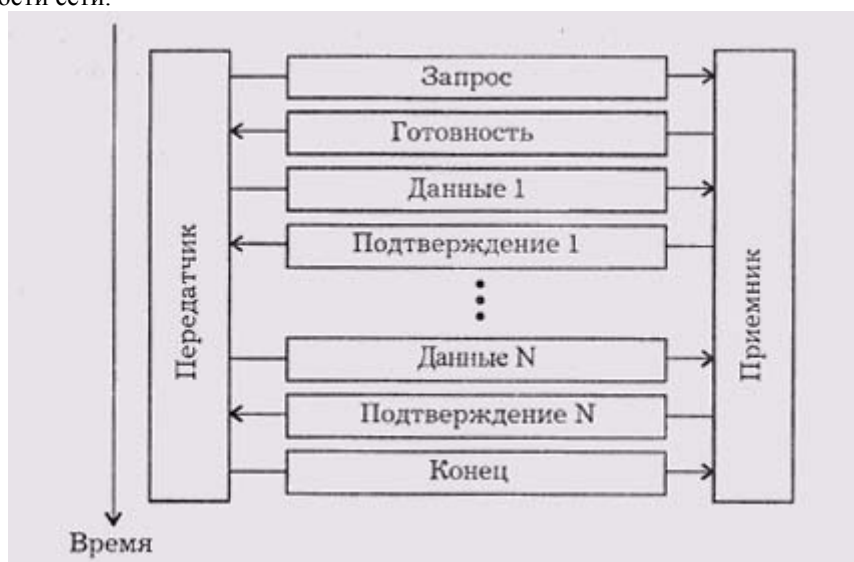


Рис. 3.2. Пример обмена пакетами при сеансе связи

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).

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.

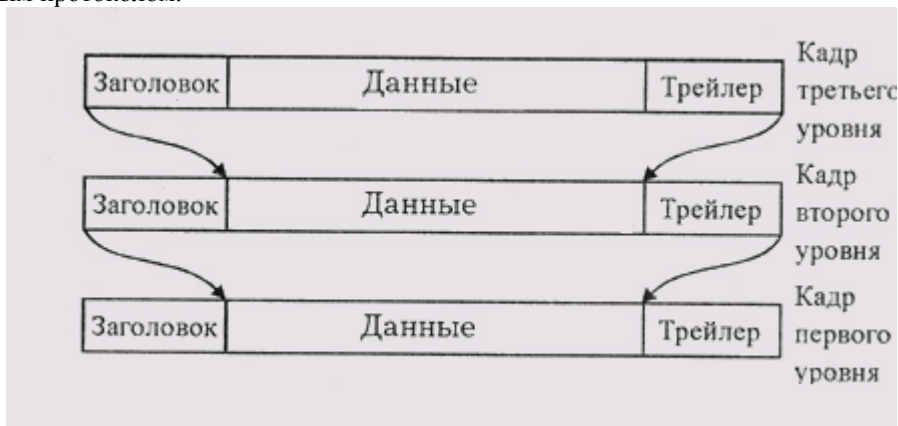


Рис. 3.3. Многоуровневая система вложения кадров

### 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).

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 OUI 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 (многоточковым 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, 100VG-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.

#### 4. Уровни сетевой архитектуры

##### 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.

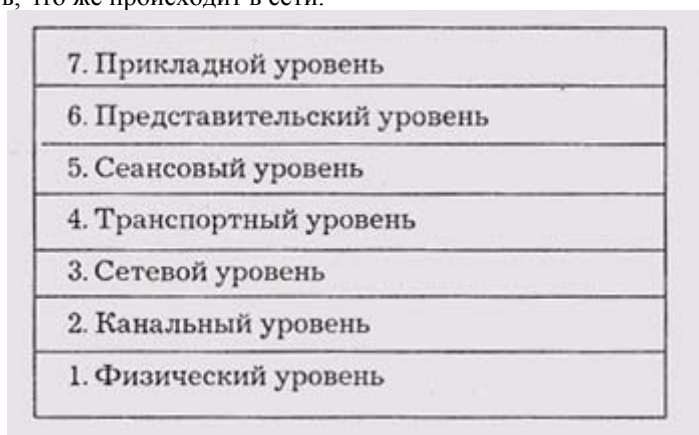


Рис. 4.1. Семь уровней модели OSI

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).

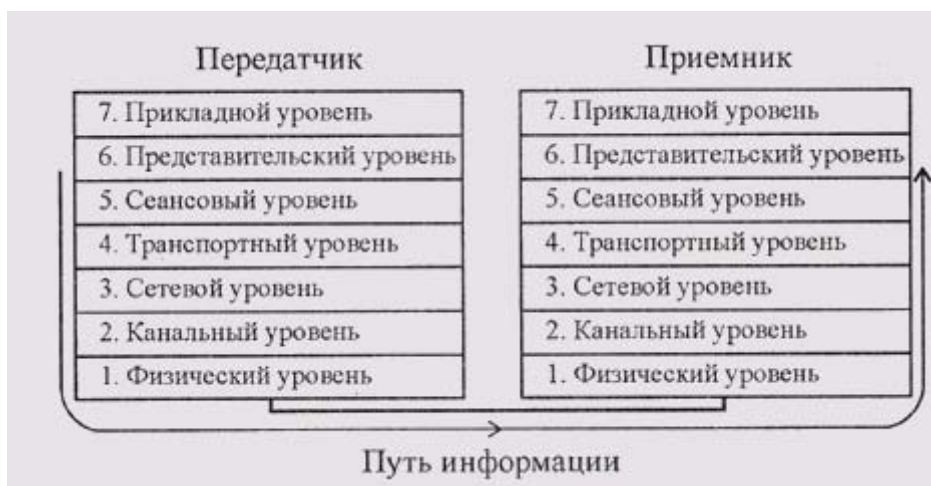


Рис. 4.2. Путь информации от абонента к абоненту Рассмотрим подробнее функции разных уровней.

- 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 - ширококвещательная 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» (100VG-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 ISA или PCI). Плата сетевого адаптера обычно имеет также один или несколько внешних разъемов для подключения к ней кабеля сети (рис. 4.3).

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.

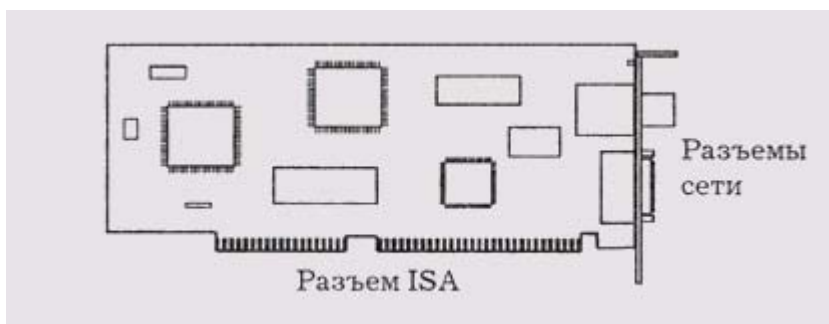


Рис. 4.3. Плата сетевого адаптера

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 переключателей (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 входящих 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.

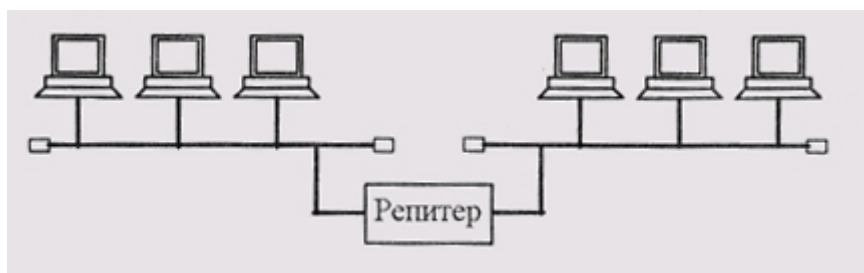


Рис. 4.4. Соединение репитером двух сегментов сети

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. 4.4). 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. 4.5). 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.

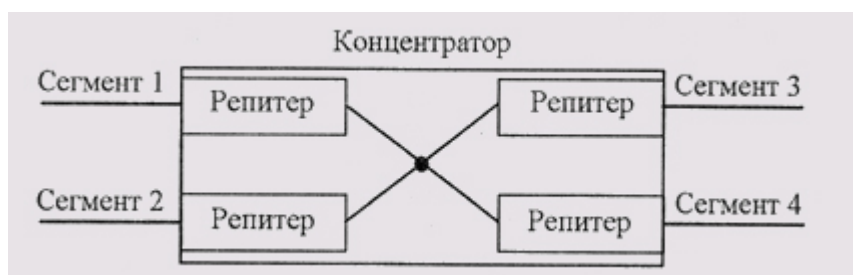


Рис. 4.5. Структура репитерного концентратора

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 переключаящие 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. 4.6). 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.

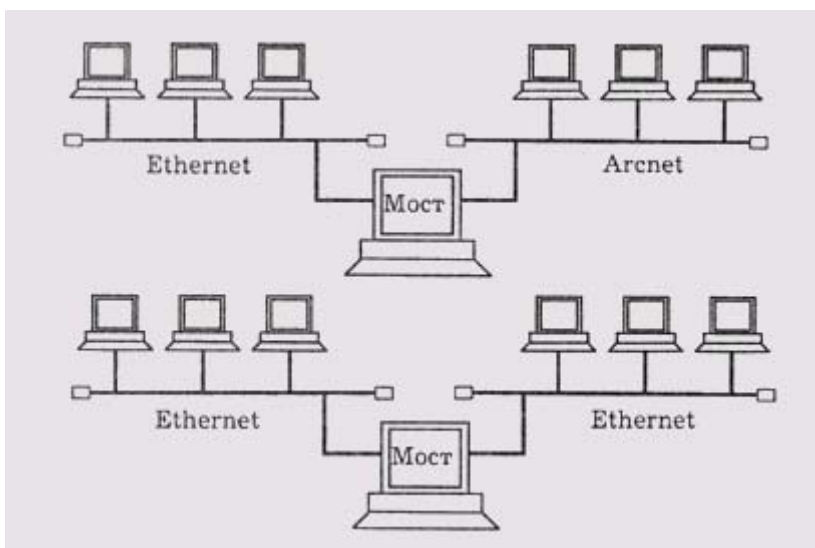


Рис. 4.6. Включение моста

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 репитерные 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 аппаратных 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 основных 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.

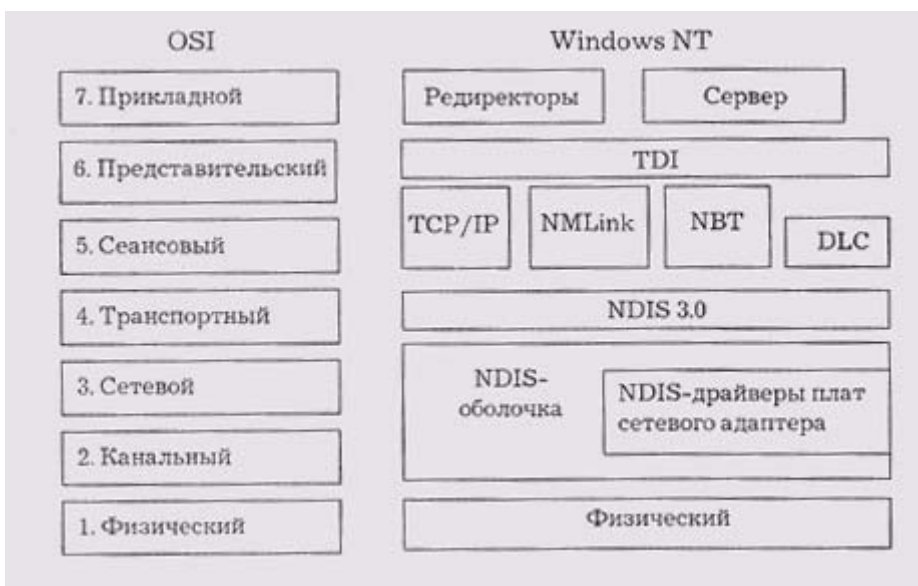


Рис. 4.7. Соотношение уровней модели OSI и протоколов операционной системы Windows NT

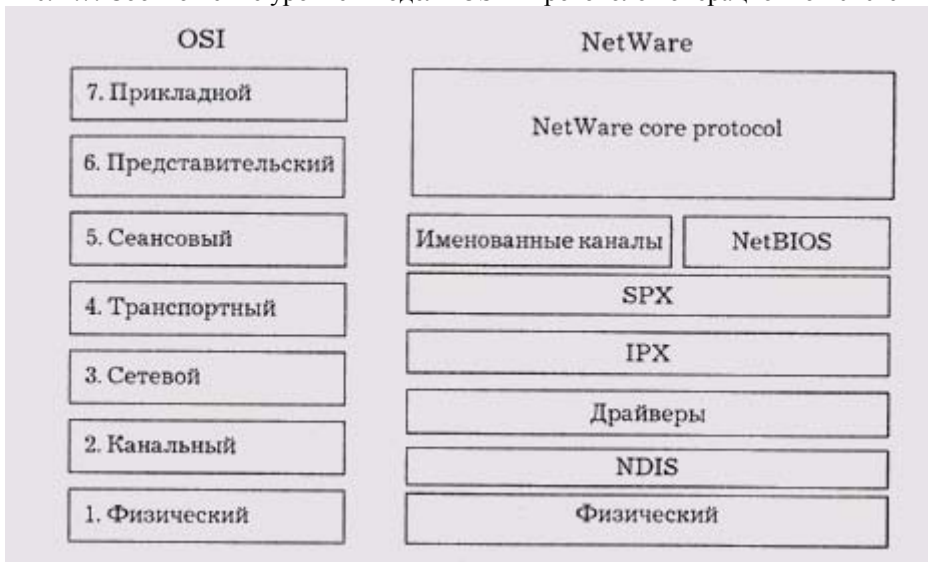


Рис. 4.8. Соотношение уровней модели OSI и протоколов операционной системы NetWare

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 буферизоваться 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.

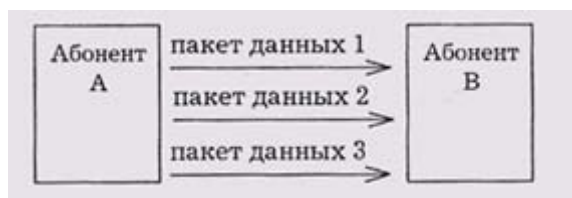


Рис. 4.10. Метод дейтаграмм

- 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.

#### 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 вызваны 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 ридиректором.

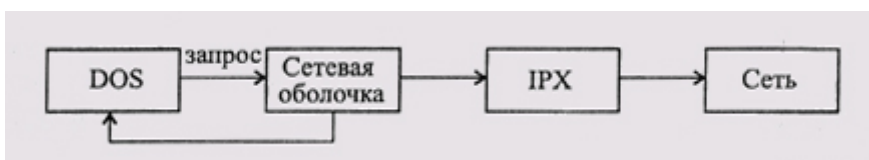


Рис. 4.13. Обработка запросов DOS сетевой оболочкой

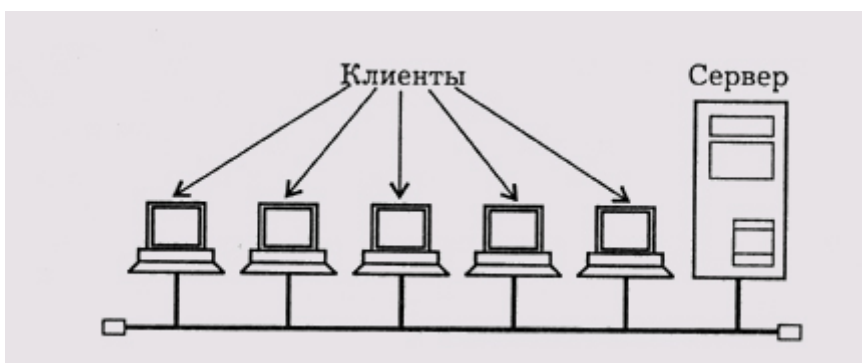


Рис. 4.14. Сеть на основе сервера

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.

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 надежен. 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.

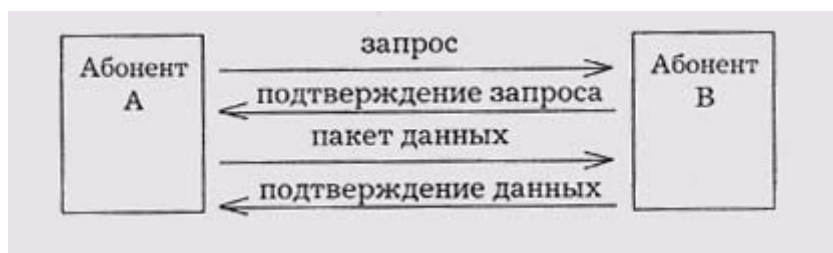


Рис. 4.11. Метод с логическим соединением

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.

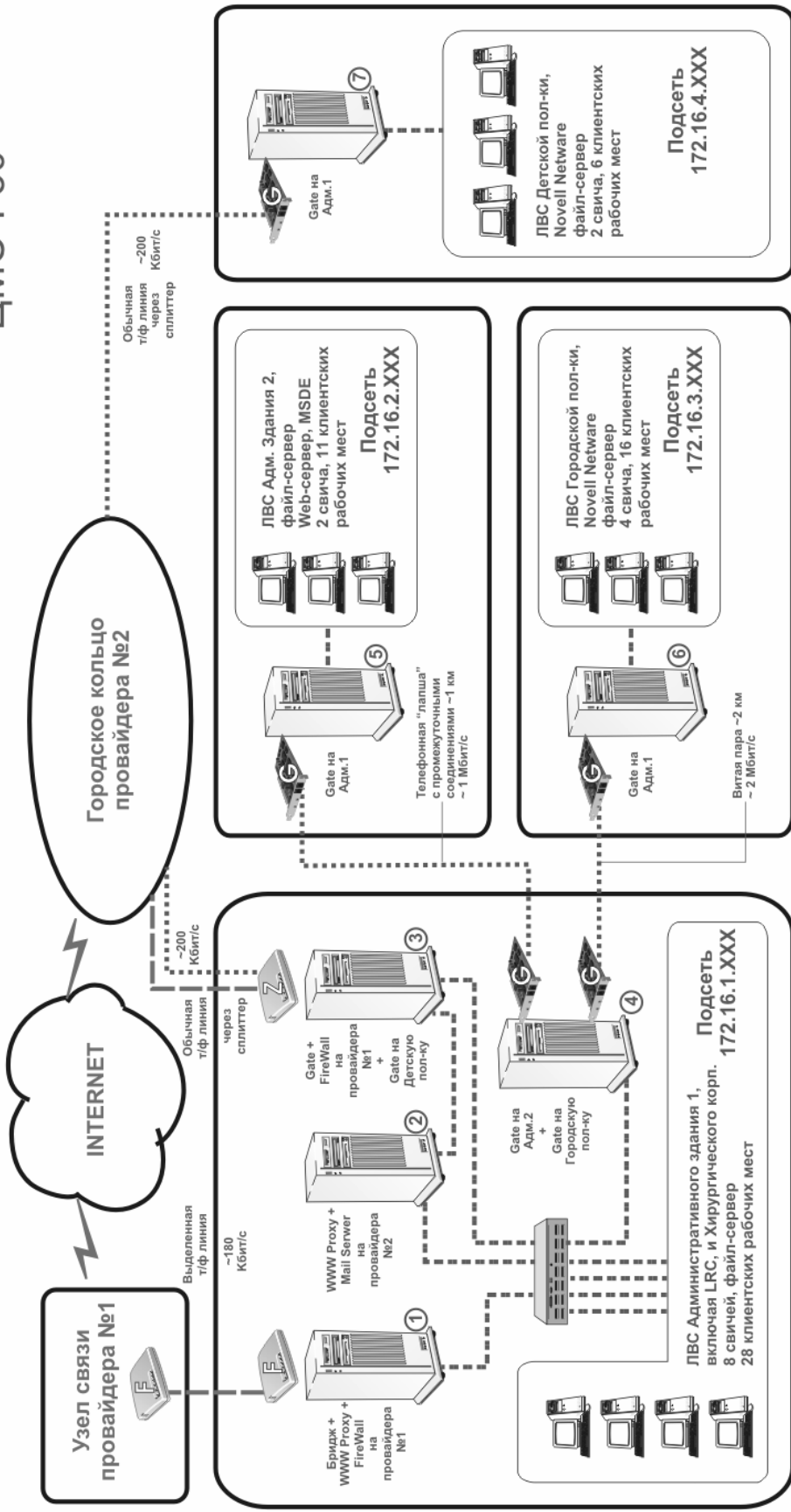
Протоколы IPX/SPX образуют набор, используемый в сетевых программных средствах локальных сетей фирмы Novell (NetWare), которые в наше время являются одними из самых популярных. Это сравнительно небольшой и быстрый протокол, поддерживающий маршрутизацию. Прикладные программы могут обращаться непосредственно к уровню IPX, например, для отправки 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 абонентов которой подключается по коммутируемым линиям (то есть обычным 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 - низкая скорость работы.

Протокол NetBIOS (сетевая базовая система ввода/вывода) был разработан фирмой IBM первоначально для сетей IBM PC Network и IBM Token-Ring по образцу системы BIOS персонального компьютера. С тех пор 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, однако в последующих сетях на более низких уровнях используются стандартные протоколы (например, IPX/SPX), а на долю эмулятора NetBIOS остается 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 протоколов, где каждый протокол точно соответствует конкретному уровню стандартной модели OSI. 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.

# Схема построения корпоративной вычислительной сети ЦМСЧ-50



- Коммутационные устройства**
- МодемFlex DSL
  - DSL модемZuXei-645M
  - Гранч SBNI-1211
- Операционные системы**
- ① Windows XP Pro
  - ② Windows NT4 Client
  - ③ ④ ⑤ ⑥ ⑦ Linux RedHat