Оглавление

1. Компьютерные сети. Основные понятия.

1.1. Компьютерные сети – частный случай распределенных вычислительных систем

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

Создание распределенных систем служит двум основным целям:

- Повышению производительности системы за счет распределения процесса решения задач между компонентами системы.
- Повышению надежности и отказоустойчивости системы (то есть способности системы функционировать в условиях отказа некоторых ее частей) за счет переноса вычислительной нагрузки отказавших компонентов на функционирующие.

В мультипроцессорных компьютерах имеется несколько процессоров, каждый из которых может независимо от остальных обращаться к общей памяти и выполнять собственную программу. Все периферийные устройства являются для общими для всех процессоров такого компьютера. В мультипроцессорном компьютере существует общая для всех процессоров операционная система, которая распределяет вычислительную нагрузку между процессорами. Мультипроцессорным компьютерам не свойственна территориальная распределённость – все его блоки располагаются в одном или нескольких близко расположенных конструктивных элементах, как у обычного компьютера.

Многомашинный комплекс (кластер) – это вычислительная система, состоящая из нескольких компьютеров (каждый из них работает под управлением собственной операционной системы), а также программные и аппаратные средства, связывающие эти компьютеры в одно целое. Связь по данным осуществляется через общую разделяемую дисковую память. Для обмена служебной информацией (распределение вычислительной нагрузки между компьютерами, синхронизация вычислений, реконфигурация системы при отказах) используются более быстрые межпроцессорные связи.

Вычислительная сеть – это совокупность компьютеров, соединенных линиями связи. Линии связи образованы кабелями, сетевыми адаптерами и другими коммуникационными устройствами. Все сетевое оборудование работает под управлением системного и прикладного программного обеспечения. Связи между компьютерами здесь еще слабее, чем в кластерных системах. Каждый компьютер работает самостоятельно под управлением своей ОС, по мере необходимости обмениваясь сообщениями с другими компьютерами. Поток данных, пересылаемых по линиям связей компьютерной сети, называется *сетевым трафиком*.

Основной целью создания вычислительной сети является разделение локальных ресурсов отдельных компьютеров (хранилищ данных, внутренних и периферийных аппаратных устройств – процессоров, дисководов, принтеров) между всеми пользователями сети.

Чтобы компьютер мог работать в сети, его операционная система должна быть дополнена серверными и клиентскими модулями сетевых служб, а также средствами передачи данных между компьютерами. В результате такого добавления операционная система становится сетевой (рис.1.1).

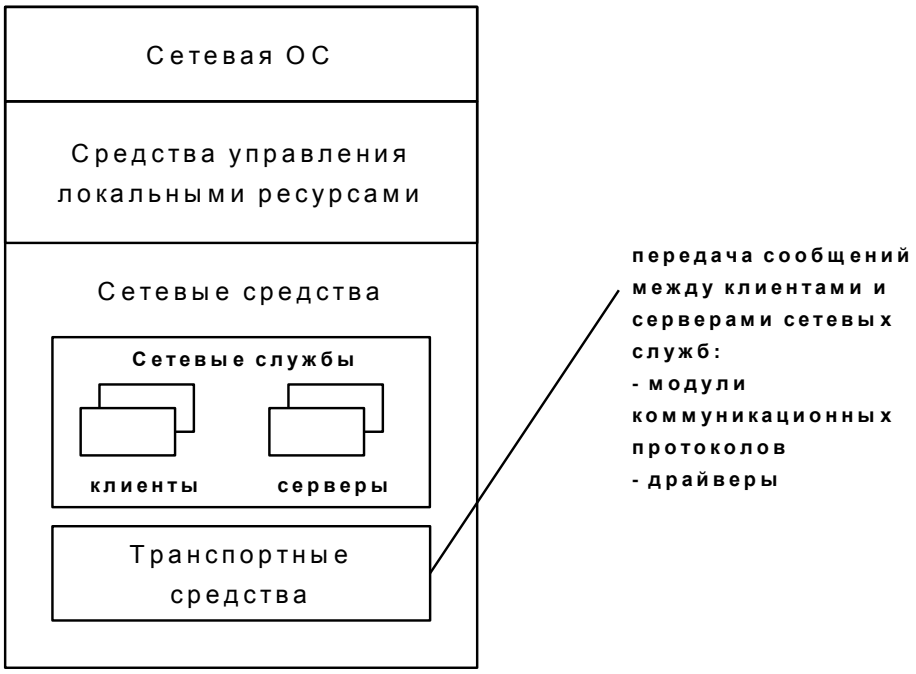


Рис. 1.1. Основные компоненты сетевой операционной системой

Модули первого вида называются *программными серверами* (server), так как их главная задача – обслуживать (serve) запросы на доступ к ресурсам своего компьютера, поступающие от других компьютеров, которые для формирования и передачи на нужный компьютер сетевых запросов должны быть снабжены модулями, называемыми *программными клиентами* (client). К одному серверу могут обращаться несколько клиентов.

Пара модулей «клиент-сервер» обеспечивает совместный доступ пользователей к ресурсам определенного типа, например, к файлам. В этом случае говорят, что пользователь имеет дело с файловой *службой* (service). Обычно сетевая операционная система поддерживает несколько видов сетевых служб для своих пользователей – файловую службу, службу печати, службу электронной почты, службу удаленного доступа и т. п. (например, рис.1.2).

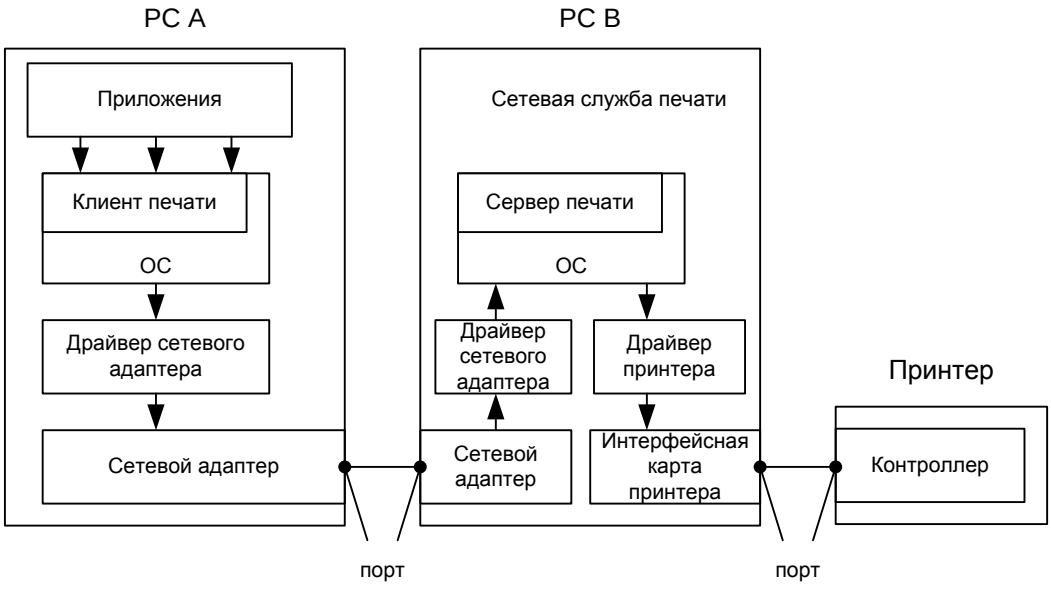


Рис.1.2. Пример использования сетевой службы печати

Сетевые службы относятся к *распределенным* системным *программам*. Однако в сети могут выполняться и распределенные прикладные программы – приложения. Распределенное приложение также состоит из нескольких частей, каждая из которых выполняет какую-то часть работы по решению прикладной задачи. Например, одна часть приложения, выполняющаяся на компьютере пользователя, может поддерживать специализированный графический интерфейс, вторая – работать на мощном удаленном компьютере и заниматься статистической обработкой введенных пользователем данных, третья – заносить полученные результаты в базу данных на компьютере с установленной стандартной СУБД. Распределенные приложения в полной мере используют потенциальные возможности распределенной обработки, предоставляемые вычислительной сетью, и поэтому часто называются *сетевыми приложениями*.

Следует подчеркнуть, что не всякое приложение, выполняемое в сети, является сетевым. Существует много популярных приложений, которые не являются распределенными и целиком выполняются на одном компьютере сети, но могут с помощью встроенных в ОС сетевых служб пользоваться возможностями сети. Например, такие приложения могут с помощью файловых служб получать с удаленных компьютеров данные и обрабатывать их на клиентской машине, как локальные.

Термины «клиент» и «сервер» используются не только для обозначения программных модулей, но и компьютеров, подключенных к сети. Если компьютер предоставляет свои ресурсы другим компьютерам сети, то он называется *сервером*, а если он потребляет эти ресурсы – то клиентом или *рабочей станцией*. Иногда один и тот же компьютер может одновременно быть и сервером, и клиентом. С точки зрения такого деления различают *одноранговые сети* и *серверные сети*.

В одноранговой сети каждый компьютер может быть как сервером, так и клиентом (это сети на основе Windows-98, Windows for Workgroups, Windows XP, и т.д.). В серверных сетях выделяются отдельные компьютеры для серверов и клиентские компьютеры (Novell NetWare, MS Windows NT/2000/2003 и т.д. server). Для разных

видов ресурсов могут использоваться разные сервера (файловые сервера, сервера печати и т. д.).

Итак, использование вычислительных сетей дает предприятию следующие возможности:

- Способность распараллеливать вычисления, увеличивая скорость решения задач.
- Повышение отказоустойчивости системы.
- Совместное использование данных и устройств сети всеми ее пользователями.
- Оперативный доступ к широкому информационному пространству, и, следовательно, возможность быстрого и качественного принятия решений.
- Совершенствование коммуникаций (E-mail, аудио- и видеоконференции и т. д.)

1.2. Классификация компьютерных сетей

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

- Телефонные сети оказывают *интерактивные услуги* (interactive services), так как два абонента, участвующих в разговоре (или несколько, если это конференция), попеременно проявляют активность.
- Радиосети и телевизионные сети оказывают *широковещательные услуги* (broadcast services), при этом информация распространяется только в одну сторону – из сети к абонентам, по схеме «один ко многим» (point-to-multipoint).

В настоящее время ведутся активные работы по созданию универсальных мультисервисных сетей, способных совмещать передачу разных видов трафика: видео, голоса, данных.

Классифицируя сети по территориальному признаку, различают глобальные (*Wide Area Network*, WAN), локальные (*Local Area Network*, LAN) и городские (*Metropolitan Area Network*, MAN) сети.

Локальные сети сосредоточены на территории, не превышающей нескольких километров. Они построены с использованием дорогих высококачественных линий связи, которые позволяют использовать более простые методы передачи данных и оборудование, чем в глобальных сетях, и достигать более высоких скоростей обмена данными (порядка 100 Мбит/с и более). Предоставляемые услуги отличаются широким разнообразием и обычно предусматривают реализацию в интерактивном режиме (on-line).

Глобальные сети появились хронологически первыми. Они объединяют компьютеры, удаленные друг от друга на сотни и тысячи километров. Из-за высокой стоимости линий связи глобальные компьютерные сети часто используют линии связи других телекоммуникационных сетей, качество которых зачастую ниже, чем в локальных сетях. Кроме того, необходимость передавать большие объемы данных по глобальным

сетям и высокая стоимость такой передачи вынуждают ограничивать полосу пропускания для отдельных пользователей. Следовательно, скорость обмена данными в глобальных сетях обычно существенно ниже, чем в локальных (в среднем до 2 Мбит/с). Это ограничивает и набор предоставляемых услуг, реализуемых в основном не в оперативном, а в фоновом режиме.

Одним из проявлений сближения локальных и глобальных сетей является появление сетей масштаба большого города, занимающих промежуточное положение между локальными и глобальными сетями. *Городские сети* (MAN) предназначены для обслуживания территории крупного города. При довольно больших расстояниях между узлами (десятки километров) они располагают качественными линиями связи с высокими скоростями обмена, иногда даже превосходящими таковые в локальных сетях. Сети MAN обычно представляют собой магистрали глобальных сетей, они также могут обеспечивать соединение локальных сетей между собой и подключение локальных сетей к глобальным.

Другим важным признаком классификации сетей является спектр предоставляемых услуг. *Сети операторов связи* (сети поставщиков услуг) оказывают общедоступные услуги, а *корпоративные сети* – услуги сотрудникам предприятия-владельца сети.

Специализированное предприятие, создающее телекоммуникационную сеть для оказания общедоступных услуг, владеющее этой сетью и поддерживающее ее работу, традиционно называют ***оператором связи*** (telecommunication carrier).

Традиционный оператор связи в первую очередь оказывает низкоуровневые транспортные услуги – простую передачу трафика (телефонного или данных) между географическими пунктами без его дополнительной обработки (предоставление каналов в аренду, соединение двух абонентов телефонной сети). Понятие ***поставщик услуг*** (provider) подчеркивает, что предприятие в первую очередь оказывает высокоуровневые информационные услуги – например, доступ в Интернет, размещение в своей сети информационных ресурсов (web-сайтов, баз данных) и не обязательно владеет собственной развитой транспортной инфраструктурой, арендуя транспортные услуги у других операторов. К информационным услугам телефонных сетей относится переадресация вызовов, доступ к справочным службам, голосовая связь и т. д.

Оператора, который предоставляет услуги другим операторам связи, обычно называют *оператором операторов* (carrier of carriers).

Нередко оператор и провайдер услуг выступают в одном лице.

Поставщиков услуг Интернет можно классифицировать по видам оказываемых услуг.

Общий термин *поставщик услуг Интернета* (Internet Service Provider, ISP) в первую очередь относят к компаниям, которые только обеспечивают передачу трафика пользователей в сети других ISP.

*Поставщиком интернет-контента (*Internet Content provider, ICP) называют ISP, который имеет собственные информационно-справочные ресурсы, предоставляя их содержание — **контент** (content) — в виде веб-сайтов. Многие ISP являются одновременно и ICP.

Поставщик услуг хостинга (Hosting Service Provider, HSP) — это компания, которая предоставляет свое помещение, свои каналы связи и серверы для размещения контента, созданного другими предприятиями.

Поставщики услуг по поддержке приложений (Application Service Provider, ASP) — предоставляют клиентам *доступ к крупным универсальным программным продуктам,* которые самим пользователям сложно поддерживать. Обычно это корпоративные пользователи, которых интересуют приложения класса управления предприятием, такие как SAP R3.

В последнее время растет количество поставщиков, предоставляющих сугубо специализированные услуги, например, *поставщики биллинговых услуг* (Billing Service Provider, BSP) обеспечивают оплату счетов по Интернету, сотрудничая с коммунальными службами.

Множество клиентов – потребителей телекоммуникационных услуг – может быть разделено на индивидуальных клиентов и корпоративных клиентов.

Корпоративная сеть – это сеть, главным назначением которой является поддержание работы конкретного предприятия, владеющего данной сетью. Пользователями корпоративной сети являются только сотрудники данного предприятия.

В зависимости от масштаба производственного подразделения, в пределах которого действует сеть, а также от сложности и многообразия решаемых задач различают сети рабочих групп, отделов, здания, кампуса и собственно сети предприятий или корпоративные сети.

Сеть рабочей группы используется небольшой группой сотрудников (обычно не более 15-20 человек), работающих над общей задачей. Эта сеть в основном предназначена для разделения приложений, данных, дорогостоящих периферийных устройств. Такая сеть может содержать один -два файловых сервера. Такие сети обычно не разделяются на подсети, они создаются на основе какой-либо одной сетевой технологии LAN, могут работать на базе одноранговых сетевых ОС. Примером может служить сеть компьютерного класса.

Сеть отдела объединяет несколько сетей рабочих групп в рамках решения общей задачи; имеет один -два общих сервера для обмена данными между рабочими группами; может разделяться на подсети, использовать разные сетевые технологии LAN и ОС в разных рабочих группах; обычно работает под управлением серверной сетевой ОС. В качестве примера можно привести сеть кафедры.

Сеть здания объединяет сети отделов предприятия, расположенные в одном здании на разных этажах. Для объединения не используются внешние связи, распространенным решением является стянутая в точку магистраль на коммутаторе LAN. Например, сеть факультета.

Сеть кампуса: объединяет сети, расположенные в отдельных зданиях на территории предприятия площадью в несколько квадратных километров, при этом глобальные соединения не используются. Для объединения используется локальная распределенная магистраль на базе одной технологии LAN. На уровне сети кампуса возникают

проблемы интеграции и управления неоднородным программным и аппаратным обеспечением. Например, сеть КПИ.

Сеть предприятия (корпоративная сеть) объединяет сети производственных подразделений, расположенных на территории города, страны или нескольких стран, используя для организации внешних связей технологии MAN и WAN. На этом уровне в еще большей степени, чем в сетях масштаба кампуса, проявляются проблемы, связанные с неоднородностью программного и аппаратного обеспечения подразделений и с необходимостью управления и защиты информации, сохраняемой на большом количестве серверов и передаваемых по каналам связи. По аналогии с предыдущими примерами – меж ВУЗовская сеть.

1.3. Архитектура компьютерной сети

Архитектура включает следующие компоненты:

- Топология – структура связей элементов в сети.
- Протоколы – правила взаимодействия функциональных элементов сети.
- Интерфейсы – средства сопряжения функциональных элементов-узлов и программных модулей.
- Технические средства – устройства, которые обеспечивают объединения компьютеров в единую сеть (сетевые адаптеры, концентраторы, кабели и т. д.)
- Сетевые программные средства – управляют работой сети и предоставляют пользовательский интерфейс (сетевые ОС, вспомогательные служебные программы).

Компьютерная (вычислительная) сеть – это совокупность компьютеров, соединенных между собой с помощью каких-то коммуникационных средств. Все сетевое оборудование работает под управлением системного программного обеспечения (ПО), в среде которого выполняются пользовательские прикладные программы.

Параметры компьютеров сети должны соответствовать в первую очередь требованиям прикладного ПО и соответственно требованиям системного ПО, в среде которого оно выполняется .

Протоколы и интерфейсы – это, соответственно, правила взаимодействия и средства сопряжения функциональных элементов сети, т. е. физических устройств и программных модулей (подробнее об этом – в разделе «стандартизация в компьютерных сетях»).

Сетевая технология – это согласованный набор стандартных протоколов и реализующих эти протоколы программно-аппаратных средств, который является минимально достаточным для построения компьютерной сети.

Топология – структура связей между компьютерами и коммутирующими устройствами (подробнее рассмотрена ниже).

Коммуникационные средства включают в себя соединительные кабели, сетевые адаптеры, коммуникационные устройства: повторители, концентраторы, мосты , коммутаторы, маршрутизаторы.

Для обмена данными с внешними устройствами в компьютерах и коммуникационных устройствах предусмотрены *порты* (физические интерфейсы), для которых определены форматы представления данных, электрические характеристики и правила обмена данными с другими устройствами. Логикой передачи данных на внешний интерфейс компьютера управляет аппаратное устройство – сетевой адаптер (контроллер). Программная связь между сетевым адаптером и ОС компьютера осуществляется через драйвер адаптера.

Повторитель используется для усиления сигнала в линии связи и, таким образом, для передачи его на большие расстояния.

Концентратор – многопортовый повторитель, кроме усиления сигнала, пришедшего на один из портов, он рассылает полученные данные на другие порты в соответствии с алгоритмом (логической топологией сети), принятым в конкретной технологии. Например, в технологии Ethernet данные, пришедшие на один порт, концентратор рассылает на все остальные порты, т.е. всем подключенным к нему компьютерам.

Коммутатор и мост – в отличие от концентратора полученные на один порт данные отсылаются только на тот порт, к которому подключен компьютер-адресат. Это соответствие мост или коммутатор определяет из сопоставления адреса назначения в полученных данных и перечня адресов компьютеров, подключенных к его портам (таблицы коммутации).

Маршрутизатор – в отличие от коммутатора, может выбирать наиболее рациональный маршрут (например, кратчайший) до компьютера-адресата в большой сложной сети. Несколько маршрутов от отправителя к адресату могут проходить через разные порты маршрутизатора. Оптимальный маршрут выбирается по таблице маршрутизации, и данные пересылаются на соответствующий этому маршруту порт.

Системное ПО – это сетевые ОС и вспомогательные служебные программы. От того, какие концепции управления локальными и распределенными ресурсами положены в основу сетевой ОС, зависит эффективность работы всей сети. При проектировании сети важно учитывать, насколько просто выбранная ОС может взаимодействовать с другими, насколько она обеспечивает безопасность и защищенность данных, до какой степени она позволяет наращивать число пользователей, можно ли перенести ее на компьютер другого типа и множество других моментов. Основные службы – файловая и печати, обычно предоставляются сетевой ОС, а вспомогательные службы , например, служба баз данных, факса или передачи голоса – системными сетевыми приложениями, или утилитами, работающими под управлением ОС. Вообще говоря, распределение служб между собственно ОС и утилитами весьма условно и меняется в конкретных реализациях ОС.

Кроме собственно обмена данными, сетевые службы должны решать и другие, более специфические задачи, например, задачи распределенной обработки данных. К таким задачам относятся обеспечение непротиворечивости нескольких копий данных, расположенных на разных машинах (служба репликации), или организация выполнения одной задачи параллельно на нескольких машинах (служба вызова удаленных процедур).

Административные службы предназначены для управления работой сети в целом. К ним относятся: служба администрирования учетных записей о пользователях, которая позволяет администратору вести общую базу данных о пользователях сети; система

мониторинга сети, позволяющая просматривать и анализировать сетевой трафик; служба безопасности, в функции которой может помимо всего прочего входить выполнение процедуры доступа с последующей проверкой имени и пароля; и другие.

1.4. Топология компьютерной сети

Структурно компьютерную сеть можно представить в виде множества рабочих станций и серверов, соединенных каналами связи. Разные виды топологий связей имеют свои преимущества и недостатки. Выбирать топологию сети следует так, чтобы она максимально соответствовала структуре организации и ее экономическим возможностям. Среди множества возможных конфигураций связей различают *полно- и неполносвязные*.

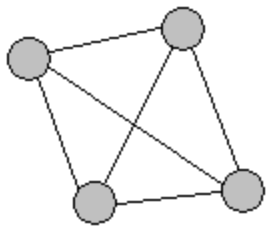


Рис. 1.3. Полносвязная топология

Полносвязная топология (рис.1.3.): каждый узел сети непосредственно связан со всеми остальными. Для объединения N узлов необходимо N * (N – 1) / 2 связей. Достоинства: высокая надежность за счет большого количества резервных связей – от каждого узла к любому другому существует 1 + (N – 2)2 путей. Такая топология может применяться на магистралях сетей с небольшим количеством соединяемых узлов (коммутаторов, маршрутизаторов). Недостатки: низкая экономическая эффективность из-за большого количества связей.

Все остальные топологии являются неполносвязными. Из них наиболее распространены следующие:

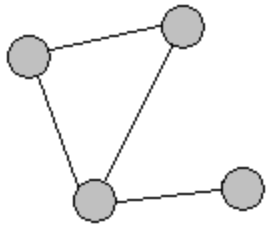


Рис. 1.4. Неполносвязная (ячеистая) топология

Ячеистая топология (рис.1.4). Получается из полносвязной путем удаления из нее части дублирующихся связей. Достоинства: для наиболее важных частей сети обеспечивается надежность за счет резервирования связей. Недостатки: те же, что и у полносвязной топологии. Используется для соединения большого количества узлов (обычно – коммутирующих устройств).

Топология «общая шина». Компьютеры подключаются к общему коаксиальному кабелю по принципу «монтажное или» (рис.1.5).

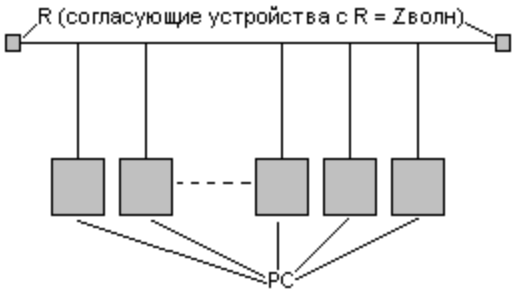


Рис. 1.5. Топология «общая шина»

Сигнал от каждого компьютера распространяется в обе стороны.

Достоинства: дешевизна, простота проводки и подключения компьютеров.

Недостатки: низкая надежность – при нарушении целостности общего кабеля или одного из многочисленных разъемов вся сеть становится неработоспособной.

Топология «звезда» (рис.1.6).

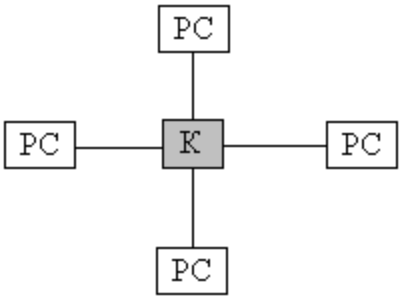


Рис. 1.6. Топология «звезда»

Сервера и рабочие станции подключаются к общему коммутирующему устройству (К). Информация может передаваться двумя способами: всем рабочим станциям (если коммутирующее устройство – концентратор Ethernet), конкретной рабочей станции, которой эта информация предназначена (если коммутирующее устройство – коммутатор или маршрутизатор).

Кроме того, коммутирующее устройство вносит элемент отказоустойчивости в сеть, тестируя свои связи в свободное от передачи данных время и указывая неисправную, а также может выполнять элементарную обработку передаваемых данных, например, фильтровать их.

Достоинства: надежность сети. При выходе из строя луча звезды коммутирующее устройство может отключить неработающую станцию, а вся остальная сеть останется работоспособной.

Недостатки: за счет использования индивидуальных связей расходуется больше кабеля, чем в топологии «общей шины», кроме того, необходимо коммутирующее устройство, поэтому стоимость сети возрастает.

Топология «кольцо» (рис.1.7).

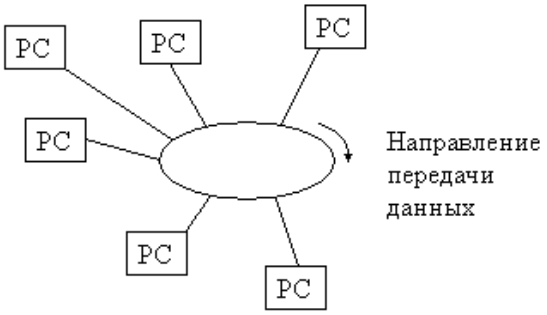


Рис. 1.7. Топология «кольцо»

Данные передаются от одного компьютера другому (с помощью их сетевых адаптеров) по кольцу, пока не достигнут станции-адресата. Станция-адресат копирует пакет данных в свой буфер, ставит на нем пометку о корректном приеме, и отправляет дальше по кольцу. Когда пакет сделает полный оборот по кольцу, он вернется к станции-отправителю, которая прочтет информацию, добавленную в пакет получателем, и уничтожит пакет.

Достоинства: Наличие обратной связи удобно для организации тестирования связности сети и поиска некорректно работающих узлов.

Недостатки: выход из строя любой станции или повреждение кабеля выводят из строя всю сеть. При обычном выключении PC пассивный переключатель ее сетевого адаптера замыкается, сохраняя целостность кольца.

Для повышения надежности используется топология «двойное кольцо». Она образуется при введении в топологию обычного кольца резервного кабеля и устройств реконфигурации сети, представляющих собой пассивные переключатели.

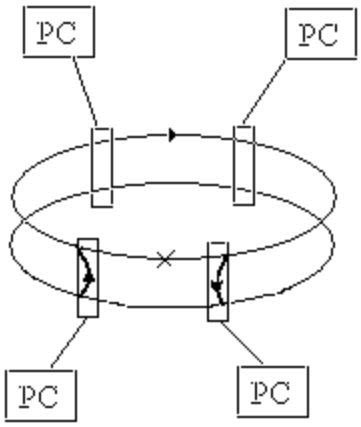


Рис. 1.8. Топология «двойное кольцо» – исключение участка кабеля

В случае неисправности участка кабеля или рабочей станции переключатели соседних РС замыкаются, кольцо разворачивается, исключая поврежденный участок кабеля или станцию (рис.1.8 и рис.1.9).

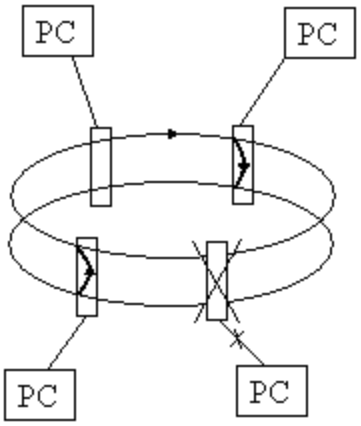


Рис. 1.9. Топология «двойное кольцо» – исключение неисправной станции

Топология «древовидная структура»(рис.1.10).

Образуется соединением между собой нескольких звездообразных топологий.

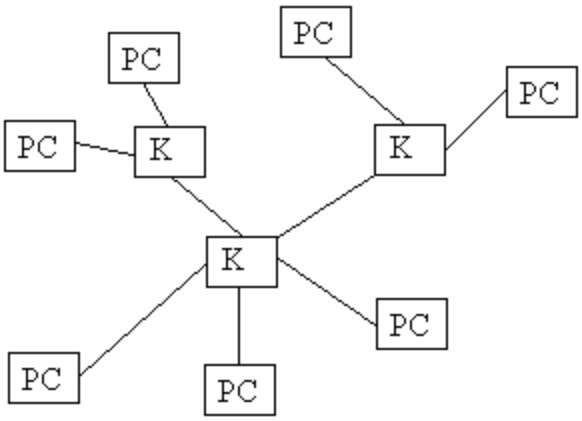


Рис. 1.10. Топология «древовидная структура»

К – коммутирующее устройство.

В настоящее время такая структура является наиболее распространенной как в локальных, так и в глобальных сетях, так как при выходе из строя отдельной ветви «дерева» остальная часть сети остается работоспособной в большей мере, чем в других топологиях.

Достоинства: большая надежность, соответствие реальной структуре информационных потоков.

Четыре рассмотренные топологии являются базовыми, на их основе строятся реальные сети – как объединение тех базовых технологических решений, которым в

наибольшей степени соответствует структура конкретной организации. Получаемые в результате топологии называют смешанными.

1.4.1. Физическая и логическая топологии сети

В компьютерной сети принято различать физические и логические связи.

Физическая топология – это конфигурация физических соединений компьютеров (например, кабельная система).

Логическая топология – это маршруты информационных потоков между узлами сети.

Логическая и физическая топологии сети могут совпадать (например, физическая топология «кольцо», в которой данные передаются по кругу). Однако они могут и быть различными (например, физическая топология «звезда» с концентратором, а логическая – «общая шина», так как данные, получаемые от любого компьютера, рассылаются концентратором всем остальным компьютерам).

1.4.2. Линии связи

Линии связи подразделяются на:

- Индивидуальные
- Разделяемые

Индивидуальные линии связывают пары устройств, обменивающихся между собой данными. При этом скорость обмена данными между этими устройствами будет максимально возможной, но какую-то часть времени линия будет не использоваться (так как не всегда есть данные для передачи). Кроме того, на организацию индивидуальных линий связи расходуется больше кабеля, чем на организацию разделяемых.

Разделяемые линии связи – это линии, которые попеременно используются разными устройствами. Они вводились исходя из экономических соображений. Для их организации необходимо разрешить ряд проблем:

- обеспечение электрических характеристик сигнала при подключении нескольких приемников и передатчиков к одному проводу;
- разделение во времени данных, передаваемых разными устройствами, то есть определение порядка доступа станций к общей линии связи, поскольку в один момент времени может передавать данные только одна станция.

При большом количестве компьютеров быстродействие разделяемой среды оказывается ниже, чем среды с индивидуальными линиями, так как устройствам приходится ожидать доступа к общей линии. Однако при этом более эффективно используются сами линии (отсутствуют простои).

Поскольку решение перечисленных выше проблем, связанных с организацией разделяемой среды, в глобальных сетях резко усложняется, то в этих сетях разделяемые среды не используются.

1.5. Адресация узлов в компьютерных сетях

В пределах одной компьютерной сети адреса всех узлов должны быть уникальными. Выделяют три типа адресов, которые можно использовать одновременно в ЛВС.

1. Аппаратные или MAC-адреса. Они применяются для идентификации узлов ЛВС и жестко связаны с аппаратурой, например, сетевыми адаптерами. Они выглядят, например, так: 0081005e24a8. Уникальность адресов гарантируется фирмой-изготовителем, каждой из которых выделяется определенный диапазон адресов.

При замене аппаратуры изменяется и адрес узла, например, при замене адаптера – адрес компьютера.

2. Числовые адреса применяются для структурированных сетей, то есть таких, которые состоят из подсетей. Эти адреса назначаются программным путем при настройке узлов и легко могут быть изменены. Такие адреса имеют иерархическую структуру. Типичными примерами иерархических числовых адресов являются сетевые адреса IP и IPX. В них поддерживается двухуровневая иерархия, адрес делится на старшую часть – номер сети и младшую часть – номер узла. Такое деление позволяет передавать сообщения между сетями только на основании номера сети, а номер узла используется после доставки сообщения в нужную сеть – точно так же, как название улицы используется почтальоном только после того, как письмо доставлено в нужный город. Пример IP-адреса – 126.82.11.103.

3. Символьные адреса и имена предназначены для запоминания людьми и поэтому обычно являются осмысленными. Они могут использоваться как в небольших сетях, где за их уникальность отвечает сетевой администратор (например, cad, dragon2), так и в крупных сетях. В крупных сетях такие адреса имеют многоуровневую иерархическую организацию. Пример такого адреса – www.jpl.nasa.gov.

За уникальность числовых и символьных адресов в крупных сетях ответственен ряд специальных организаций, например, в Internet – InterNIC, IANA.

В современных сетях, как правило, используются все типы адресов. Пользователи адресуют компьютеры символьными именами, которые автоматически заменяются в передаваемых сообщениях на числовые. С помощью числовых адресов сообщения передаются из одной сети в другую, а после доставки сообщения в сеть-адресат вместо числового адреса используется аппаратный адрес компьютера-адресата.

Проблема установления соответствия между адресами различных типов, которой занимаются протоколы разрешения адресов, может решаться как *централизованными*, так и *распределенными* средствами. В случае централизованного подхода в сети выделяются один или несколько компьютеров (серверов имен), в которых хранится таблица соответствия друг другу имен различных типов, например, символьных и числовых. Все остальные компьютеры обращаются к серверам имен, чтобы по символьному имени определить числовое имя компьютера, с которым необходимо обменяться данными.

При другом, распределенном, походе, каждый компьютер сам решает задачу установления соответствия между адресами. Например, если пользователь указал в качестве узла назначения числовой номер, то перед началом передачи данных

компьютер-отправитель посылает всем компьютерам сети широковещательное сообщение с просьбой опознать это числовое имя. Все компьютеры, получив это сообщение, сравнивают полученное имя с собственными именами. Компьютер, обнаруживший совпадение, посылает ответ, содержащий его аппаратный адрес, после чего становится возможным обмен данными.

Хотя распределенный подход упрощает организацию разрешения адресов, но сильно загружает сеть широковещательными запросами и потому пригоден лишь для небольших локальных сетей. В качестве примера можно привести протокол ARP (ARP – Address Resolution Protocol), который применяется для нахождения соответствия между сетевыми и аппаратными адресами. Централизованный подход может использоваться в сетях любого масштаба. Наиболее известная служба централизованного разрешения адресов – это служба доменных имен (DNS – Domain Name Service) в Internet, которая применяется для нахождения соответствия между символическими и сетевыми адресами.

Перечисленные три типа адресов могут быть *индивидуальными*, то есть идентифицировать конкретный порт узла сети (компьютера или коммуникационного устройства). Также они могут быть *групповыми* – то есть адресами нескольких узлов, которым одновременно передаются данные, или *широковещательными* – данные, направленные по таким адресам, должны быть переданы всем узлам сети. Групповые и широковещательные адреса при необходимости назначаются узлам в дополнение к их индивидуальным адресам.

После того, как пересылаемые по сети данные достигают узла-адресата, ПО компьютера - адресата должно направить их соответствующей программе – процессу, адрес которого прилагается к адресу узла. Уникальность адреса процесса должна обеспечиваться только в пределах компьютера. Примерами адресов процессов являются *номера портов* протоколов TCP и UDP из стека TCP/IP.

1.6. Стандартизация в компьютерных сетях

Стремление максимально упорядочить и упростить процессы разработки и модернизации компьютерных сетей, обеспечить совместимость оборудования различных производителей определило необходимость введения определенных стандартов.

Идеологической основой стандартизации в компьютерных сетях стал многоуровневый подход к разработке средств сетевого взаимодействия. Для организации взаимодействия сетевых компонентов двух узлов необходимы следующие средства:

Протокол – это формальные правила, которые определяют формат и последовательность сообщений, которыми обмениваются сетевые компоненты одного уровня, но в разных узлах.

Интерфейс – это формальные правила, которые определяют взаимодействие сетевых компонентов соседних уровней одного узла.

Иерархический набор согласованных между собой протоколов, достаточный для организации взаимодействия узлов сети (на всех уровнях), называется *стеком коммуникационных протоколов*. Наиболее известные стеки протоколов:

- TCP/IP (на этом стеке построен Internet).
- IPX/SPX
- SNA
- OSI
- NetBIOS/SMB
- DECnet

Протоколы могут реализовываться как программно, так и аппаратно. На нижних иерархических уровнях протоколы реализуются как аппаратно, так и программно, а на верхних – программно.

В стандартизации важную роль играет понятие *открытой системы*. Открытая система – это любая система (компьютер, сеть, ОС, программный пакет и так далее), построенная в соответствии с общедоступными спецификациями стандартов, принятых в результате публичного обсуждения всеми заинтересованными сторонами.

Спецификация – это формальное описание программных и аппаратных компонентов (принципы их функционирования, взаимодействия с другими компонентами, а также набор их характеристик и ограничений).

Открытые спецификации – это общедоступные спецификации, опубликованные и соответствующие стандартам. Такими спецификациями, например, являются ОС Unix, модель OSI, сеть Internet. *Закрытые спецификации* не публикуются. Их применение возможно по лицензии фирмы-разработчика за определенную плату, например, ОС Windows.

В начале 1980-х годов ряд международных организаций по стандартизации разработал модель, сыгравшую большую роль в развитии сетей - модель OSI (Open

System Interconnection). Эта модель стандартизирует взаимодействие открытых систем, определяет 7 уровней такого взаимодействия, дает им стандартные имена и указывает, какие функции должен выполнять каждый уровень (рис.1.11).

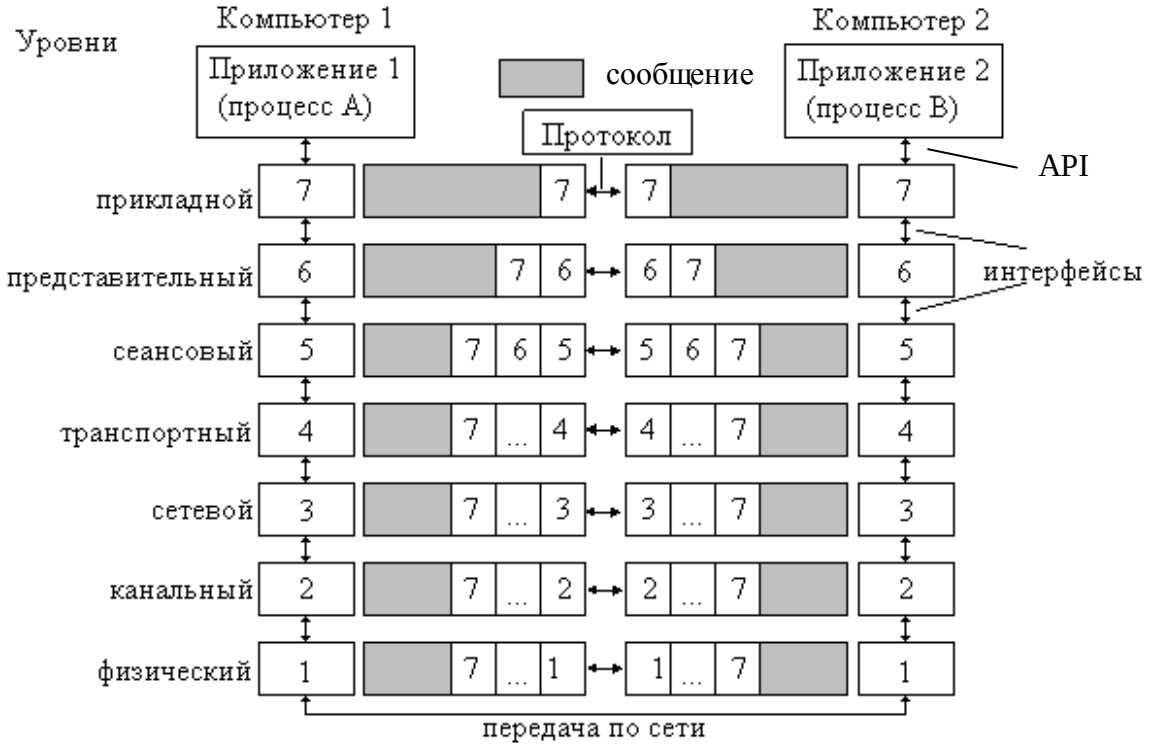


Рис. 1.11. Уровни модели OSI

Пусть, например, приложение обращается с запросом к файловой службе (прикладному уровню, реализованному в ОС) с целью записи файла на удаленном компьютере. Прикладной уровень формирует сообщение, состоящее из пересылаемых данных и заголовка со служебной информацией для прикладного уровня компьютера-адресата (тип операции, место записи и так далее). Затем прикладной уровень передает сформированное сообщение нижележащему уровню. Каждый последующий уровень выполняет над полученным сообщением действия, которые указаны в заголовке предыдущего уровня, и добавляет к сообщению свой заголовок. В нем содержатся указания для протокола аналогичного уровня на компьютере-адресате, и для протокола нижележащего уровня на локальном компьютере.

На компьютере-адресате каждый уровень выполняет действия, указанные в соответствующем заголовке полученного сообщения, удаляет свой заголовок и направляет сообщение протоколу более высокого уровня.

Таким образом, сообщение имеет следующий вид, показанный на рис.1.12.

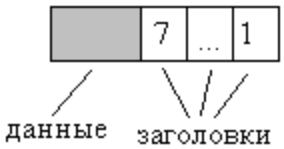


Рис. 1.12. Структура сообщения

Приложения могут брать на себя функции протоколов некоторых уровней описанной модели. Например, СУБД может располагать встроенными средствами доступа к файлам. Такие приложения могут обращаться напрямую к протоколам транспортного или даже сетевого уровня, которые реализованы в ОС.

1.6.1. Основные функции уровней модели OSI

Прикладной уровень – это набор разнообразных протоколов, с помощью которых выполняются прикладные задачи. С их помощью пользователь получает доступ к разделяемым *ресурсам сети* (файлам, принтерам, Web-страницам, e-mail и так далее). Примеры таких протоколов – FTP, HTTP, SMTP из стека TCP/IP.

Протоколы представительного уровня обеспечивают выбор вида представления данных, их интерпретацию, преобразование их кодировки и синтаксиса для разных протоколов прикладного уровня, шифрование данных. Пример – SSL из стека TCP/IP.

Сеансовый уровень предназначен для организации сеансов связи между прикладными процессами на разных рабочих станциях, то есть установки и завершения сеансовых соединений, управления обмена данными, синхронизации соединения. Этот уровень введен для увеличения надежности передачи информации. Он практически не используется самостоятельно, чаще – как часть вышележащего прикладного уровня, или нижележащего - транспортного.

Единица данных, сформированная протоколами трех верхних уровней, называется *сообщением*.

Транспортный уровень обеспечивает верхним уровням стека протоколов передачу данных с требуемой степенью надежности. Это относится к возможности восстановления разорванного соединения, установления приоритета передачи данных. Главная задача этого уровня – обнаружение и устранение ошибок передачи данных, в частности, организация повторной передачи поврежденных и/или потерянных сообщений. Примеры транспортных протоколов – TCP и UDP из стека TCP/IP, SPX из стека IPX.

Сетевой уровень предназначен для обеспечения маршрутизации информации и управления информационными потоками, а также обнаружения ошибок и сообщения о них протоколам верхних уровней.

Единица данных, сформированная протоколами сетевого и транспортного уровней, называются *пакетами*.

Маршрутизацией называется выбор наилучшего (по каким-либо критериям) маршрута для передачи данных между узлами сети. Сеть может быть составной, то есть состоять из фрагментов, выполненных по разным технологиям и соединенных между собой маршрутизаторами. Внутри сети определенной технологии доставка данных осуществляется протоколами канального уровня с использованием локальных (например, аппаратных) адресов, а между сетями – протоколами сетевого уровня (например, IP из стека TCP/IP) с использованием сетевых адресов. Маршрутизаторы собирают информацию о топологии составной сети и запоминают ее в таблицах

маршрутизации. Например, PC A из сети 1 на рис.1.13 посылает сообщение PC B из сети 5.

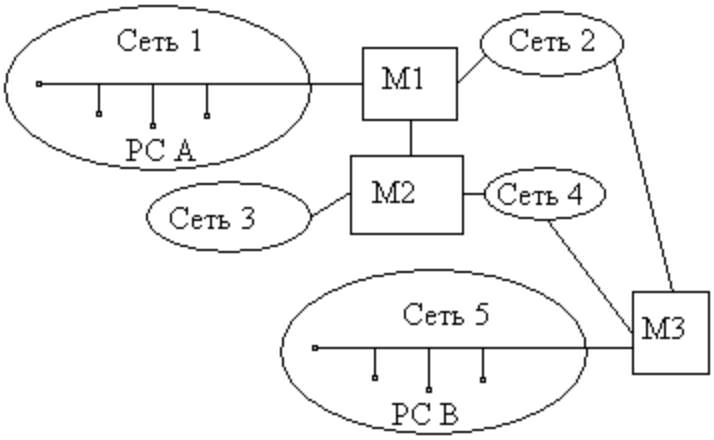


Рис. 1.13. Организация маршрутизации

Передача возможна по двум путям – M1-M3 или M1-M2-M3. Первый маршрут короче, но выбор может осуществляться по критерию максимальной пропускной способности канала или минимальному времени прохождения пакета.

Канальный уровень обеспечивает организацию логического канала между получателем и отправителем в физической среде передачи. Канальный уровень ориентирован на конкретную сетевую технологию. Одна из его основных задач – организация доступа к среде передачи. Метод доступа определяет алгоритм, задающий порядок, в соответствии с которым компьютеры обмениваются данными в общей физической среде. Для организации такого обмена необходимо так же определить формат пакета данных и формат локальных адресов в данной технологии. Еще одна важная задача канального уровня – обнаружение, и, возможно, коррекция ошибок при передаче данных. Он обязательно вычисляет контрольную сумму для всего пакета и помещает ее в заголовок (или концевик) пакета. Но исправление обнаруженных ошибок в полученных пакетах не является обязательной функции канального уровня, протоколы отдельных технологий могут это делать, а других - нет. Примеры канальных протоколов – Ethernet, FDDI, и т.д.. Сообщения этого уровня называются *кадрами*.

Физический уровень обеспечивает механическую (стандартизация разъемов, контактов) и электрическую (форма сигналов, уровни тока и напряжения сигналов и 1.0), совместимость оборудования (приемников и передатчиков), определяет типы кодирования, скорость передачи и функциональные средства организации физических соединений при передаче данных между узлами. Он реализован во всех устройствах, которые подключаются к сети. Этот уровень не является логическим и имеет дело с передачей *потока бит* информации в виде сигналов по физическим линиям связи.

Четыре нижних уровня (включая транспортный) образуют *транспортную службу* компьютерной сети, которая и обеспечивает передачу данных между рабочими станциями, а три верхних уровня обеспечивают *логическое взаимодействие прикладных процессов*.

Соответствие функций сетевых устройств уровням модели OSI и их типичное место в локальной сети показано на рис.1.14 и 1.15.

На конечном компьютере протоколы физического уровня реализуются аппаратно в сетевых адаптерах и портах (например, последовательном, параллельном и т.д.), протоколы канального уровня – частично аппаратно в сетевом адаптере, частично программно в драйвере сетевого адаптера, который осуществляет взаимодействие с ОС. Протоколы остальных уровней модели OSI реализуются в ОС в виде программных модулей.

Компьютер с установленной на нем ОС взаимодействует с другим компьютером по протоколам всех 7-ми уровней модели OSI. Это взаимодействие компьютеры осуществляют через различные коммуникационные устройства сети. В зависимости от типа устройства оно может работать на разных уровнях модели OSI. Например, повторитель выполняет свои функции только на физическом уровне, а маршрутизатор - на физическом, канальном и сетевом (иногда используется и транспортный).

Под шлюзами в настоящее время подразумеваются аппаратно-программные или чисто программные комплексы, которые располагаются на границе двух сетей интерсети и осуществляется преобразование используемых в них протоколов на всех 7-ми уровнях модели OSI. Например, брандмауэры, прокси – серверы, и т.д.

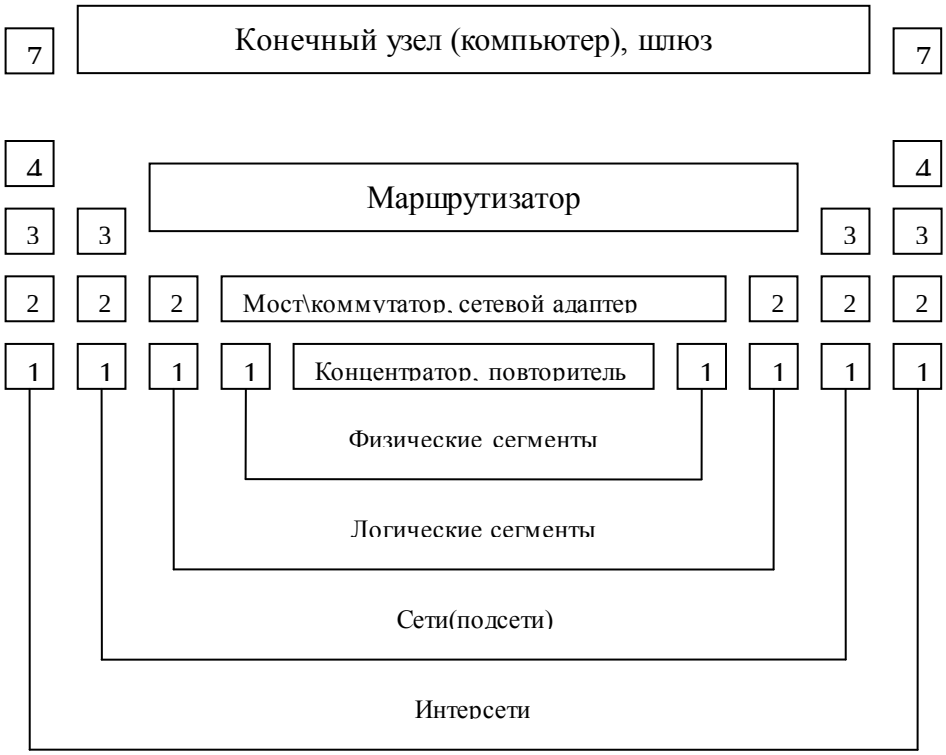


Рис. 1.14. Соответствие функций сетевых устройств уровням модели OSI

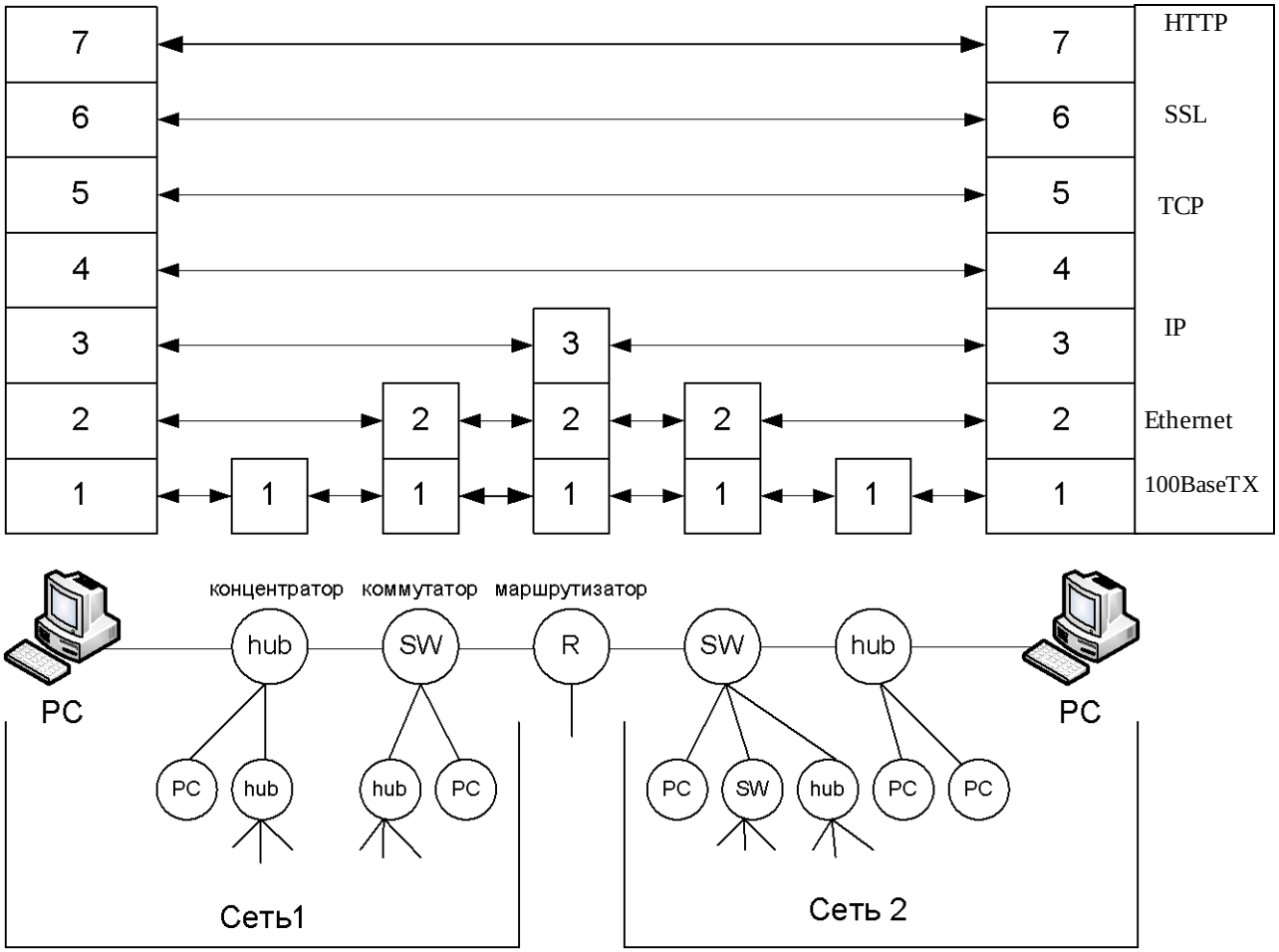


Рис. 1.15. Уровни модели OSI, поддерживаемые разными сетевыми устройствами

1.6.2. Источники стандартов

Работу по стандартизации выполняет большое количество организаций, и в соответствии с этим различают :

1. Международные стандарты (ISO - международная организация по стандартизации, ITU - международный союз электросвязи) ;

2. Национальные стандарты - американский национальный институт стандартов ANSI,

Национальный центр компьютерной безопасности Министерства обороны США NCSC (например, стандарты безопасности для ОС).

3. Стандарты специальных комитетов и объединения различных фирм. Например, ATM FORUM, Fast Ethernet Alliance и т.д.

4. Фирменные стандарты. Например, стек протоков DECnet фирмы Digital Equipment для компьютеров DEC.

1.7. Основные характеристики компьютерных сетей

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

Существует два основных подхода к обеспечению качества работы сети. Первый состоит в том, что сеть гарантирует пользователю соблюдение некоторой числовой величины показателя качества обслуживания. Например, сети frame relay и ATM могут гарантировать пользователю заданный уровень пропускной способности. При втором подходе - "с максимальными усилиями" (best effort) - сеть старается по возможности более качественно обслужить пользователя, но при этом ничего не гарантирует.

1. Время реакции сети - время от запроса до получения ответа. Оно включает:

- формирование запроса;
- время подготовки запроса на клиенте;
- время передачи через сегменты;
- время передачи через коммутационное оборудование;
- время обработки сервером;
- время на обратную передачу;
- время обработки ответа клиентом.

2. Пропускная способность сети - объём передаваемых данных в единицу времени.

Пропускная способность характеризует передачу данных между узлами и коммутационным оборудованием. Принято различать:

- общую пропускную способность;
- среднюю пропускную способность;
- максимальную пропускную способность;
- минимальную пропускную способность.

3. Задержка передачи данных в сети - интервал времени между поступлением сообщения на вход сетевого устройства и появлением этого сообщения на выходе устройства.

4. Коэффициент готовности сети - доля времени, в течении которого сеть может быть использована.

5. Безопасность сети - обеспечение защиты от несанкционированного доступа.

6. Отказоустойчивость сети - способность работать в условиях отказа некоторых её элементов.

7. Расширяемость сети - возможность достаточно легко наращивать компоненты сети.

8. Масштабируемость сети - возможность увеличивать в широких пределах количество и протяженность связи без ухудшения производительности сети.

9. Прозрачность сети - способность сети скрывать от пользователя своё внутреннее устройство.

10. Управляемость сети - возможность централизовано собирать информацию и управлять узлами сети (работой сети в целом).

11. Совместимость сети - способность сети включать в себя разное аппаратное и программное обеспечение.

2. Передача данных на физическом уровне

2.1. Линии связи

Линия связи состоит в общем случае из физической среды, по которой передаются информационные сигналы, аппаратуры передачи данных и промежуточной аппаратуры. Синонимом термина линия связи (line) является термин канал связи (channel).

В локальных сетях промежуточная аппаратура не используется. На линиях связи большой протяженности (глобальные сети) промежуточная аппаратура решает две основные задачи:

1) усиление (повышение мощности) и регенерации (восстановление формы и длительности) сигналов;

2) создание между двумя точками сети непрерывного составного канала из отрезков физической среды с усилителями и регенераторами.

Физическая среда передачи данных может представлять собой кабель (медный или оптоволоконный), земную атмосферу или космическое пространство, через которые распространяются информационные сигналы. В современных компьютерных (и телекоммуникационных) сетях информация передается с помощью электрического тока или напряжения, радиосигналов, световых сигналов, т.е. электромагнитных колебаний разной природы и частоты.

2.2. Физические аспекты передачи сигналов

Из теории гармонического анализа известно, что любой сигнал можно представить в виде суммы бесконечного числа синусоидальных колебаний разной амплитуды и частоты. Каждая составляющая синусоида называется также *гармоникой*, а набор всех гармоник называют спектральным разложением исходного сигнала или *спектром сигнала* (рис.2.1.).

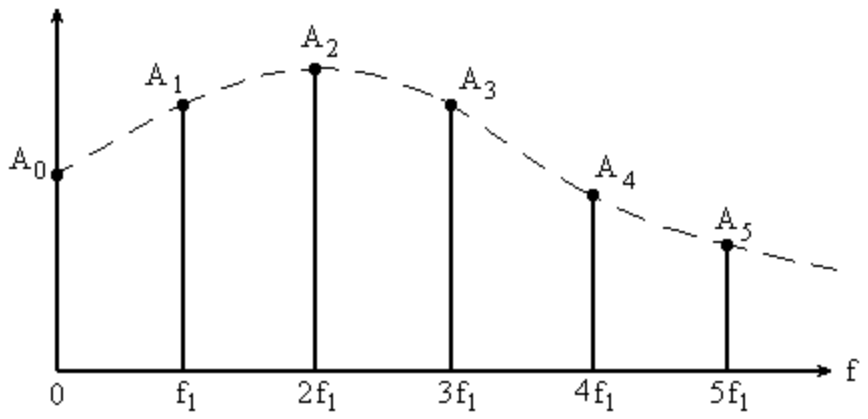


Рис. 2.1. Спектр сигнала

Сигналы, передаваемые в компьютерной сети, являются *периодическими*. Некоторые гармоники в спектрах конкретных периодических сигналов могут отсутствовать, т.е. их амплитуды будут равны нулю. Но главное, что в отличие от непериодических сигналов в периодических частоты гармоник находятся в простых кратных соотношениях. Например, несколько первых гармоник периодического сигнала, состоящего из последовательности импульсов длительностью в T/2, показаны на рис.2.2. Чем круче фронты прямоугольных импульсов, тем больше высокочастотных гармоник необходимо учитывать для воспроизведения их формы.

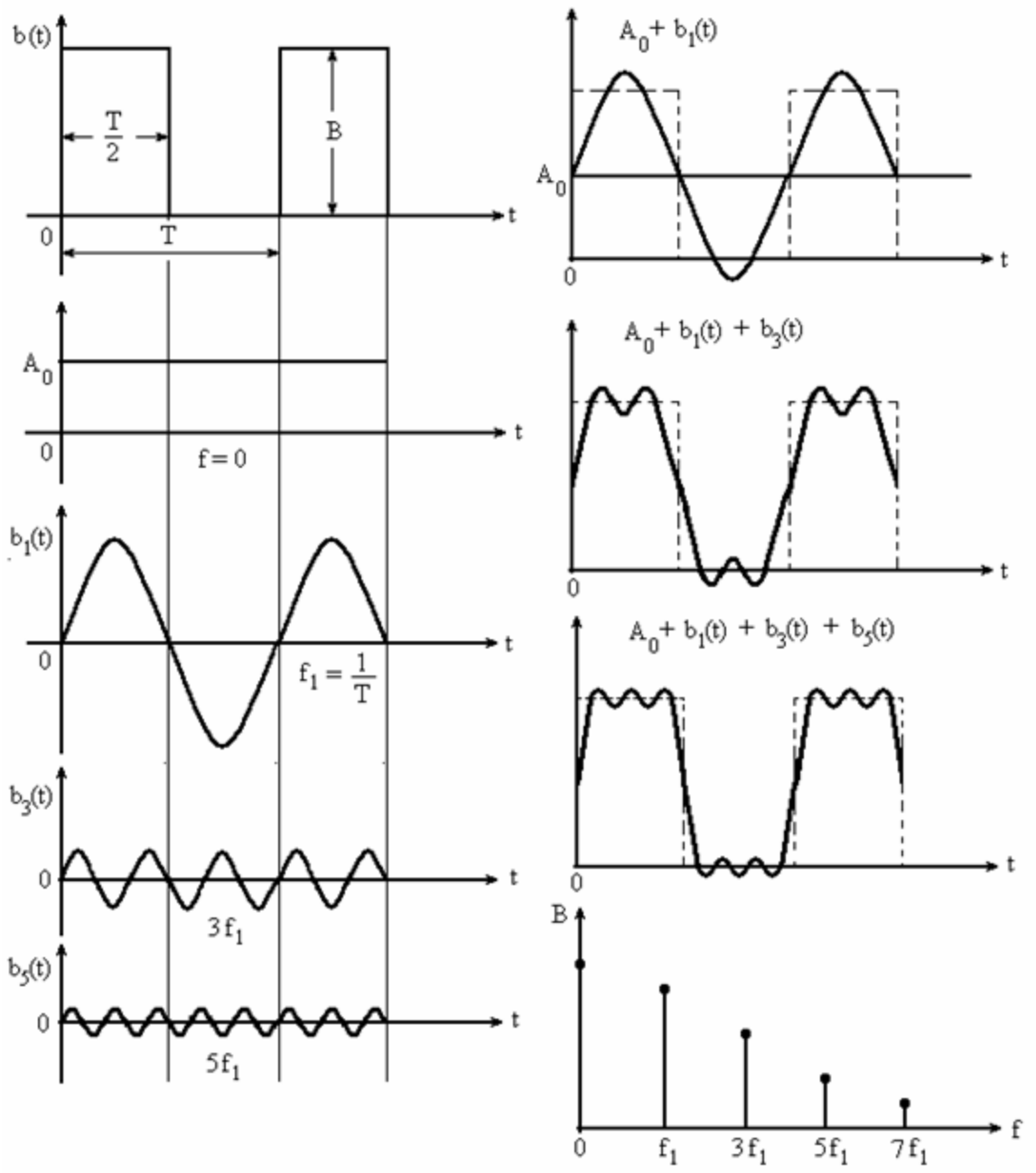


Рис. 2.2. Гармоники спектра сигналов

Сигнал, передаваемый по линии связи, постепенно затухает и претерпевает искажения. Вследствие этого на приемном конце линии он может плохо распознаваться.

Причиной этих явлений является не идеальность физических параметров среды передачи данных (комплексное погонное сопротивление линии), а также внешние помехи.

Для разных гармоник передаваемого сигнала, линия будет обладать разным полным сопротивлением, т.е. синусоидальные составляющие разной частоты будут затухать неодинаково (неравномерность АЧХ) и иметь разные фазовые сдвиги относительно друг друга (нелинейность ФЧХ). Все это ведет к искажению формы сигналов.

Кроме искажений сигналов, вносимых внутренним сопротивлением линии связи, существуют и внешние помехи, которые вносят свой вклад в искажение формы сигналов на выходе линии. Эти помехи создают различные электрические двигатели, электронные устройства, атмосферные явления и т.д.

Несмотря на защитные меры, предпринимаемые разработчиками кабелей, и наличие усилительно-коммутирующей аппаратуры, полностью компенсировать влияние внешних помех не удается. Кроме внешних помех в кабеле существуют и внутренние помехи - так называемые наводки одной пары проводников на другую.

Качество исходных сигналов (крутизна фронтов, общая форма импульсов) зависит от качества передатчика, генерирующего сигналы в линию связи.

2.3. Основные характеристики линий связи

Затухание показывает, насколько уменьшается мощность эталонного синусоидального сигнала на выходе линии связи по отношению к мощности сигнала на входе этой линии. Затухание А обычно измеряется в децибелах, дБ (decibel, dB) и Вычисляется по следующей формуле;

$A = 10 \cdot \lg(P_{вых}/P_{вх})$.

Здесь $P_{вых}$ – мощность сигнала на выходе линии, $P_{вх}$ – мощность сигнала на входе линии.

Поскольку затухание связано с внутренним сопротивлением линии связи, то его значение возрастает с увеличением протяженности линии при отсутствии промежуточных усилителей. По этой же причине для пассивной линии значение затухания – всегда **отрицательная величина**. Для удобства часто оперируют с абсолютными величинами затухания.

Затухание измеряется для основной частоты передаваемого сигнала, гармоника которой вносит наибольший вклад в его амплитуду и мощность. Например, кабель на витой паре категории 5, на котором работают практически все технологии локальных сетей, характеризуется затуханием не ниже 23,6 дБ для частоты 100 МГц при длине кабеля 100м.

Оптический кабель имеет существенно более низкие величины затухания, обычно в диапазоне от 0,2 до 3 дБ при длине кабеля в 1000 м для используемых длин волн (850 нм, 1310 нм, 1550 нм). Причем, с увеличением длины волны затухание уменьшается (для длины волны 1550 нм – A~0,2 dB).

В качестве характеристики мощности передатчика используется абсолютный уровень мощности сигнала в ваттах, относительный уровень мощности (на входе и выходе линии), которое, как и затухание сигнала, измеряется в децибелах. Часто удобно пользоваться другой абсолютной единицей мощности – опорной мощностью:

Ро =10·lg(Р/1мВт) [дБм].

Здесь Р – абсолютная мощность сигнала в милливаттах, а дБм (dBm) – единица измерения уровня мощности (децибел на 1 мВт).

Для нормального распознавания информации приемником необходимо, чтобы минимальная опорная мощность передатчика Ровых с учетом затухания сигнала в линии превосходила *порог чувствительности приемника* (минимально допустимую опорную мощность сигнала на его входе) Ровх: Ровых – А > Ровх.

Полоса пропускания – одна из важнейших характеристика линии связи. Теоретически наиболее точными характеристиками линии связи являются АЧХ и ФЧХ (амплитудно- и фазо-частотная характеристика), которые отражают значения Авых/Авх и ФUвых/ФUвх для всех частот диапазона [0, fmax], которые могут передаваться по линии, т. е. входить в состав спектров передаваемых сигналов. Ввиду сложности измерения этих характеристик на практике вместо них используется такая характеристика как полоса пропускания. Полоса пропускания определяет диапазон частот, которые передаются линией связи с приемлемым затуханием. Часто граничными частотами считаются частоты, на которых мощность выходного сигнала уменьшается в два раза по отношению к входному, что соответствует затуханию в -3дБ (рис.2.3).

Рис. 2.3. Полоса пропускания

Важным параметром медных кабелей является волновое сопротивление линии – это комплексное сопротивление, которое встречает электромагнитная волна определенной частоты при распространении вдоль однородной линии. Волновое сопротивление измеряется в омах и не зависит от длины линии. В линии, длина которой превышает длину распространяющихся в ней колебаний, возникают прямые и отраженные волны. Чтобы энергия сигнала полностью поглощалась приемником, и не возникало отраженных волн, выполняется согласование линии, т.е. выходное сопротивление передатчика и приемника должно быть равно волновому сопротивлению линии. Согласование обычно выполняется с помощью линейных трансформаторов (от слов «линия связи»). Следует отметить, что эти трансформаторы не пропускают постоянную составляющую и близкие к ней низкочастотные гармоники сигнала.

Итак, перед передачей по линии связи сигналы кодируются и формируются. Проходя по линии связи, сигналы претерпевают затухание. Неравномерность АЧХ и нелинейность ФЧХ линии из-за комплексного погонного сопротивления линии, а также внешние шумы и, возможно, перекрестные помехи от близко расположенных проводников приводят к искажениям формы сигнала.

Передаваемый по линии связи сигнал будет правильно распознан приемником, если полоса пропускания линии будет перекрывать те гармоники спектра сигнала, которые вносят основной вклад в мощность и форму этого сигнала. Например, для качественной передачи сигнала, изображенного на рисунке 2.2, необходима линия связи с полосой от ~0Гц до >= $7f_1$. Гармониками с $f > 7f_1$, можно пренебречь из-за их малого вклада в результирующий сигнал.

Помехоустойчивость линии определяет ее способность уменьшать уровень помех, создаваемых во внешней среде или на внутренних проводниках самого кабеля. Помехоустойчивость линии зависит от типа используемой физической среды, а также от экранирующих и подавляющих помехи средств самой линии. Наименее помехоустойчивым являются радиолинии, хорошей устойчивостью обладают кабельные линии и отличной – волоконно-оптические линии, малочувствительные к внешнему электромагнитному излучению. Обычно для уменьшения помех, появляющихся из-за внешних электромагнитных полей, проводники экранируют и/или скручивают.

Параметры, характеризующие перекрестные помехи (одного проводника на другой внутри кабеля), обычно применяются для кабелей, которые состоят из нескольких витых пар, для других типов кабелей (коаксиальные и оптоволоконные) при качественном монтаже эти наводки не существенны.

Пропускная способность линии характеризует максимально возможную скорость передачи данных по линии данного типа. Это также одна из важнейших характеристик линии связи. Измеряется пропускная способность в бит/сек, поскольку данные передаются по линии последовательно (побитово). Такие единицы измерения, как килобит, мегабит или гигабит, в сетевых технологиях строго соответствуют степеням 10 (то есть килобит - это 1000 бит, а мегабит – это 1000000 бит), как это принято во всех отраслях науки и техники, а не близким к этим числам степеням 2, как это принято в программировании, где приставка "кило" равна $2^{10} = 1024$, а "мега" - $2^{20} = 1048576$.

Максимально возможную пропускную способность линии определённого типа определяют формула Шеннона и формула Найквиста.

Формула Шеннона учитывает влияние соотношения сигнал/шум в линии:

$$C = F \cdot \log_2 (1 + P_c/P_ш).$$

Здесь C – максимальная пропускная способность линии в битах в секунду, F - ширина полосы пропускная линии в герцах, P_c – мощность сигнала, $P_ш$ – мощность шума.

Из соотношения видно, что повысить пропускную способность линии можно за счет увеличения мощности передатчика или же уменьшения мощности шума (помех) на линии связи. На практике изменение этих параметров сверх определенных значений ведет к значительному повышению сложности и стоимости аппаратуры. К тому же,

например, при достаточно типичном исходном отношении мощности сигнала к мощности шума в 100 раз повышение мощности передатчика в два раза даст только 15% увеличения пропускной способности линии (логарифмическая зависимость).

Близкой по сути, к формуле Шеннона является *формула Найквиста*, которая также определяет максимально возможную пропускную способность линии связи, но без учета влияния шумов, а с учетом влияния метода кодирования передаваемого сигнала:

$C = 2F \cdot \log_2 M$, где M – количество различимых состояний информационного параметра.

Для периодического синусоидального сигнала информационными параметрами могут быть амплитуда, частота и фаза, для последовательности прямоугольных импульсов – изменение знака потенциала. Периодический сигнал, параметры которого изменяются с целью наложения информации, называется *несущим сигналом*. Способ изменения параметров в соответствии с передаваемой информацией называется *методом кодирования*.

Скорость изменения информационного параметра (одного или сразу нескольких) несущего периодического сигнала измеряется в *бодах* (*baud*). Один бод равен одному изменению информационного параметра в секунду. Период времени между соседними изменениями информационного параметра называется *тактом работы передатчика*. Скорость передачи в битах в секунду в общем случае не совпадает со скоростью в бодах. Она может быть как выше, так и ниже скорости в бодах. Это соотношение зависит от способа кодирования информации. Рассмотрим примеры. Если у периодического сигнала будет изменяться один информационный параметр, который может иметь 4 состояния (например, 4 значения амплитуды сигнала), то одному боду будет соответствовать 2 бита информации – $2^2 = 4$. Если один бит будет кодироваться четырьмя последовательными изменениями амплитуды (для повышения надежности передачи), то одному биту будет соответствовать 4бода. В первом случае за 1 такт работы передатчика будет передано 2 бита информации, а во втором случае за 4 такта – 1бит.

Хотя формула Найквиста явно не учитывает наличие шума, косвенно его влияние отражается в выборе количества состояний информационного параметра. С увеличением количества состояний сигнала соотношение $P_c/P_ш$ снижается.

Формулы Шеннона и Найквиста определяют максимально возможную скорость передачи данных по линии связи с полосой пропускания F. *Конкретную скорость* (меньше максимально допустимой), с которой передатчик передает данные по линии связи, можно определить как:

$C_п = f_п \cdot \log_2 M$, где $f_п$, – тактовая частота передатчика.

То есть, при выбранном способе кодирования скорость передачи данных по линии связи будет тем больше, чем выше частота несущего периодического сигнала (тем больше бод, а значит, и бит в секунду будет передаваться по линии).

Если сопоставить эту формулу с формулой Шеннона, то можно видеть ограничения значений $f_п$ и M. С ростом тактовой частоты передатчика спектр результирующего сигнала будет расширяться в область ВЧ (см. рис. 2.2, где f1=1/T, а T

– такт работы передатчика). А значит, для качественной передачи такого сигнала нужна линия связи с более широкой полосой пропускания F. Максимальное значение M, как уже отмечалось, ограничено соотношением сигнал/шум в линии связи.

Таким образом, скорость возможной передачи данных по линии связи зависит от её внутренних параметров (полосы пропускания), внешних параметров (уровня помех и степени их ослабления) и выбранных параметров (способа кодирования данных, тактовой частоты и мощности передатчика). **Выбранные параметры задаются протоколом физического уровня.**

То есть, если для линии связи задан протокол физического уровня (с учетом её полосы пропуская и уровня помех), то именно он и будет определять максимальную скорость передачи данных по линии. Поэтому часто, когда говорят о пропускной способности канала, имеют в виду скорость, ограниченную протоколом, а не физическими возможностями самой линии.

2.4. Типы линий связи

В компьютерных сетях применяются кабели, удовлетворяющие определенным стандартам. Современные стандарты определяют характеристики не только отдельного кабеля, но и полного набора элементов, необходимого для создания кабельного соединения (шнуры, разъемы...)

В настоящее время наиболее употребляемыми являются такие стандарты:

- американский EIA/TIA-568A
- международный ISO/IEC-11801
- европейский EN5011173
- фирменные стандарты IBM

Стандарты определены для трех типов кабеля:

- на основе экранированной (Shielded Twisted Pair - STP) и неэкранированной (Unshielded Twisted Pair - UTP) медной витой пары
- медного коаксиального
- оптоволоконного

2.4.1. Кабели на витой паре

Скрученная пара покрытых изоляцией медных проводников. Четыре пары таких проводников покрываются общей защитной оболочкой, образуя кабель (рис.2.4). В случае экранированной витой поры между проводниками и защитной оболочкой располагается слой электромагнитной изоляции, в качестве которой чаще всего применяется проводящая медная оплетка.

Скрутка проводников снижает влияние внешних помех и взаимных наводок соседних пар проводов на полезный сигнал. Кабель на основе неэкранированной витой пары в зависимости от электрических и механических характеристик делится на пять категорий. Наиболее употребляемыми являются:

- категория 3 - для передачи голоса и компьютерных данных

- категория 5 - для поддержания высокоскоростных протоколов компьютерных данных, используется в скоростных технологиях, таких как: FDDI, Fast и Gigabit Ethernet

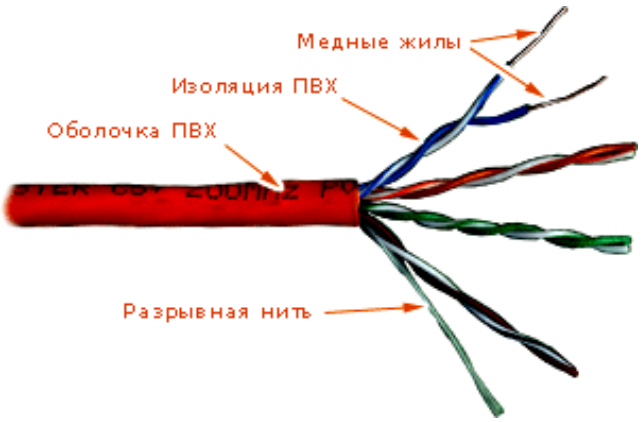


Рис. 2.4. Кабель - витая пара

Кабели на основе экранированной витой пары хорошо защищают передаваемый сигнал от внешних помех, а пользователей – от излучений. Они существенно дороже и сложнее в прокладке по сравнению с неэкранированными. Используются только для передачи данных. Основным стандартом является фирменный стандарт IBM. В нем определено девять типов кабеля, из них основными являются кабель типа 1 (Type1). Кабели на витой паре обладают наилучшим соотношением цена/качество.

2.4.2. Коаксиальные кабели

Состоят из проводящей медной жилы, покрытой слоем диэлектрической изоляции и заключенной в медный экран. Снаружи находится слой защитной изоляции. Экран одновременно играет роль второго проводника сигнала (рис.2.5). Существует много типов кабеля, которые отличаются характеристиками и областями применения (для локальных сетей, для глобальных сетей, для телевидения).

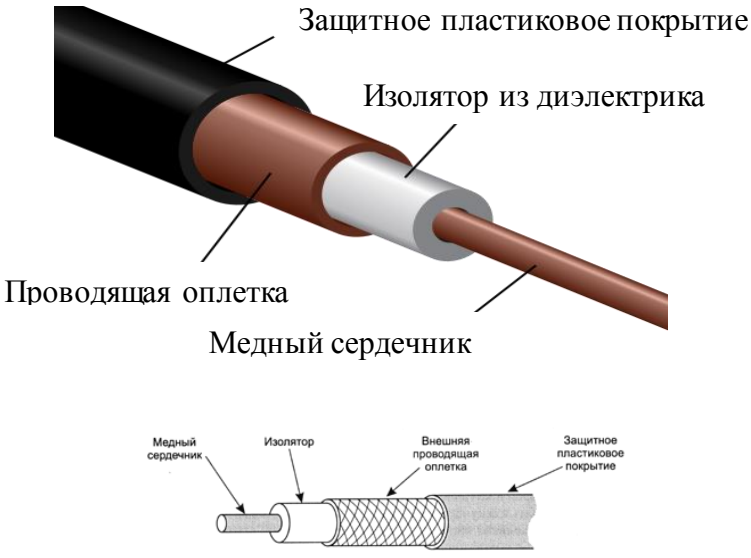


Рис. 2.5. Коаксиальный кабель

В локальных сетях используется "толстый" кабель и несколько разновидностей "тонкого" кабеля – в основном в технологии Ethernet. "Тонкий" кабель обладает худшими электрическими и механическими характеристиками, но дешевле и за счет гибкости удобнее в монтаже. К недостаткам кабеля следует отнести то, что он не допускает сильных изгибов и сдавливания и из-за большого диаметра занимает много места в каналах и коробах для разводки кабеля.

Коаксиальный кабель имеет более широкую полосу пропускания, чем витая пара, но и более высокую стоимость.

2.4.3. Волоконно-оптический кабель

Волоконно-оптический кабель обладает наилучшими электромеханическими характеристиками и помехозащищенностью. Это наиболее перспективный вид передающей среды во всех типах телекоммуникаций. Однако монтажные работы по его прокладки сложнее и дороже, чем для других типов кабеля.

Структура волоконно-оптического кабеля показана на рис.2.6.

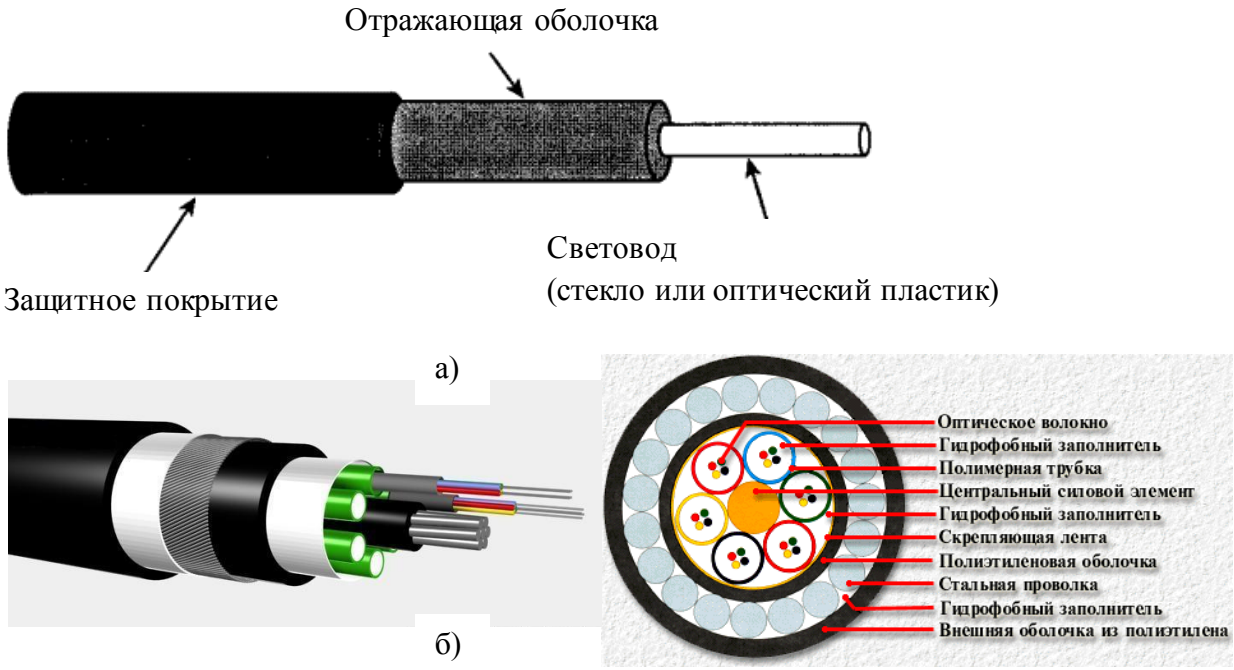


Рис. 2.6. Волоконно-оптический кабель: а) структура одножильного кабеля; б) структура многожильного (магистрального) кабеля

Волоконно-оптические кабели делятся на:

- одномодовые;
- многомодовые.

Модой называется угол отражения световых лучей от отражающей оболочки (стеклянной оболочки с меньшими показателем преломления, чем у сердечника).

В одномодовом кабеле используется центральный сердечник – световод с диаметром, соизмеримым с длиной света (5-10 микрон). Все лучи распространяются вдоль оптической оси световода и почти не отражаются оболочкой.

Полоса пропускания такого кабеля – до нескольких сотен ГГц/км. Кабель используются для передачи данных на расстояние в несколько сотен километров. Технологический процесс сложный и дорогой. В такое волокно трудно направить пучок света без потери значительной части энергии.

Многомодовые кабели имеют диаметр сердечника намного больше длины волны. По нему одновременно распространяется большое число лучей, которые отражаются под разными углами, но несут один сигнал (рис.2.7).

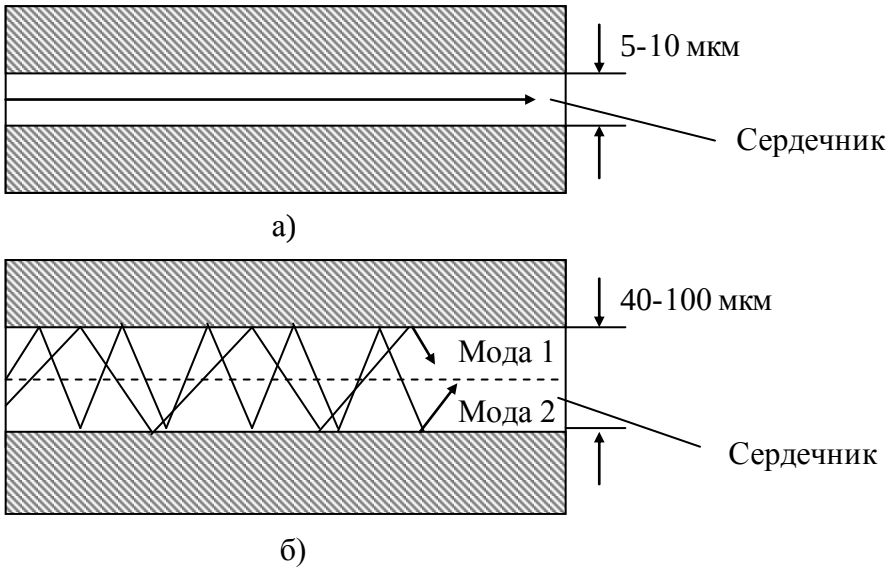


Рис.2.7. Распространение светового сигнала: а) в одномодовом кабеле, б) в многомодовом кабеле

Многомодовые кабели проще в изготовлении и дешевле одномодовых, но имеют более узкую полоску пропускания из-за потерь энергии на отражениях лучей и интерференции разных мод. Последнее означает, что луч одного сигнала, распространяющийся вдоль оси сердечника, может догнать лучи предыдущего сигнала, отражающиеся под острыми углами, наложиться на них и исказить предыдущий сигнал. По этим причинам многомодовые кабели используются для передачи данных на меньшие расстояния (до 300-2000 м) и на скоростях не более 1 Гбит/с.

В качестве источников света используются:

- для многомодовых кабелей – светодиоды;
- для одномодовых – для концентрации пучка полупроводниковые лазеры (лазерные диоды).

Быстродействие лазерных диодов позволяет модулировать световой поток с частотой 10ГГц и более, а также имеют отличные электромагнитные и механические характеристики, недостаток их состоит в сложности и высокой стоимости монтажных работ.

2.4.4. Радиоканалы наземной и спутниковой связи

В компьютерных сетях применяется радиосвязь в диапазонах УКВ и СВЧ. В диапазоне УКВ электромагнитная волна распространяется, многократно отражаясь от ионосферы и огибая поверхность Земли. При этом скорости обеспечиваются небольшие – 1-2Мбит/сек. Расстояние из-за затухания сигнала также небольшое – порядка нескольких сотен метров.

В диапазоне СВЧ (свыше 30МГц) сигналы уже не отражаются от ионосферы Земли, поэтому требуется либо прямая видимость между передатчиком и приемником, либо наличие каналов радиорелейной и спутниковой связи. Спутниковые и радиорелейные связи используются в глобальных сетях (где нельзя проложить кабель) и для мобильных пользователей. Спутниковые каналы, хотя и обладают в целом большой пропускной способностью, но пользователям предоставляют скорости в пределах 360-380 кбит/с. Основной недостаток этих каналов – большие задержки передачи сигналов. При соблюдении условий прямой видимости в локальных сетях, сотовых телефонных сетях и стационарных каналах доступа типа «точка – точка» распространен так называемый микроволновой диапазон (свыше 300МГц). Пропускная способность радио-канала в современных локальных сетях может достигать 300 Мбит/сек при расстоянии около 100м, в районных сетях –300 Мбит/сек при расстоянии в несколько км.

В локальных сетях также используются инфракрасные лучи. Инфракрасная технология в ЛВС обеспечивает скорости до 16 Мбит/сек при дальности связи порядка 30 м. Для распространения инфракрасных лучей необходима прямая видимость между приемником и передатчиком. Распространение инфракрасных лучей сильно зависит от погодных условий (туман, дождь, снег). Однако существуют коммерческие системы, размещаемые на крышах зданий, которые обеспечивают скорость передачи данных до 155Мбит/сек на расстояние до 3-15км, а также экспериментальные системы, позволяющие на тех же расстояниях достигать скоростей до 10Гбит/сек.

Пока наиболее распространенными радио-сетями являются мобильные телефонные сети. Компьютерные сети в основном представлены сетями радио Ethernet (WI-FI) и радио-каналами «точка-точка» (WI-MAX). Скорости этих технологий уже сопоставимы со скоростями проводных локальных сетей. В мобильных сетях нового, так называемого третьего поколения (3d generation, 3G) предусматривается одновременная передача голоса и компьютерных данных со скоростью 2Мбит/сек, при этом каждый вид трафика считается одинаково важным.

Главной проблемой для каналов беспроводной связи являются помехи от различных внешних источников излучения, а также влияние природных условий (снег, туман, солнечные бури), к которым особенно чувствительны микроволновой и световой диапазоны. Поэтому в беспроводных системах связи применяются различные методы и средства, направленные на снижение влияния помех.

2.5. Виды кодирования сигналов

Кодирование на физическом уровне можно разделить на физическое и логическое.

Выбор способа представления дискретной информации в виде сигналов, подаваемых на линию связи, называется *физическим*, или *линейным* (от слова линия) *кодированием*. Способ кодирования данных влияет на спектр передаваемых сигналов и, следовательно, на пропускную способность линии связи.

Логическим называется **кодирование**, которое выполняется до физического и подразумевает замену битов исходной информации новой последовательностью битов, несущей ту же информацию, но обладающей дополнительными свойствами. К ним относятся методы, повышающие способность приемной стороны обнаруживать ошибки в принятых данных. Например, каждый байт исходной информации дополняется одним битом четности — этот метод часто применяется при передаче данных с помощью модемов. Возможно, также исправлять некоторые единичные ошибки передачи, например, при использовании метода прямой коррекции ошибок (FEC), кодов Хемминга, решетчатых кодов. Другим примером являются методы, применяемые для улучшения спектра сигнала при последующем физическом кодировании (например, исключение длинных последовательностей нулей или единиц). Еще одним примером логического кодирования может служить шифрование данных, обеспечивающее их конфиденциальность при передаче через общедоступные каналы связи.

Большинство способов **физического кодирования** используют изменение какого-либо параметра периодического сигнала – частоты, амплитуды и фазы синусоиды или же знак потенциала последовательности импульсов. Периодический сигнал, параметры которого изменяются, называют *несущим сигналом* (или *несущей частотой*, если в качестве такого сигнала используется синусоида).

При передаче дискретных данных по каналам связи применяются два основных типа физического кодирования — на основе синусоидального несущего сигнала и на основе несущего сигнала, представляющего собой последовательность прямоугольных импульсов. Первый способ часто называется также *модуляцией*, или *аналоговой модуляцией*, подчеркивая тот факт что, кодирование осуществляется за счет изменения параметров (модуляции) аналогового сигнала.

Второй способ обычно называют *цифровым кодированием.* Спектр сигнала, состоящего из последовательности прямоугольных импульсов, получается весьма широким. Применение синусоиды приводит к спектру гораздо меньшей ширины при той же скорости передачи данных. Однако для аналоговой модуляции требуется более сложная и дорогая аппаратура, чем для цифрового кодирования.

С другой стороны, исходный *модулирующий сигнал* может быть как дискретным, так и непрерывным. В настоящее время все чаще данные, изначально имеющие непрерывную форму — речь, телевизионное изображение, — передаются по каналам связи в дискретном виде, то есть в виде последовательности единиц и нулей. Процесс представления аналоговой информации в дискретной форме называется *дискретизацией,* а иногда дискретной модуляцией. Вообще термины «модуляция» и «кодирование» часто используют как синонимы. Цифровая форма представления данных повышает качество передачи, так как при этом могут применяться эффективные

методы обнаружения и исправления ошибок, недоступные для систем аналоговой передачи.

2.5.2. Дискретизация аналоговых сигналов

Аналоговая информация также может передаваться по телекоммуникационным сетям в цифровой форме. Это повышает качество передачи, так как при этом могут применяться эффективные методы обнаружения и исправления ошибок, недоступные для систем аналоговой передачи. Рассмотрим принципы дискретной модуляции на примере *импульсно-кодовой модуляции, ИКМ (Pulse Amplitude Modulation, PAM),* которая широко применяется в цифровой телефонии.

Амплитуда исходной непрерывной функции измеряется с заданным периодом — за счет этого происходит дискретизация по времени. Затем каждый замер представляется в виде двоичного числа определенной разрядности, что означает дискретизацию по значениям функции — непрерывное множество возможных значений амплитуды заменяется дискретным множеством ее значений. Устройство, которое выполняет подобную функцию, называется *аналого-цифровым преобразователем* (*АЦП*). После этого замеры передаются по каналам связи в виде последовательности единиц и нулей

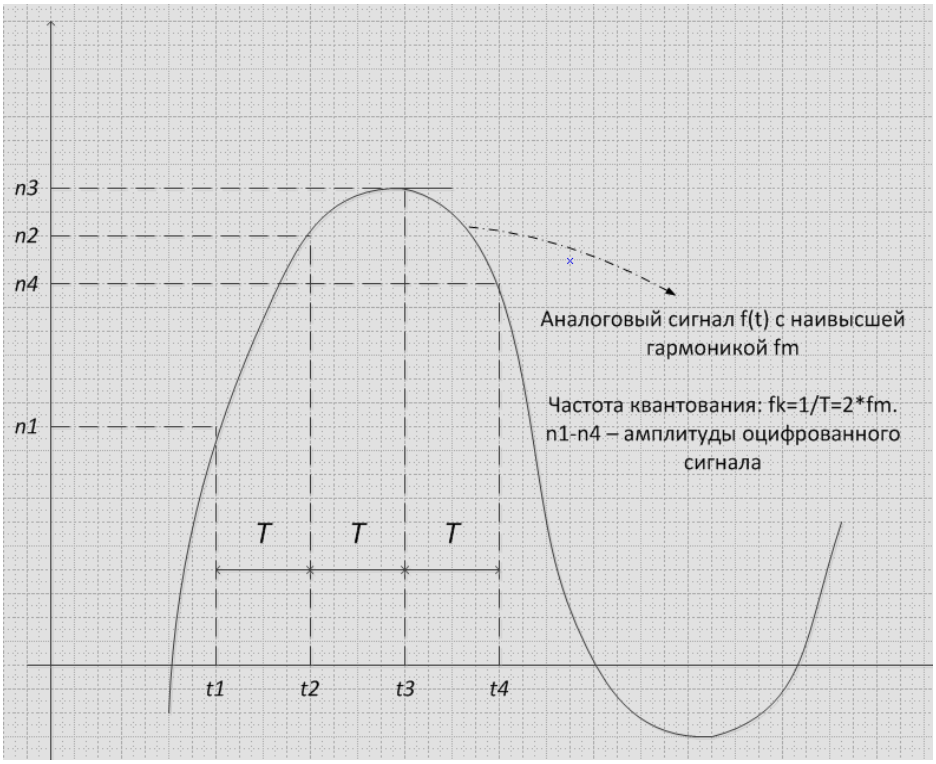


Рис. 2.9. Дискретная модуляция непрерывного процесса

На приемной стороне линии коды преобразуются в исходную последовательность битов, а специальная аппаратура, называемая *цифро-аналоговым преобразователем (ЦАП)*, производит демодуляцию оцифрованных амплитуд непрерывного сигнала, восстанавливая исходную непрерывную функцию времени.

Дискретная модуляции основана на *теории отображения Найквиста-Котельникова.* В соответствии с этой теорией аналоговая непрерывная функция,

переданная в виде последовательности ее дискретных по времени значений, может быть точно восстановлена, если частота дискретизации была в два или более раз выше, чем частота самой высокой гармоники спектра исходной функции.

Если это условие не соблюдается, то восстановленная функция будет существенно отличаться от исходной.

Для качественной передачи голоса в методе ИКМ используется частота квантования амплитуды звуковых колебаний в 8000 Гц. Это связано с тем, что в аналоговой телефонии для передачи голоса был выбран диапазон от 300 до 3400 Гц, который достаточно качественно передает все основные гармоники собеседников. В соответствии с теоремой Найквиста – Котельникова для качественной передачи голоса достаточно выбрать частоту дискретизации, в два раза превышающую самую высокую гармонику непрерывною сигнала, то есть 2*3400=6800Гц. Выбранная в действительности частота дискретизации 8000 Гц обеспечивает некоторый запас качества. В методе ИКМ обычно используется 7 или 8 бит кода для представления амплитуды одного замера. Следовательно, для передачи одного голосового канала при использовании 8 – битового кода:

8000 * 8 = 64000 бит/с или 64 кбит/с.

Это стандартный цифровой канал, который также называется *элементарным каналом цифровых телефонных сетей.*

Существуют и другие методы дискретной модуляции, позволяющие представить замеры голоса в более компактной форме, например в виде последовательности 4-битных или 2-бигных чисел. При этом один голосовой канал требует меньшей пропускной способности, например 32 кбит/с, 16 кбит/с или еще меньше. С 1985 года применяется стандарт CCITT кодирования голоса, называемый Adaptive Differential Pulse Code Modulation (ADPCM). Коды ADPCM основаны на нахождении разностей между последовательными замерами голоса, которые затем и передаются по сети. В коде ADPCM для хранения одной разности используется 4 бит, и голос передается со скоростью 32 кбит/с. Более современный метод, Linear Predictive Coding (LPC), делает замеры исходной функции реже, но использует прогнозирование направления, в котором изменяется амплитуда сигнала. При помощи этого метода можно понизить скорость передачи голоса до 9600 бит/с.

2.5.3. Аналоговая модуляция

Основные способы аналоговой модуляции для дискретных данных показаны на рис.2.8. На диаграмме (рис 2.8, *а*) показана последовательность битов исходной информации, представленная потенциалами высокого уровня для логической единицы и потенциалом нулевого уровня для логического нуля. Такой способ кодирования называется потенциальным кодом и часто используется при передаче данных между блоками компьютера.

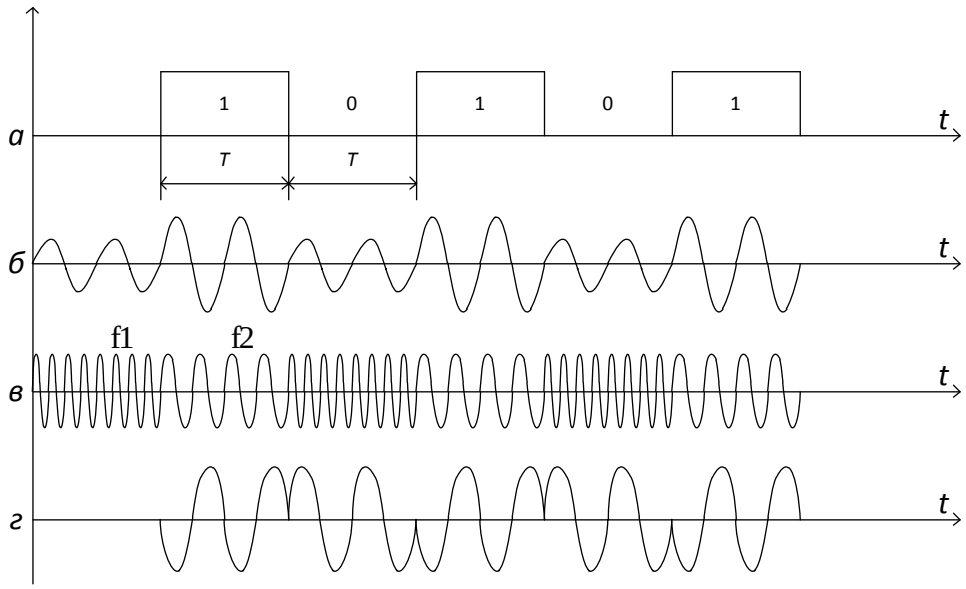


Рис. 2.8. Различные типы модуляции

При *амплитудной модуляции* ASK(Amplitude Shift Keying) для логической единицы выбирается один уровень амплитуды синусоиды несущей частоты, а для логического нуля — другой (рис. 2.8, *б*). Этот способ редко используется в чистом виде на практике из-за низкой помехоустойчивости, но часто применяется в сочетании с другим видом модуляции — фазовой модуляцией.

При *частотной модуляции* FSK(Frequency Shift Keying) значения 0 и 1 исходных данных передаются синусоидами с различной чистотой —f_0 и f_1(рис. 2.8, *в*). Этот способ модуляции не требует сложных схем в модемах и обычно применяется в низкоскоростных модемах, работающих на скоростях 300 или 1200 бит/с. При использовании только 2-х частот модуляция называется BFSK (Binary FSK). Возможно использование большего количества частот для увеличения числа бит, которые можно передать одним изменением частоты передатчика. Такая модуляция называется MFSK (Multilevel FSK).

При *фазовой модуляции* PSK(Phase Shift Keying) значениям данных 0 и 1 соответствуют сигналы одинаковой частоты, но различной фазы, например 0 и 180^0 (рис. 2.8, *г*). При использовании 2-х значений фазы модуляция называется BPSK (Binary PSK), а при использовании 4-х значений фазы (например, 0, 90, 180 и 270^0) – QPSK (Quadrature PSK).

Для повышения скорости передачи данных используют комбинированные методы модуляции. Наибольшее распространение получил метод *квадратурной амплитудной модуляции QAM* (Quadrature Amplitude Modulation), для которого характерны 4 уровня амплитуды несущей синусоиды и 8 значений фазы. Не все из возможных 32 сочетаний метода QAM используются для передачи данных. Наличие запрещенных сочетаний позволяют приемнику распознавать искажения данных, возникшие в процессе передачи.

Поскольку аналоговая модуляция обеспечивает более узкий спектр результирующею сигнала по сравнению с цифровым кодированием при той же скорости передачи исходных данных, то применяется она для передачи дискретных

данных по каналам с узкой полосой пропускания. Типичными представителями таких каналов является каналы, предоставляемые в распоряжение пользователям телефонными сетями. Устройство, которое выполняет модуляцию/демодуляцию синусоидального сигнала двоичными данными, называется *модемом*.

Помимо узкого спектра результирующею сигнала методы аналоговой модуляции обладают свойством самосинхронизации, и обеспечивают хорошее распознавание ошибок.

2.5.4. Цифровое кодирование

По методу изменения информационного параметра несущего сигнала цифровые коды делятся на:

- потенциальные
- импульсные

В потенциальных методах кодирования данные представляются уровнями потенциала сигнала, а в импульсных – либо полярностью самих импульсов, либо направлением переключения их фронтов.

Требования, предъявляемые к методам кодирования

Хороший метод, как цифрового кодирования, так и аналоговой модуляции, должен обеспечивать:

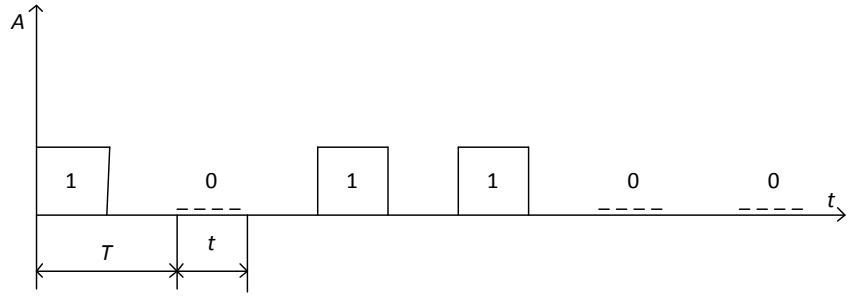
1) при одной и той же битовой скорости передачи наименьшую ширину спектра результирующего сигнала;
2) синхронизацию между передатчиком и приемником;
3) хорошую распознаваемость ошибок передачи данных (помехоустойчивость);
4) отсутствие постоянной составляющей в спектре результирующей сигнала;
5) по возможности низкую мощность передатчика и стоимость реализации.

Рассмотрим подробнее, как эти принципы обеспечиваются в методах цифрового кодирования.

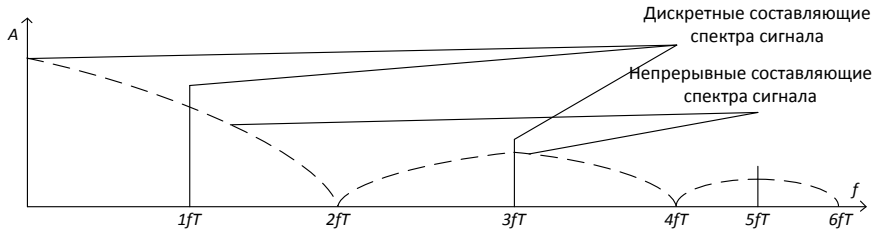
Узкий спектр результирующего сигнала позволяет обеспечить необходимую скорость передачи данных на более дешевых линиях связи, имеющих более узкую полосу пропускания.

Кроме того, нужно учесть, что реально спектр сигнала постоянно меняется в зависимости от того, какие данные передаются по линии связи. Например, передача длинной последовательности нулей или единиц в потенциальных методах кодирования сдвигает спектр в сторону низких частот, а в крайнем случае, когда передаваемые данные состоят только из единиц (или только из нулей), спектр состоит из гармоники нулевой, частоты.

Например, при передаче произвольной последовательности сигналов спектр рассматриваемого нами ранее потенциального кода (рис.2.2.) будет иметь вид, показанный на рис. 2.10.



а)



б)

Рис. 2.10. Спектр (б) потенциального кода с t_n = T/2 (а)

В спектрах ряда кодов дискретные составляющие могут отсутствовать (их амплитуда равна 0).

Синхронизация передатчика и приемника нужна для того, чтобы приемник точно знал, в какой момент времени необходимо считывать новую информацию с линии связи.

Принципиально вопрос синхронизации в компьютерных системах решается следующим образом:

- Отдельная линия, по которой передаются периодические синхросигналы. Это способ достаточно дорог, т.к. в кабеле необходимо выделять дополнительную отдельную линию, по которой данные не передаются и, кроме этого, на больших расстояниях синхросигналы могут, как опережать, так и отставать от данных. Поэтому данный способ применяется на небольшом расстоянии, например, между блоками компьютера или между компьютером и принтером.
- С помощью периодической синхронизации заранее известными кодами иди импульсами характерной формы, которые отличаются от основных данных. Применяется, в основном, в протоколах канального уровня (перед данными), но, если передается длинная последовательность данных, все равно со временем может произойти сдвиг.
- Применение *самосинхронизирующихся кодов,* сигналы которых несут для передатчика указания о том, в какой момент времени нужно осуществлять распознавание очередного бита (или нескольких битов, если код ориентирован более чем на два состояния сигнала). Любой резкий перепад сигнала — так называемый фронт — может служить хорошим указанием для синхронизации приемника с передатчиком. При использовании синусоидального несущего сигнала результирующий код обладает свойством самосинхронизации, так как

изменение амплитуды несущей частоты дает возможность приемнику определить момент появления входного кода.

Свойством хорошей помехоустойчивости и распознаваемости ошибок могут обладать коды, которые используют резко отличающиеся значения параметров изменяемого несущего сигнала. Например, большую разницу амплитуд сигналов при потенциальном кодировании. Такой сигнал будет лучше различим при воздействии искажений и помех.

Требование отсутствия постоянной составляющей в спектре сигнала возникает при его передаче по линиям связи, в которых используются согласующие трансформаторы, которые препятствуют протеканию постоянного тока между передатчиком и приемником (постоянной составляющей) и сильно подавляют НЧ–составляющие спектра сигнала.

Для борьбы с 0-вой составляющей используется переход от одноуровневого двух полярного кода (рис.2.2., 2.8.а, 2.10.а.), где «0» кодируется нулевым, «1» – высоким уровнем напряжения, к многоуровневому двух полярному, где к примеру, «0» кодируется положительным, «1» – отрицательным уровнем напряжения, а U = 0 вообще не используется. Это дает отсутствие постоянной составляющей, но только при передаче чередующихся нулей и единиц.

2.5.5. Распространенные цифровые коды

Рассмотрим несколько примеров распространенных цифровых кодов (рис. 2.11.).

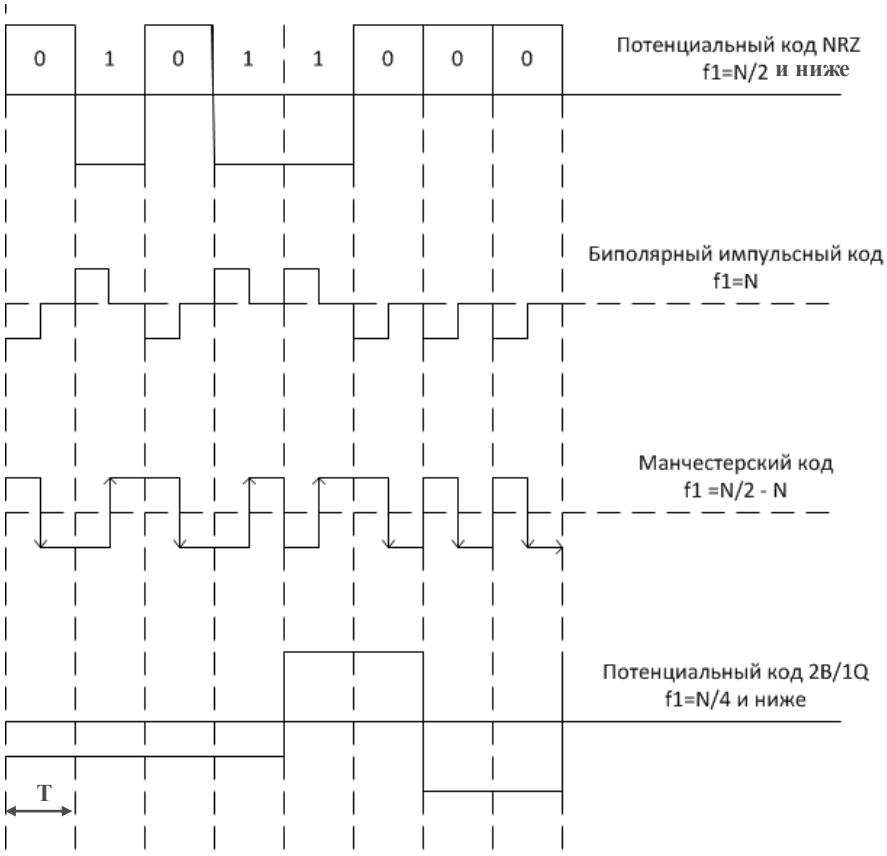


Рис. 2.11. Примеры распространенных цифровых кодов, N – исходная битовая скорость.

Потенциальный код NRZ не возвращается к 0-му уровню потенциала при передаче нескольких единиц или нулей в течение такта.

Достоинства :

- неширокий спектр;
- хорошее распознавание ошибок, т.к. использует 2 резко различающихся потенциала;
- простота реализации.

Недостатки :

- не самосинхронизирующийся;
- при длинной последовательности нулей или единиц возникают низкочастотные составляющие спектра, которые приближаются к постоянной составляющей (возникает постоянный потенциал).

В чистом виде код не используется.

Биполярный импульсный код – имеет «1»-ые импульсы одной полярности и «0»-ые импульсы другой полярности, а импульсами сигналы называются потому, что имеют длительность 1/2 такта.

Достоинства :

- четкая самосинхронизация;
- легко распознаются ошибки.

Недостатки :

- при передаче длинной последовательности единиц или нулей может появиться постоянная составляющая;
- этот код имеет самый широкий спектр т.к. при передаче каждого бита сигнал дважды изменяет свое состояние (для передачи одного бита используется 2 бода).

В чистом виде код используется редко.

Манчестерский код -наиболее популярный из импульсных кодов. Информацию несет направление переключения сигнала в середине каждого такта.

Достоинства :

- никогда не имеет постоянной составляющей;
- обладает хорошей самосинхронизацией;
- обладает хорошей способностью к распознаванию ошибок.

Недостатки :

- имеет спектр более широкий, чем у потенциальных кодов, но уже, чем у биполярного импульсного кода.

Используется в Ethernet, Token Ring.

Потенциальный код 2B/1Q – использует четыре уровня напряжения. Каждый уровень кодирует два бита исходной информации.

Достоинства :

- среди всех рассмотренных кодов имеет самый узкий спектр.

Недостатки :

- обладает самой низкой способностью распознавания ошибок;
- необходим более мощный передатчик для обеспечения помехоустойчивости сигналов, чтобы диапазон уровней сигналов превышал уровень шумов в линии связи.

Главным преимуществом потенциальных кодов перед импульсными кодами является более узких спектр результирующего сигнала, что позволяет для передачи данных с той же битовой скоростью использовать линию связи с более узкой полосой пропускания, а значит, более дешевую.

Для преодоления недостатков потенциальных кодов (появление постоянной составляющей в спектре и потеря самосинхронизации) используются методы логического кодирования, исключающие длинные последовательности единиц и нулей.

Эти методы основаны:

- на использовании избыточных кодов;
- скрэмблировании исходных данных.

В первом случае в исходные данные вводятся избыточные биты информации. Например, в коде 4B/5B, каждые исходные 4 бита данных заменяются 5-ю битами. При этом из возможных 2^5=32 комбинаций выбираются 2^4=16 комбинаций, которые не содержат подряд три «0» или «1». Помимо борьбы с постоянной составляющей и улучшения самосинхронизации, избыточные коды позволяют приемнику распознавать искаженные биты (если получен запрещенный код, значить на линии произошло искажение сигнала). Чтобы скорость передачи исходных данных не упала за счет времени потраченного на передачу избыточной информации, необходимо увеличить тактовую частоту передатчика.

Методы скремблирования заключаются в побитовом вычислении результирующего кода путем сложения (по определенному алгоритму) текущих и предыдущих битов исходного кода. Перемешивание данных выполняется с целью сделать вероятность появления «0»-лей и «1»–ц в результирующем коде примерно одинаковой. Примером такого кодирования является код 2B1Q.

При скремблировании лишние биты по линии связи не передаются, но необходимо на передающей стороне использовать дополнительно устройство – скремблер, а на приемной дескрэмблер. Это связано с дополнительными затратами.

Улучшенные логическим кодированием потенциальные коды обладают более узким спектром, чем импульсные, поэтому они находят применение в высокоскоростных технологиях, таких как FDDI, Fast Ethernet, Gigabit Ethernet.

3.Методы передачи данных на канальном уровне

Основной задачей протоколов канального уровня является организация *логического* канала между отправителем и получателем в физической среде передачи. Пакеты, сформированные протоколами верхних уровней доставляются по аппаратным (локальным) адресам. Форматы локальных адресов, как и методы доступа к среде передачи, специфичны для каждой сетевой технологии, и в общем случае для других технологий не подходят (напомним, что для всех технологий LAN формат MAC адреса одинаков). Наиболее существенные характеристики методов передачи, по которым классифицируют протоколы канального уровня, таковы:

1. Асинхронные или синхронные
2. Символьно – ориентированные или бит – ориентированные
3. С установлением соединения или дейтаграммные
4. С обнаружением искажений и потерь данных или без них
5. С восстановлением искаженных или потерянных данных или без него
6. С поддержкой сжатия данных или без нее

Следует отметить, что **характеристики 3-5 относятся не только к протоколам канального**, но и к протоколам более высоких уровней модели OSI.

3.1. Асинхронные и синхронные протоколы

Этот признак классификации относится к методу синхронизации приёмника с передатчиком при распознавании переданных данных.

Асинхронные протоколы разрабатывались для обмена данными в низкоскоростных устройствах. В этих протоколах для управления обменом данными используются не кадры, а отдельные символы. Эти символы отделяются друг от друга старт-стопными символами, которые берутся из нижней (служебной) части таблиц ASCII или EBCDIC.

Сигнал «start» извещает приемник о приходе данных и обеспечивает ему интервал времени, необходимый для организации синхронизации и приема байта данных. Позднее пользовательские данные стали оформлять в кадры, но байты в этих кадрах все равно отделяются друг от друга стартовыми и/или стоповыми сигналами.

Асинхронным такой режим называется потому, что каждый байт может быть смещен во времени относительно побитовых тактов предыдущего байта. Однако при этом можно использовать более простую и дешевую аппаратуру.

Асинхронный режим передачи:

СТАРТ	БАЙТ 1	СТОП	…	СТАРТ	БАЙТ N	СТОП

Синхронные протоколы собирают пользовательские данные в кадры, которые предваряются байтами синхронизации с заранее известными значениями (например, 01111110). Старт – стоповые сигналы между байтами отсутствуют, что ускоряет передачу пользовательских данных. При получении синхробайта приемник настраивается на распознавание начала очередного байта. Иногда для более надежной синхронизации передается несколько синхробайтов.

Синхронный режим передачи:

СИНХРОБАЙТ	БАЙТ 1	…	БАЙТ N	СИНХРОБАЙТ

Так как при передаче длинного кадра у приемника может возникнуть проблема с синхронизацией отдельных битов, то целесообразно использовать самосинхронизирующиеся коды.

3.2. Символьно - ориентированные и бит-ориентированные синхронные протоколы

В синхронных протоколах для введения приемника в синхронизацию с передатчиком перед посылкой данных передается настроечная синхро – последовательность. Когда достигается побитовая синхронизация, и приемник уже может распознавать границы байтов, а затем и отдельных полей внутри кадра, передатчик посылает символ начала кадра.

В зависимости от **способов выделения начала и конца кадра** синхронные протоколы делятся на:

- символьно- ориентированные, в которых для выделения начала и конца кадров используются символы из таблиц ASCII или EBCDIC;
- бит- ориентированные, в которых для этого используются специальные последовательности битов, называемые флагами или ограничителями.

Поскольку бит-ориентированные протоколы для обнаружения стартового и стопового флагов сканируют данные побитово, то длина кадра в битах не обязательно должна быть кратной 8 (как в символьно– ориентированных протоколах).

Для исключения из поля данных кадра последовательностей, которые могут совпадать с закрывающим флагом используется операция, которая называется называется *стаффинг* (stuffing). Эта операция добавляет в совпадающую с флагом последовательность биты или символы по заранее известной схеме. Бит-ориентированные протоколы более рационально расходуют поле данных кадра, добавляя в совпадающую последовательность битов только один новый бит, а не целый символ, как это делают символьно– ориентированные протоколы.

…1111111	01111110	1101100111110**1**1011111**0**00…11	01111110	111…
	Открывающий флаг	Поле данных	Закрывающий флаг	

Жирным шрифтом выделены биты, добавленные для стаффинга.

Теперь приведем пример стаффинга в символьно– ориентированном протоколе SLIP:

CO	Данные	CO
Открывающий флаг		Закрывающий флаг

Если в поле данных встречается символ CO, то он заменяется на комбинацию DB+DC, а, если встречается символ DB, то он заменяется на комбинацию DB+DD.

Чтобы избежать операций стаффинга, в составе открывающих и закрывающих флагов можно использовать сочетания битов или сигналы, запрещенные для использования в данных. Например, при использовании манчестерского кодирования открывающий флаг может иметь вид JK0JK000, закрывающий флаг – JK1JK100, где J и K – запрещенные сигналы (не 0 и не 1).

Кадры большинства протоколов состоят из служебных полей фиксированного размера и полей данных, длина которых может изменяться. В этом случае конец кадра может определяться не по закрывающему флагу, а вычисляется по содержимому поля длины данных, которое имеет фиксированный размер. Есть протоколы, кадры которых состоят из переменного числа полей, каждое из которых может иметь переменную длину. Тогда каждое такое поле предваряется двумя фиксированными полями – длины и типа, а конец кадра определяется либо по полю «общей длины», либо по закрывающему флагу.

Определение длины кадра по значению поля длины данных позволяет отказаться от использования закрывающего флага и связанных с ним проблем, но требует включения в кадр дополнительного поля длины. Кадр при этом может выглядеть примерно так:

101010…10	10101011	Фиксированный заголовок	Поле длины поля данных	Поле данных	Фиксированное завершение кадра
Преамбула	Стартовый ограничитель				

Если при передаче данных признаком свободного канала является периодическая посылка передатчиком особых байтов (например, 11111111), то приемник всегда находится в побитовой синхронизации с передатчиком и кадр данных начинается сразу с открывающего флага. А если признаком свободной среды является полное отсутствие передачи, то для введения приемника в синхронизацию с передатчиком передающая станция перед открывающим флагом посылает настроечную последовательность битов – *преамбулу*. В символьно– ориентированных протоколах вместо преамбулы посылается несколько символов с несимметричным кодом (например, 00101100).

3.3. Протоколы с установлением соединения и дейтаграммные протоколы

При дейтаграммной передаче (без предварительного установления соединения) кадр посылается в сеть без предупреждения, исходя из того, что сеть всегда готова его

принять. При этом доставка кадра узлу назначения не гарантируется, зато значительно увеличивается скорость передачи. Ответственность за надежность доставки данных при этом возлагается на протоколы более высоких уровней.

Протоколы с предварительным установлением соединения и подтверждениями (их ещё называют протоколами надёжной или гарантированной доставки) более надёжны, но менее производительны и требуют большей вычислительной мощности от узла назначения. Процедура работы этих протоколов состоит из следующих этапов:

- установление соединения узла-источника с узлом-приемником с помощью посылки служебных кадров по принципу «запрос-подтверждение»;
- передача данных с помощью информационных кадров по принципу «посылка кадра – получение квитанции подтверждения приема»;
- разрыв соединения с помощью служебных кадров по принципу «запрос-подтверждение».

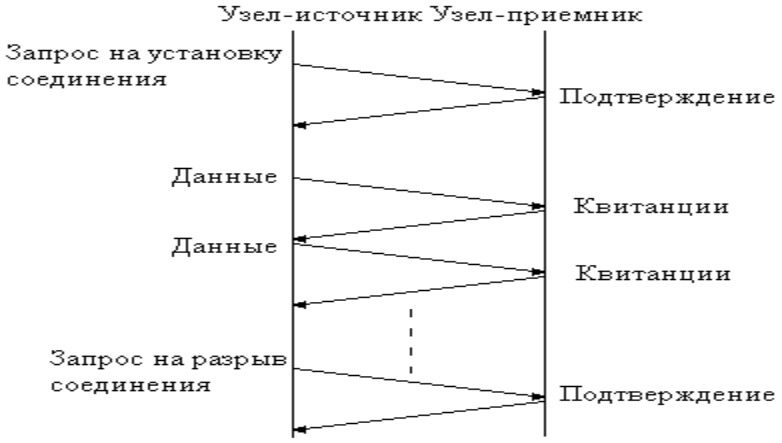


Рис. 3.1. Обмен сообщениями в протоколах с установлением соединения

3.4. Протоколы с восстановлением искаженных и потерянных данных и протоколы без восстановления

Протоколы канального уровня всегда должны **обнаруживать** ошибки передачи данных, связанные с искажением битов в принятом кадре или с потерей кадра. Восстановление данных не является обязательной процедурой канального уровня.

Большинство протоколов канального уровня только обнаруживают ошибки передачи, а **восстановление** искаженных или потерянных данных с помощью повторной передачи пакетов обычно инициируется протоколами верхних уровней. Это характерно для сетей с качественными линиями связи, которые используются в ЛВС. Поскольку протоколы верхних уровней, например, транспортного или сеансового, восстанавливают данные с большой задержкой, то в линиях связи низкого качества целесообразно поручить восстановление данных протоколам канального уровня.

Все *методы обнаружения ошибок* основаны на передаче в составе кадра служебной информации, которая называется контрольной суммой. Контрольная сумма

вычисляется как функция от основной информации. Алгоритмы вычисления контрольной суммы отличаются сложностью и способностью обнаружения разных типов ошибок. Наиболее популярные алгоритмы основаны на использовании циклических избыточных кодов (CRC – Cyclic Redundancy Code). Эти алгоритмы довольно сложны с вычислительной точки зрения, но позволяют обнаружить все одиночные ошибки, двойные ошибки и ошибки в нечетном числе битов.

Для *восстановления кадров* используется метод повторной передачи на основе квитанций. Наиболее популярен *метод «скользящего окна»*. Он заключается в следующем:

Устанавливаются два параметра:

- *размер окна*, определяемый исходя из вероятности повторной передачи и качества линии связи;
- *таймаут* – время ожидания квитанции, которое зависит от задержки передачи кадров сетью.

Во многих реализациях значения этих параметров определяются адаптивно, в зависимости от состояния сети.

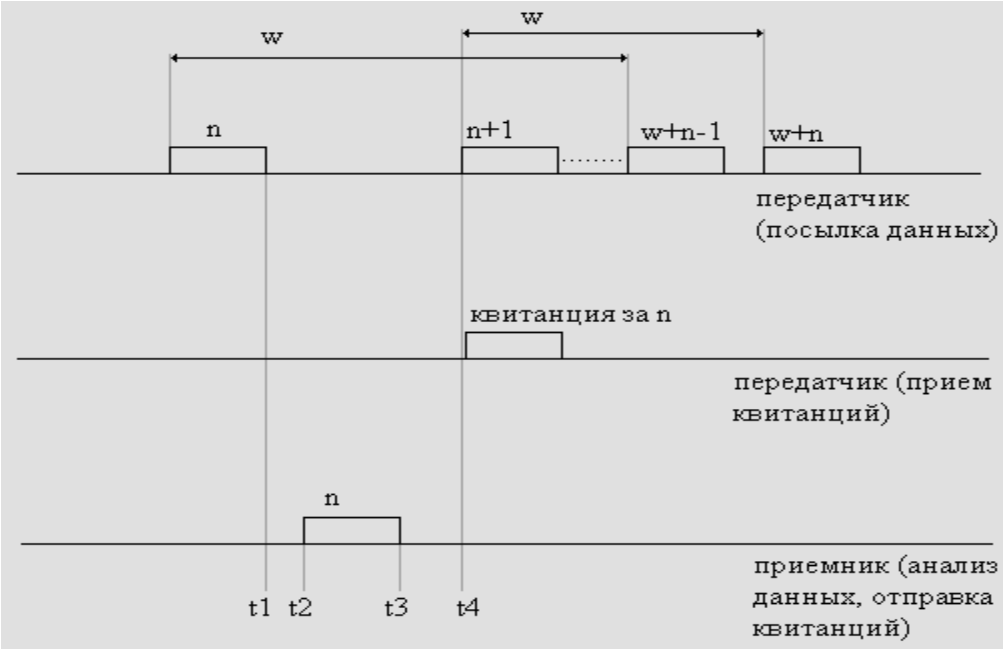


Рис. 3.2. Метод скользящего окна

Допустим, что размер окна равен W кадров сообщения. При получении квитанции на очередной кадр передатчиком начало окна сдвигается на следующий кадр. После отправки в сеть кадра с номером n+1 передатчику разрешается отправить еще W-1 кадров до получения квитанции на кадр n+1. Если за это время квитанция получена не будет, то передача приостанавливается, и по истечении некоторого времени тайм-аута кадр (или квитанция на него) считается потерянным. В этом случае W кадров, начиная с n и заканчивая w+n-1, будут переданы заново.

Если квитанции поступают относительно регулярно, то скорость передачи методом скользящего окна практически не ограничивается. При необходимости частых

повторных пересылок большой размер окна может существенно снизить скорость передачи полезных данных.

3.5. Протоколы с поддержкой сжатия данных или без нее

Для повышения скорости пересылки данных по медленным линиям связи применяется так называемая *динамическая компрессия*, которая в отличие от *статической компрессии* выполняется автоматически при отправке данных. Статическое сжатие данных выполняется до их передачи с помощью прикладных программ, например, ZIP, RAR. Для сжатия данных используются различные алгоритмы, в которых в зависимости от типа данных и алгоритма обеспечивается сжатие 1:2-1:8.

Поскольку, на динамическую компрессию/декомпрессию затрачивается дополнительное время, выигрыш от ее применения достигается только в низкоскоростных каналах связи – до 64 кбит/с. В ЛВС динамическая компрессия/декомпрессия не применяется.

4. Базовые технологии локальных вычислительных сетей

4.1. Структура стандартов IEEE802.x

В 1980 году американский национальный институт IEEE (Institute of Electrical and Electronics Engineering) образовал комитет 802 по стандартизации ЛВС. В результате его работы было принято семейство стандартов IEEE 802.x, которые охватывают два уровня модели OSI:

- физический;
- канальный.

Напомним, что основной задачей физического уровня является передача потока бит информации между передатчиком и приемником в виде физических сигналов, которые распространяются в конкретной физической среде. Канальный уровень ответствен за передачу данных на логическом уровне между отправителем и получателем, которые подключены к общей физической среде передачи. Поэтому, он определяет формат кадра данных, формат локальных адресов, алгоритм последовательности, в которой РС могут предавать данные по общей среде (алгоритм доступа к разделяемой среде), а также метод обнаружения ошибок передачи, и возможно, ряд дополнительных функций. Конкретные протоколы этих двух уровней определены в технологии.

Напомним, что для транспортировки данных в пределах простой одно– сегментной ЛВС, в принципе, достаточно протоколов канального и физического уровня, к которым могут непосредственно обращаться прикладные протоколы. Протоколы других уровней нужны для передачи данных в сложных много– сегментных гетерогенных сетях. Однако на практике, чтобы обеспечивать приложениям возможность работы в любой сети универсальным образом, на конечных узлах устанавливаются полные стеки сетевых протоколов.

В 1985 году международная организация по стандартизации, взяв за основу стандарты IEEE, приняла серию международных стандартов ISO/DIS 8802-2-5 физического и канального уровней.

Структура стандартов:

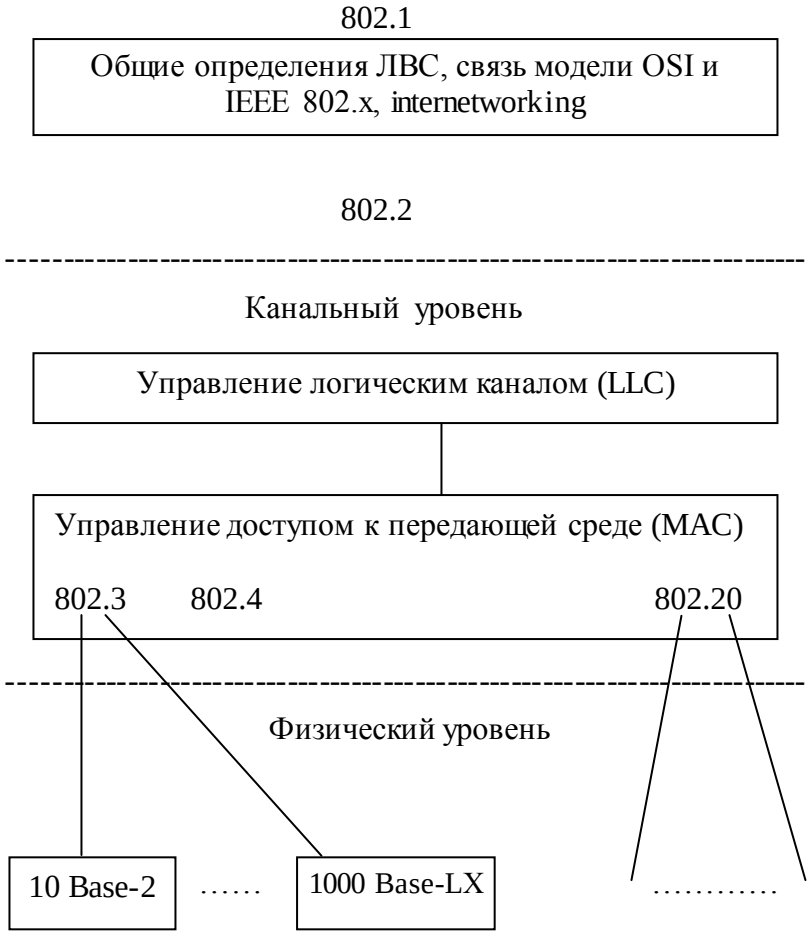


Рис. 4.1. Структура стандартов IEEE 802.x

В разделе 802.1 internetworking стандартизует **средствами канального уровня** для объединения локальных сетей разных технологий, включает стандарты по построению много – сегментных сетей; описание основных и дополнительных функций **мостов и коммутаторов**.

Раздел 802.2 описывает стандарты канального уровня, разделяя этот уровень на два подуровня – LLC и MAC.

Уровень LLC (Logical Link Control) отвечает за передачу данных с требуемой степенью надежности (аналогично транспортному уровню), но на канальном уровне, а также реализует функции интерфейса с сетевым и MAC уровнем. Еще LLC указывает точку входа в протокол вышележащего уровня (обычно сетевого), которому предназначен пакет.

Уровень MAC (Media Access Control) обеспечивает логическую связь узлов сети, и конкретизирует для каждой сетевой технологии способ реализации основных функций канального уровня.

Во всех базовых технологиях ЛВС предусматривается использование разделяемой среды передачи данных и, следовательно, метода доступа к ней. Построение крупных сетей на основе сегментов базовых технологий с помощью коммутаторов описывается в 802.1.

Алгоритмы поочерёдного использования общей физической среды всеми, подключенными к ней узлами (методы доступа к разделяемой среде) можно разделить на:

- методы случайного доступа;
- методам детерминированного доступа.

В *методах случайного доступа* компьютеры могут захватывать среду для передачи порции своих данных в очередном цикле доступа случайным образом в конкурентном режиме. Эти методы просты в реализации, но с ростом загруженности сети возрастает и конкуренция между узлами, вследствие чего, определенная доля пропускной способности сети конкретному узлу может вообще не доставаться. Поэтому такие сети должны работать в недогруженном режиме.

Детерминированные методы доступа гарантируют любой станции получение доступа к общей разделительной среде в течение цикла доступа в равноправном режиме. Детерминированные методы обеспечивают возможность работы сети без заметного замедления в условиях большей нагрузки, чем методы случайного доступа. Кроме того, пропускная способность сети между рабочими станциями распределяется более равномерно. Основным недостатком детерминированных методов по сравнению со случайными методами является сложность алгоритмов, усложнение и удорожание реализующей их аппаратуры.

На конечном компьютере уровень LLC реализуется программно соответствующим модулем ОС, а MAC уровень – частично аппаратно в сетевом адаптере, частично программно в драйвере сетевого адаптера.

Стандарты 802.3-802.20 определяют методы доступа и спецификации физического уровня для разных технологий, например: 802.3 – сети Ethernet с методом доступа CSMA/CD; 802.6 – сети мегаполисов с использованием технологий кабельного телевидения (до 25 км), передачи речи и видеоданных; 802.11 – беспроводные и радиосети для мобильных ПК. В настоящее время стандарт продолжает развиваться и пополнятся.

Каждому стандарту канального уровня, как правило, соответствует несколько стандартов физического уровня для разных сред и разных скоростей передачи данных.

4.1.1. Стандарт IEEE 802.2. Протокол LLC

В основу протокола положен протокол ISO HDLC. Протокол LLC обеспечивает необходимый уровень транспортных услуг на канальном уровне для тех стеков протоколов, которые не поддерживают необходимые функции на транспортном уровне или для устройств, которые поддерживают протоколы только канального и физического уровня, например, некоторая промышленная установка. Второй задачей протокола LLC является организация интерфейса между вышележащим (обычно сетевым) уровнем и нижележащим уровнем MAC.

При передаче данных сверху вниз протоколы сетевого уровня передают через межуровневый интерфейс данные для протокола LLC — свой пакет (например, пакет IP, IPX или NetBEUI), адресную информацию об узле назначения, а также требования к качеству транспортных услуг, которое протокол LLC должен обеспечить. Протокол

LLC помещает пакет протокола верхнего уровня в свой кадр, который дополняется необходимыми служебными полями. Далее через межуровневый интерфейс протокол LLC передает свой кадр вместе с MAC адресом получателя соответствующему протоколу уровня MAC, который помещает LLC в поле данных своего кадра (например, кадра Ethernet). При передаче данных снизу вверх протокол LLC распределяет поток кадров, поступающих из сети, по разным протоколам сетевого уровня.

Кадры уровня LLC имеют единый формат:

Адрес точки входа службы назначения (DSAP)	Адрес точки входа службы источника (SSAP)	Управляющее поле (Control)	Данные (Data)

Поле данных кадра LLC предназначено для передачи по сети пакетов протоколов вышележащих уровней — сетевых протоколов IP, IPX, AppleTalk, DECnet, в редких случаях — прикладных протоколов, когда те вкладывают свои сообщения непосредственно в кадры канального уровня. Поле данных может отсутствовать, например, в управляющих кадрах.

Адресные поля DSAP и SSAP занимают по 1 байту. Они позволяют указать, какая служба верхнего уровня пересылает данные с помощью кадра канального уровня.

Для идентификации этих протоколов верхнего уровня вводятся так называемые адреса точки входа службы (Service Access Point, SAP). Значения адресов SAP приписываются протоколам в соответствии со стандартом 802.2. Например, для протокола IP значение SAP равно 0x6 (т.е.16-ричная 6), для протокола NetBIOS — 0xF0. Значения DSAP и SSAP могут совпадать. Например, если оба поля содержат код протокола IPX, то обмен кадрами осуществляется между двумя IPX-модулями, выполняющимися в разных узлах. Но в некоторых случаях в кадре LLC указываются различные DSAP и SSAP. Это возможно только в тех случаях, когда служба имеет несколько адресов SAP, т.е. несколько точек входа (часто используется протоколом NetBEUI).

Протокол сетевого уровня может обращаться к одной из 3-х процедур (служб), предоставляемых LLC:

1. LLC-1 – без установления соединения и без подтверждения (дейтаграммный способ).

2. LLC-2 – с установлением соединения и подтверждением приема данных.

3. LLC-3 – без установления соединения, но с подтверждением приема данных.

LLC-1 обеспечивает минимальное время и употребляется в тех случаях, когда упорядочение данных и исправление ошибок выполняется протоколами верхних уровней.

LLC-2 устанавливает соединение, упорядочивает поток данных и выполняет восстановление искаженных и утерянных кадров в режиме скользящего окна.

LLC-3 применяется тогда, когда нужно минимальное время пересылки данных, но необходима информация о корректности их приема (например, в управлении промышленными объектами).

Стеки протоколов TCP/IP и IPX/SPX используют протокол LLC-1, возлагая функции по обеспечению надежности доставки на свои транспортные протоколы. А вот стек Microsoft/IBM, основанный на протоколах NetBIOS/NetBEUI, часто использует режим LLC2. Это происходит тогда, когда стек NetBIOS/NetBEUI должен работать в режиме с восстановлением потерянных и искаженных данных, но поскольку его протоколы такими возможностями не обладают, работа перепоручается уровню LLC2. Если же стек NetBIOS/NetBEUI работает в дейтаграммном режиме, то протокол LLC тоже работает в режиме LLC1.

4.2. Стандарт IEEE 802.3. Технология Ethernet

В настоящее время стандарт стал фактически единственным, который используется для построения локальных сетей. В 1995 году появился дополнительный стандарт IEEE 802.3u – Fast Ethernet (100 Мбит/с), а в 1998 – IEEE 802.3z, ab (Gigabit Ethernet – 1 Гбит/с), а в настоящее время - IEEE 802.3ae (10G Ethernet – 10 Гбит/с).

В сетях Ethernet используется метод коллективного доступа с опознаванием несущей и обнаружением коллизий CSMA/CD, который применяется в сетях с логической топологией «общая шина». Данные распространяются в обе стороны «шины» максимально быстро. Кадр, посылаемый одной станцией, получают все остальные, но принимает только та станция, которая опознала свой MAC адрес в поле кадра «адрес получателя». Простота организации и дешевизна этого метода обеспечила популярность сетям, построенным на его основе.

Этот метод относится к *методам случайного доступа* к среде передачи данных. Он предполагает, что все станции, подключенные к сети, могут в любое время обращаться к общей шине. При этом может возникнуть одновременная передача (данные сталкиваются и искажаются). Тогда передачу нужно прекратить и продолжить, когда среда будет свободна.

Рис. 4.2. Метод доступа с опознаванием несущей и обнаружением коллизий

1. Станция прослушивает среду передачи и, если считает ее свободной (отсутствует передача данных), то начинает передачу своего кадра данных. На рис.4.2. узел 1 начал передачу, узел 2 находится в режиме ожидания, пока среда занята. Все станции просматривают кадр. Та станция, которая опознает свой адрес, записывает принятый кадр в свой внутренний буфер.

2. После окончания передачи кадра все станции выдерживают технологическую паузу с целью приведения сетевых адаптеров в исходное состояние и предотвращения монопольного захвата среды одной станцией. На рис.4.2. узел 2 дождался освобождения среды и выдержал *стандартную технологическую паузу*. Для стандарта 802.3 длительность технологической паузы равна 9.6 мкс.

3. Если несколько узлов держали паузу, то после технологического интервала они могут начать передачу одновременно или почти одновременно, что связано с конечным временем распространения сигнала. При этом данные сталкиваются, искажаются, происходит *«коллизия»*. Например, на рис.4.2. узел 3 начал передачу чуть раньше узла 1, но сигнал от узла 3 еще не успел дойти до узла 1, когда узел 1 тоже начал передачу.

4. Если передающая станция считает, что она передала информацию правильно, то искажения будут обнаружены принимающей станцией по контрольной сумме пакета, а повторная передача будет организована протоколом верхнего уровня (например, TCP из стека TCP/IP), на что может уйти до нескольких секунд. Полезная пропускная способность сети упадет. Поэтому важно, чтобы станции-отправители вовремя могли обнаружить коллизию.

5. Чтобы обнаружить коллизию станции – отправители одновременно с передачей продолжают прослушивать среду, и, если предаваемые и наблюдаемые сигналы отличаются, то фиксируется обнаружение коллизии (Collision detection). Для увеличения вероятности скорейшего распознавания коллизии всеми ее участниками, каждая станция, которая обнаружила коллизию, прерывает передачу своего кадра и посылает в сеть jam-последовательность из 32 бит для усиления ситуации коллизии. После обнаружения коллизии и передачи jam-последовательности все передающие станции выдерживают *паузу случайной длительности* (не стандартную технологическую) и снова пытаются захватить среду для повторной передачи искаженного коллизией кадра. Случайная пауза выбирается с целью уменьшения вероятности повторной коллизии между её предыдущими участниками.

Пауза выбирается следующим образом:

Пауза=L·(512·0.1) мкс, где

0.1 мкс – время передачи одного бита при скорости 10 Мбит/с, L – случайное число из диапазона $\{0\text{-}2^N\}$, N – номер повторной попытки передачи 1-10.

После 10-й попытки (с каждой последующей попыткой интервал увеличивается) интервал остается постоянным. Если после 16 попыток кадр так и не удалось передать, он отбрасывается и передача прекращается.

512 – длина минимального кадра с полем данных длиной 46 байт (без преамбулы) в битах.

Для надежного распознавания коллизий всеми станциями необходимо, чтобы соблюдалось *время двойного оборота:*

$T_{min} \geq PDV$,

PDV =2 * L.

где T_{min} – время передачи кадра минимальной длины, PDV – время распространения данных между двумя наиболее удаленными друг от друга станциями сети (L) умноженное на два.

В наихудшем случае, сигнал (первый бит кадра) от станции, которая находится в одном конце сети, должен **успеть дойти** до наиболее удаленной станции в другом конце сети и **вернуться обратно** искаженным (если там произошла коллизия), пока первая станция не закончилась передачу последнего бита своего кадра (рис.4.3).

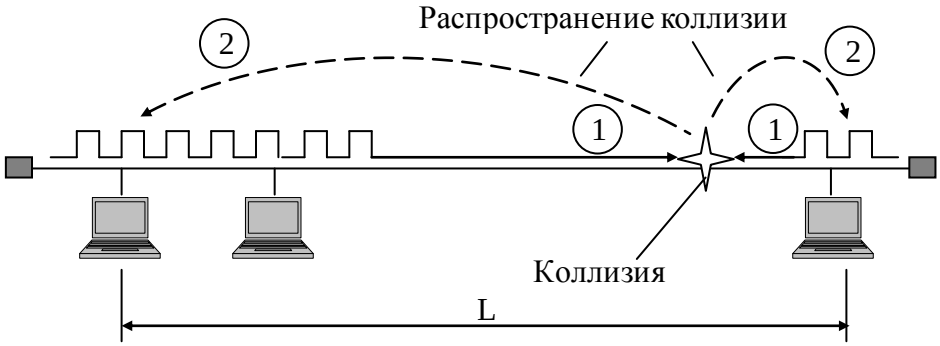


Рис. 4.3. Время двойного оборота

Только в таком случае, станция может определить, что именно ее кадр попал в коллизию. Тогда станция при следующей возможности передачи повторит испорченный кадр данных. Если же станция будет считать, что кадр передан успешно, она продолжит передавать следующие кадры, а восстановлением потерь займутся вышележащие протоколы, что сильно ухудшит производительность сети.

Время двойного оборота обеспечивается правильным выбором параметров сети, в частности, соотношением между минимальной длиной кадра и максимально возможным диаметром сети (расстояние между двумя наиболее удаленными станциями сети). Исходя из этого, минимальная длина поля данных была выбрана равной 46 байтам, а не 0, как в других технологиях, например, Token Ring фирмы IBM.

С увеличением скорости передачи данных должен либо уменьшаться диаметр сети, либо увеличиваться время передачи самого короткого кадра, т.е. его минимальная длинна.

4.2.1. Производительность сети

Максимальная пропускная способность сети Ethernet 10 Мбит/с при передаче кадров минимальной длины будет составлять 14880 кадров в секунду, а при передаче кадров максимальной длины – 813 кадров в секунду.

Полезная пропускная способность (скорость передачи собственно пользовательских данных, без служебной информации, межкадровых интервалов и ожидания доступа к среде) для кадров минимальной длины составляет 5.48 Мбит/с, для кадров

максимальной длины – 9.76 Мбит/с. Однако, в кадрах минимальной длины передаются запросы, квитанции, и к пользовательской информации они отношения не имеют.

Эти данные справедливы, если двум узлам в сети не мешают другие, то есть, нет ожидания доступа, «коллизий», повторной передачи данных. При увеличении количества станций в сети и количества, передаваемых ими данных, скорость обмена между каждой парой пользователей будет падать.

Коэффициент использования сети отображает ее загруженность.

Коэффициент использования сети = текущая пропускная способность/максимальная пропускная способность, где

максимальная пропускная способность – максимальная скорость физического протокола сети;

текущая пропускная способность – суммарная скорость трафика, генерируемого компьютером сети.

В отсутствии коллизий и ожидания доступа этот коэффициент доходит до 0.976 (для кадров максимальной длины).

Но поскольку передача данных компьютерами носит случайный характер, то можно говорить либо о мгновенных значениях текущей пропускной способности сети и о *мгновенных значениях коэффициента*, либо – о среднестатистической текущей пропускной способности и, соответственно, о *среднем значении коэффициента*. Среднестатистическое значение измеряется на длительном интервале времени типичной активности пользователей сети, например, в рабочее время без учёта обеденного перерыва.

Когда среднее значение коэффициента загруженности приближается к 50%, полезная пропускная способность сети резко падает из-за увеличения времени ожидания передачи, «коллизий», времени на повторные передачи данных. Для того, чтобы пользователи сети не замечали замедления её работы, **граничное значение коэффициента загруженности сети Ethernet равно 30 %**.

4.2.2. Формат кадров

Существует несколько стандартов кадра Ethernet. На практике, все оборудование Ethernet использует один формат кадр Ethernet DIX (иногда называемый Ethernet II). В поле данных кадра вкладывается пакет LLC-уровня, который в свою очередь содержат в своем поле данных пакет выше лежащего протокола (чаще всего, сетевого).

Структура кадра следующая:

Преамбула и открывающий флаг	Адрес получателя	Адрес отправителя	Длина поля данных	Данные LLC	Контрольная сумма
8 байтов (7 байтов 10101010 и 1 байт 10101011)	6 байтов	6 байтов	2 байта	46-1500 байта	4 байта

- Преамбула используется для синхронизации приемника с передатчиком, а открывающийся флаг (10101011) для распознавания начала кадра.
- Адрес: 1-й бит старшего байта равен 0, если адрес индивидуальный (у отправителя этот байт всегда равен 0), или 1, если адрес групповой (кадр предназначен для приема несколькими узлами). Если адрес состоит из сплошных единичных битов, то пакет широковещательный (предназначен для приема всеми станциями сети).
- Данные: если поле данных имеет длину меньше 46 байт, оно дополняется байтами заполнения. Короче 46 байт поле данных быть не может, так как будет утеряна возможность распознавания «коллизий».

4.2.3. Спецификации физической среды

В стандарте Ethernet определены 4 протокола физического уровня для нескольких сред передачи данных:

- 10 Base 5 – толстый коаксиальный кабель диаметром 0.5 дюйма
- 10 Base 2 – тонкий коаксиальный кабель диаметром 0.25 дюйма.
- 10 Base T – неэкранированная витая пара и концентраторы
- 10 Base F – оптоволоконные кабели и концентраторы

10 обозначает скорость в Мбит/с. Base – означает сеть с немодулированной передачей, т.е. сигналы передаются в цифровой форме на одной несущей частоте 10 МГц, в отличие от, так называемого, Broadband (широкополосного) канала с частотным разделением и несколькими несущими частотами.

Все спецификации используют для физического кодирования Манчестерский код. Спецификации различаются топологией, максимальным количеством компьютеров и длиной сегментов сети, что обусловлено различием в характеристиках используемых ими кабелей.

Особенности спецификаций 10 Base 5 и 10 Base 2

Сети обоих типов имеют физическую топологию «общей шины». Так как используются разные виды кабеля (с разной полосой пропускания), то спецификации отличаются максимально допустимой длиной сегментов и максимально допустимым количеством станций в сегментах. Отличаются и способы подключения к общему кабелю. Следует так же напомнить, что сама топология «общей шины», используемая в данных сетях, не отличается высокой надежностью. Для определения места неисправности в сети нужен специальный кабельный тестер.

Пример построения сети 10Base 5 показан на рис.4.4.

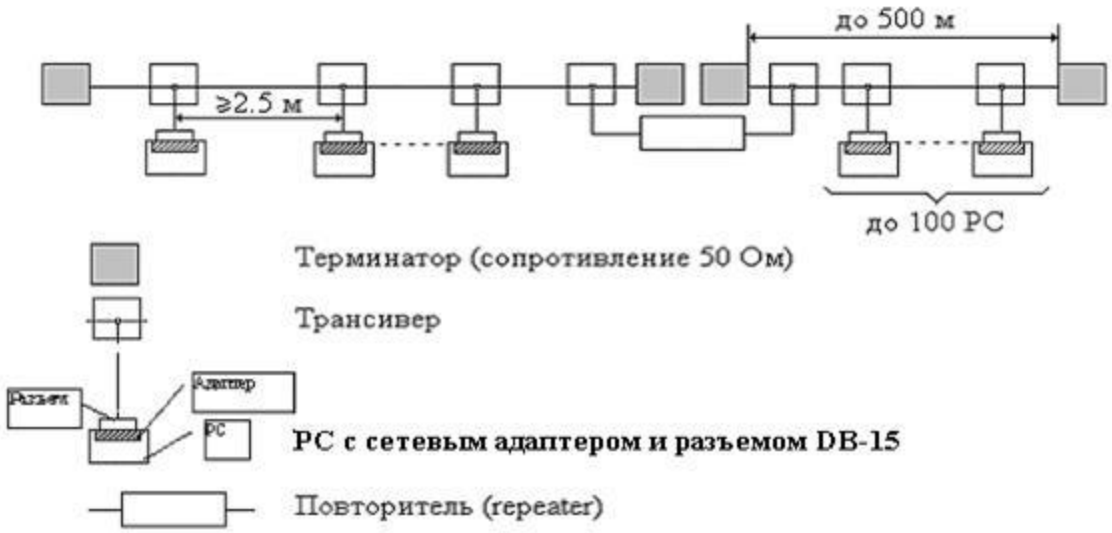


Рис. 4.4. Структура сети 10 Base 5

Терминатор – это согласующее сопротивление, по величине равное волновому сопротивлению кабеля (то есть терминаторы сопротивлением 50 Ом используются только с 50-омным кабелем). Терминатор поглощает сигнал на концах линии, препятствует его отражению и наложению на сигналы, распространяющиеся в среде кабеля.

Интерфейсный кабель между сетевым адаптером и трансивером обозначается AUI – (Attachment Unit Interface).

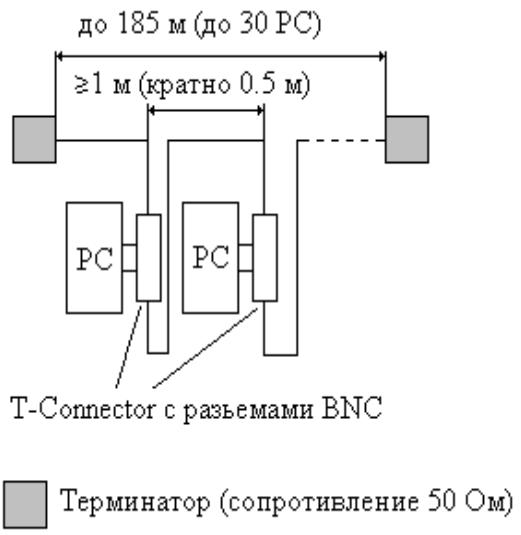
AUI состоит из четырех пар проводов:

- 1 пара – передача;
- 2 пара – прием;
- 3 пара – индикация коллизий;
- 4 пара – питание трансивера (он питается от адаптера).

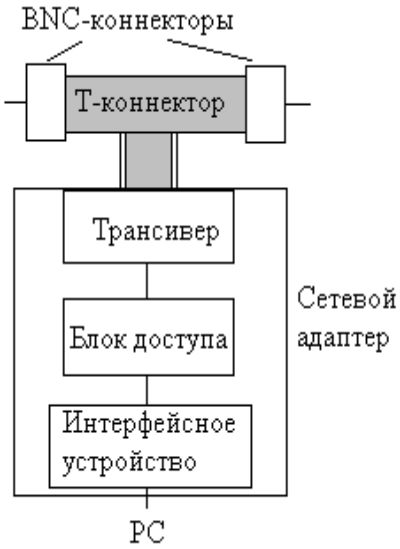
Трансивер (Transmitter + Receiver – приемопередатчик) выполняет следующие функции:

- прием и передача данных;
- определение коллизий в кабеле;
- Электрическая развязка между кабелем и адаптером;
- Защита адаптера и PC от больших перепадов напряжения, которые могут возникнуть в кабеле при его повреждениях посредством отключения адаптера от общего кабеля;
- Защита кабеля от некорректной работы адаптера посредством отключения его от общего кабеля. Неисправный адаптер может вести непрерывную передачу данных.

Пример построения сети 10Base 2 показан на рис.4.5.(а), подключение сетевого адаптера к сегменту сети 10 Base 2 – на рис.4.5 (б).



а)



б)

Рис. 4.5. Сети 10 Base 2: а) структура сегмента, б) подключение компьютера к сети

Удлинение сети с помощью повторителей в сетях 10Base 2 аналогично сетям 10Base 5 (см. рис.4.4.).

Для **соединения между собой отдельных сегментов** в сетях 10Base 5 и 10Base 2 используются *повторители*. Каждый повторитель состоит из двух трансиверов и блока повторения со своим тактовым генератором. Его задачей является увеличение мощности приходящих сигналов (усиление), восстановление их формы (формирование) и скважности (улучшение синхронизации). Поэтому каждый повторитель вносит задержку при передаче кадров из сегмента в сегмент и уменьшает межкадровое расстояние, так как задерживает несколько первых бит преамбулы для улучшения синхронизации.

Напомним, что максимальное время распространения сигналов в сети ограничено временем двойного оборота. Поэтому, общим для обеих спецификаций является правило, называемое «правило 5-4-3»: не более 5 сегментов, не более 4 повторителей, не более 3 нагруженных сегментов. Нагруженным называется сегмент, к которому подключены компьютеры.

Соединение сегментов сети может иметь разный вид. Примеры показаны на рис.4.6.

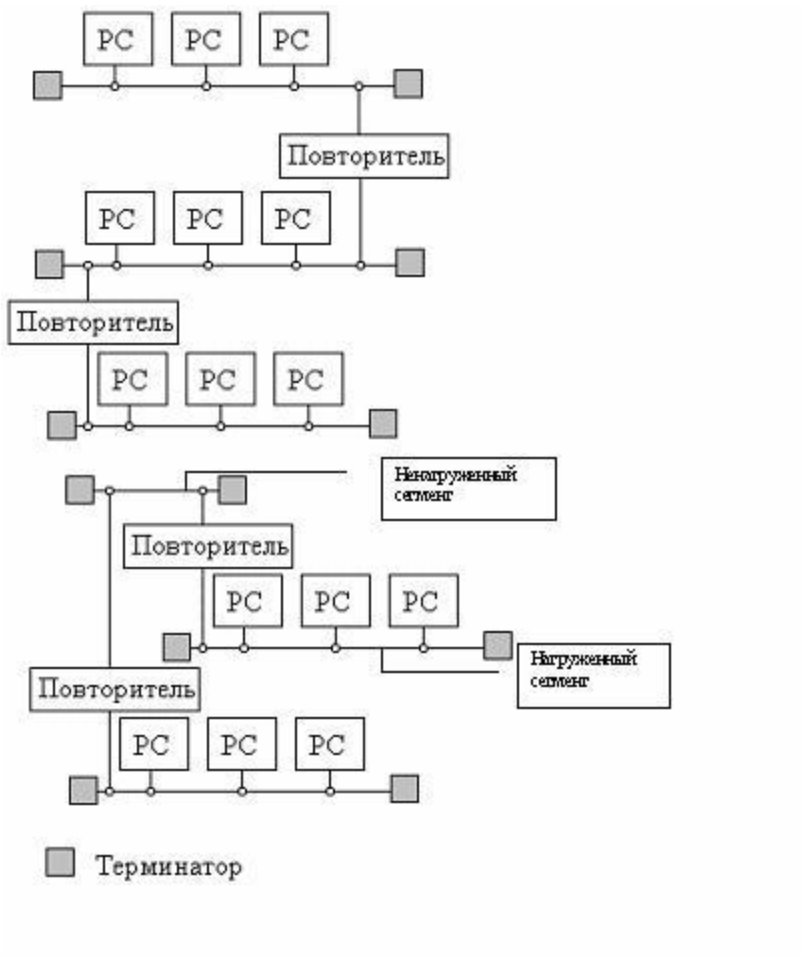


Рис. 4.6. Соединение нескольких сегментов в сетях 10Base 5 и 10Base 2

Сравнение спецификаций 10Base 5 и 10Base 2

К преимуществам спецификации 10Base 5 можно отнести хорошую защищенность от внешних помех и наличие интерфейсного кабеля, что облегчает разводку и при необходимости перемещение станций. Недостатками спецификации являются высокая цена, а также жесткость и толщина кабеля, что усложняет его прокладку и крепление.

В спецификации 10Base 2 кабель обладает худшими, по сравнению с 10Base 5, характеристиками: помехозащищенностью, механической прочностью, полосой пропускания. Но сети 10Base 2 дешевле, чем 10Base 5 или 10Base T (необходим концентратор). Кроме того, сеть 10Base 2 легче наращивается, а используемый в ней кабель гибок и удобен в монтаже. Однако, в сетях 10Base 2 много контактов и соединений, которые нередко нарушаются, что приводит к неработоспособности сети.

Спецификация 10Base T

В этих сетях каждый компьютер сегмента подключается 2-мя витыми парами к многопортовому повторителю, который называется концентратор или hub. К каждому его порту можно подключить один компьютер. Повторитель принимает сигналы по одному из своих портов и передает их на все остальные, кроме того, с которого пришел сигнал.

Данная спецификация при физической топологии «звезда» имеет логическую топологию «общая шина». Для соединений используется неэкранированная витая пара категории 3 или выше.

Если сигнал появляется одновременно на двух или более портах, то концентратор считает, что возникла коллизия, и передает jam-последовательность.

Данная спецификация хорошо подходит для мест, где есть доступная для использования телефонная разводка в подходящем состоянии.

Структура одного сегмента с концентратором показана на рис.4.7, где Tx – Transmitter (передатчик), Rx – Receiver (приёмник).

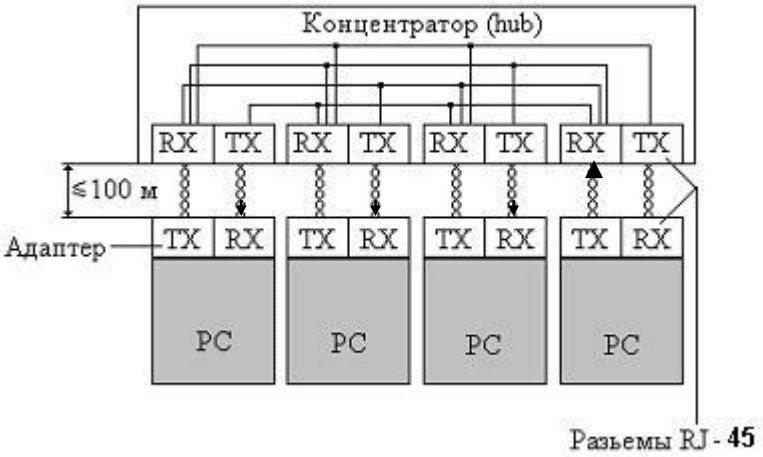


Рис. 4.7. Структура сегмента с концентратором

Для увеличения размеров сети концентраторы могут соединяться между собой, образуя древовидные структуры (рис.4.8). Общее количество станций в сети 10Base-T не должно превышать 1024, а длина отрезка витой пары между 2-мя соседними портами не должна превышать 100м. Это связано с ограниченной полосой пропускания витой пары. В соответствии с ограничением, которое налагается временем двойного оборота, максимальное количество концентраторов между любой парой станций не должно превышать четырех, или это называется правилом «4-х хабов».

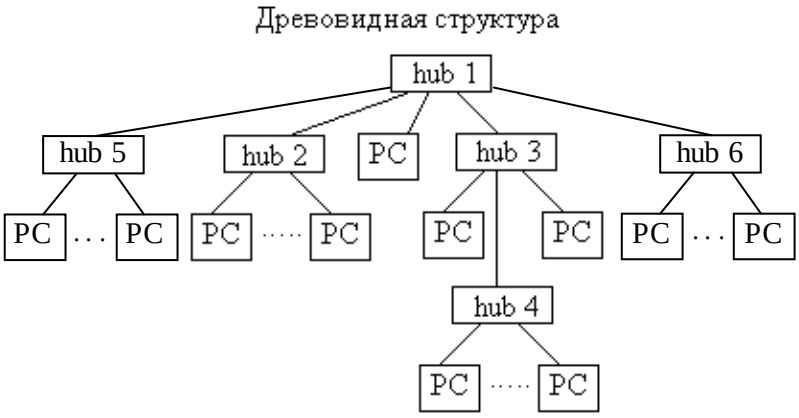


Рис. 4.8. Ссоединение концентраторов между собой в древовидную структуру

К преимуществам данной спецификации можно отнести легкость монтажа и надежность. Концентратор вносит некоторый **элемент отказоустойчивости** в работу сети. Он тестирует свои связи, обмениваясь сигналами с соседними портами в то время, когда они не заняты передачей данных. В случае обнаружения неисправности концентратор отключает неисправный порт и включает индикаторную лампочку. Неисправности могут иметь характер: обрыва (порт не отвечает), передачи станцией слишком коротких кадров (длина кадра меньше минимально допустимой) или слишком длинных кадров (длина кадра больше максимально допустимой). Через некоторое время тестирование возобновляется.

К недостаткам спецификации можно отнести необходимость применения концентратора, что повышается стоимость сети, и большой расход кабеля, так как от каждой станции к концентратору идет отдельный кабель.

Спецификации 10 Base F, 10 Base FL, 10 Base FB

Это спецификации сетей на основе оптоволоконных кабелей. В них используются 50- или 100-микронные кабели. Подключение станций организуются с помощью концентраторов аналогично подключениям в сети 10Base T.

Спецификации 10Base F, 10Base FL, 10Base FB несколько различаются между собой. Первые две различаются между собой по параметрам, а последняя спецификация используется только для соединения концентраторов между собой. Повторители стандарта 10Base FB вносят меньшую задержку в передачу сигналов, чем повторители остальных стандартов, поэтому, между 2-мя узлами, их может быть 5, а не 4.

Сравнительная характеристика спецификаций физического уровня Ethernet

Максимальные значения параметров для спецификаций технологии Ethernet приведены в таблице 4.1.

Таблица 4.1. Сравнительная характеристика спецификаций технологии Ethernet

Параметр	**10Base-5**	**10Base-2**	**10Base-T**	**10Base-F**
Кабель	Толстый коаксиальный кабель RG-8 или RG-11	Тонкий коаксиальный кабель RG-58	Неэкранированная витая пара категории 3 и выше	Многомодовый волоконно-оптический кабель
Максимальна длинна (диаметр) сегмента, м	500	185	100	2000
Максимальное расстояние между узлами сети (при использовании	2500	925	500	2500 (2740 для 10Base-FB)

повторителей), м				
Максимальное число станций в сегменте	100	30	1024	1024
Максимальное число повторителей между любыми станциями сети	4	4	4	4 (5 для 10Base-FB)

Следует обратить внимание на то, что ограничение на длину сегмента и количество станций в нём связано с ограниченностью полосы пропускания кабеля (затуханием сигнала), а ограничение на количество сегментов и число повторителей накладывается временем двойного оборота.

Конструкции концентраторов могут предусматривать порты для подключения разных спецификаций. Для таких смешанных сетей, состоящих из сегментов, работающих по разным стандартам, расчет допустимых диаметров и максимального количества станций и повторителей производится вручную. Исходные данные для расчетов поставляются комитетом по стандарту IEEE 802.3.

Дальнейшее развитие стандартов 10Base связано с использованием коммутаторов вместо концентраторов. Если вместо корневого концентратора поставить коммутатор, тогда каждый сегмент на концентраторе будет представлять собой отдельную сеть. Коллизии локализуются внутри отдельных сегментов и за пределы этих сегментов не распространяются. При этом говорят, что каждый сегмент образует домен коллизий. Кроме того, данные между сегментами, которые подключены к разным портам коммутатора, могут передаваться параллельно, что повышает общую производительность сети.

4.3. Стандарт IEEE 802.5. Сети с маркерным доступом

Маркерный метод доступа гарантирует любой станции получение доступа к общей разделительной среде в течение максимального времени оборота маркера по кольцу. Поэтому метод относится к *методам детерминированного доступа*. Это дает сетям возможность работать в условиях большей загруженности, чем метод случайного доступа, используемый, в частности, в сетях Ethernet. Если загруженность сети будет превышать критическую, то ее производительность будет падать, но степень падения производительности можно предсказать.

Из сетей этого стандарта наибольшее распространение имели сети Token Ring фирмы IBM. Технология предусматривает две битовые скорости: 4 Мбит/с и 16 Мбит/с. Использовать в одной сети две скорости одновременно нельзя.

Логическая топология сети – кольцо. Станции подключены к общему кольцу, по которому циркулирует кадр маркера. Каждая станции получив маркер, отправляет свои данные, и передает маркер следующей станции.

При передаче файлов больших размеров соотношение в потоке данных пользователя и служебных данных в этих сетях лучше, чем в сетях Ethernet.

Сети технологии Token Ring обладают элементами отказоустойчивости. Процедуры контроля за рабой сети используют обратную связь кольцеобразной структуры – посланный кадр по кольцу возвращается от получателя к отправителю с подтверждением о приеме. Кроме того, одна из станций, называемая активный монитор, постоянно контролирует работу кольца. Некоторые ошибки, например, потеря маркера, могут устраняться автоматически. В других случаях фиксируется место и тип неисправности.

В сетях Token Ring есть механизм назначения приоритетов для трафика реального времени, но пользоваться им довольно сложно. Для этого приложение или прикладной протокол должны уметь таким механизмом пользоваться. Поэтому на практике все станции обычно имели равные права доступа к кольцу.

Особенности метода доступа:

Каждая станция сети непосредственно связана с двумя соседями. Та, от которой данная станция получает данные, называется ближайшим активным соседом выше по потоку, а та, которой передает данные - ближайшим активным соседом ниже по потоку.

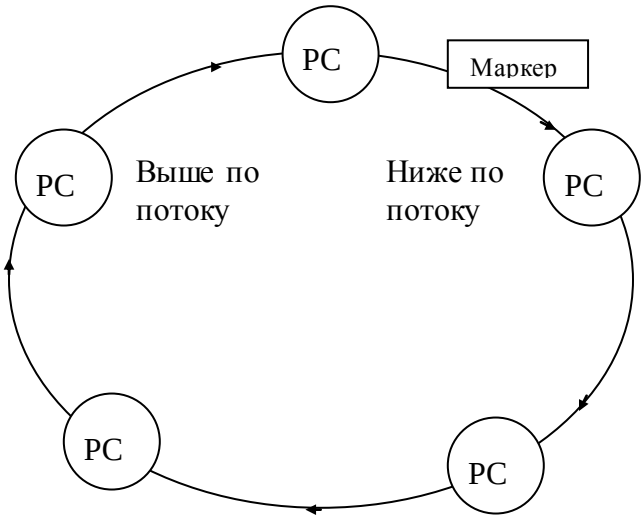


Рис. 4.9. Схема передачи данных в сети Token Ring

По сети от станции к станции циркулирует кадр-маркер. Если у станции нет данных, которые нужно передавать, то при получении маркера она передает маркер следующей станции. Если у станции есть данные, подлежащие передаче, то она вместо маркера передает один (большой) или несколько (маленьких) кадров данных в течение фиксированного *времени удержания маркера*. По умолчанию это время равно 10 мкс, отсюда максимальный размер одного кадра при скорости 4 Мбит/с равен 4 килобайтам, а при скорости 16 Мбит/с – 16 килобайтам. Адаптеры других станций побитово транслируют проходящие по сети кадры данных.

Станция, которой предназначен кадр данных, копирует его в свой буфер, сетевой адаптер ставит в кадр признак приема и передает его дальше по кольцу. Когда кадр возвращается к станции-отправителю с признаком приема, станция-отправитель удаляет этот кадр и передает кадр-маркер следующей станции. Если кадр был принят с ошибкой, станция-отправитель при следующей передаче будет пересылать его повторно.

Для скорости 4 Мбит/с станция-отправитель при передаче нескольких кадров подряд в течение времени удержания маркера может передавать следующий кадр только после получения подтверждения о доставке предыдущего.

Для скорости 16 Мбит/с используется алгоритм раннего высвобождения маркера. Маркер передается сразу же, как только данная станция закончила передачу одного или нескольких кадров за время удержания маркера, не дожидаясь подтверждения приема. Тогда в случае получения отрицательных подтверждений станция будет передавать искаженные данные повторно при следующем получении маркера. Этот алгоритм напоминает метод скользящего окна.

Кадры данных могут иметь приоритет от 0 до 7, маркер тоже имеет приоритет. Кадры и маркер имеют *основное и резервное* поле приоритета.

Станция имеет право на передачу, если приоритет ее данных больше или равен приоритету, указанному в основном поле маркера. Иначе станция передает маркер следующей станции, а в резервном поле маркера может поставить приоритет своих данных, резервируя очередь для будущей передачи. Причем изменить значение резервного поля маркера станция может только, если приоритет ее данных выше того, что уже стоит в этом поле. В результате поле резервного приоритета маркера зарезервирует очередь для станции с наивысшим приоритетом данных, но меньшим, чем у маркера. Станция, которая сможет захватить маркер, передаст свои данные, запишет в основное поле маркера значение из резервного поля, а резервное поле обнулит. Теперь при следующем проходе маркера по кольцу его захватит зарезервировавшая себе очередь станция.

Приоритетный механизм работает только, если он используется прикладным уровнем.

4.3.1. Управление сетями Token Ring

Управление работой сети осуществляет одна из ее станций, называемая *активным монитором*. Активный монитор анализирует проходящие через него кадры и выполняет следующие функции:

- Удаляет все поврежденные или некорректные кадры.
- Выдает в сеть новый маркер, если на протяжении времени тайм-аута не получает маркер из сети. Тайм-аут – время полного оборота маркера по кольцу, при условии, что все станции имеют данные для передачи.
- Активный монитор ответственен за наличие одной копии маркера в сети.
- Активный монитор оказывает помощь в локализации неисправностей в сети.
- Активный монитор выполняет функции повторителя в сети. Каждый сетевой адаптер Token Ring имеет блок повторения для регенерации и ресинхронизации сигнала, но активизируется этот блок только, если станция становится активным монитором. В этом блоке содержится 32-битовый буфер, принимающий сигналы с линии с искаженными интервалами следования и выдающий эти сигналы в скорректированном виде. Сетевые адаптеры остальных станций только усиливают сигналы без регенерации.

Некоторые функции управления сетью выполняются не активным монитором, а другими станциями, называемыми пассивными мониторами. Активный монитор каждые 3 секунды генерирует кадр, указывающий на его присутствие в сети. Если этот кадр не фиксируется другими станциями в течение 7 секунд или обнаруживаются другие сбои в работе активного монитора, то станции сети начинают процедуру выбора нового активного монитора. Они начинают генерировать кадры требования маркера. Каждая станция, получив такие кадры от других, сравнивает их адреса со своим адресом. Если ее адрес меньше, она выбывает из соревнования и начинает генерировать кадры присутствия запасного монитора. В результате соревнования побеждает станция с максимальным адресом – она становится активным монитором.

4.3.2. Форматы кадров сети Token Ring

В сети Token Ring можно выделить следующие несколько типов кадра. В начальном и конечном разделителе используются запрещенные комбинации манчестерского кода, что исключает необходимость стаффинга. Основными являются кадр маркера и кадр данных.

Структура кадра маркера:

Начальный разделитель JK0JK000	Управление доступом PPPTMRRR	Конечный разделитель +признаки JK1JK1**EI**

Структура кадра данных:

Начальный разделитель	Управление доступом	Адрес получателя	Адрес отправителя	Поле данных	Поле контрольной суммы	Конечный разделитель +признаки	Статус кадра
1 байт	2 байта	6 байт	6 байт	0-4332 байта для 4 Мбит/с; 0-17832 - для 16 Мбит/с	4 байта	1 байт	1 байт

Значения полей:

PPP – поле основного приоритета; RRR – поле резервного приоритета; T – бит маркера (устанавливается в 1 только в кадрах маркера); M – бит монитора (устанавливается в 1 только, если кадр сгенерировал активный монитор).

E – признак ошибки данных. Станция-отправитель устанавливает его в 0, а любая другая станция в случае обнаружения ошибки в контрольной сумме или длине кадра (слишком длинный или слишком короткий) устанавливает его в 1. Впоследствии первая станция, обнаружившая 1 в этом поле, регистрирует кадр. Это помогает локализовать место возникновения ошибки.

I – признак последнего (I = 0) или промежуточного (I = 1) кадра в серии кадров.

Поле статуса – содержит 2 признака: распознавания адреса получателя и копирования кадра получателем. В поле статуса указывается, был ли найден адрес получателя в сети и был ли пакет получен без ошибок. Станция-отправитель устанавливает оба признака в 0. Если адрес получателя присутствует в сети (PC получателя активна) и кадр был благополучно прочитан получателем, то оба признака будут установлены в 1. Если в последствии кадр вернется к отправителю с установленным битом ошибки E, то он будет знать, что ошибка произошла не у получателя, а в другой части кольца.

Структура поля адреса получателя аналогична таковой в стандарте 802.3. Первый бит указывает тип адреса (0 – индивидуальный адрес, 1 – групповой). Второй бит указывает способ назначения адреса: 0 – адрес назначается централизованно, 1 – адрес назначается локально. Если адрес состоит сплошь из единиц – данный кадр широковещательный (предназначен всем станциям). Поле адреса отправителя имеет следующие отличия. Если адрес групповой (первый бит = 1), то это значит, что сеть состоит из нескольких колец Token Ring, связанных между собой мостами, и для них в кадре есть дополнительное поле маршрутной информации.

Кадры данных содержат данные пользователя (например, сетевого протокола), упакованные в пакет LLC или информацию по управлению и мониторингу сети.

Размер кадров данных стандартом не ограничен и практически выбирается исходя из времени удержания маркера, то есть от 0 до 4 килобайт для 4-мегабитной и от 0 до 16 килобайт для 16-мегабитной сети.

4.3.3. Физический уровень сети Token Ring

Физическая топология сети может представлять собой кольцо или смесь звезды и кольца (рис.4.10).

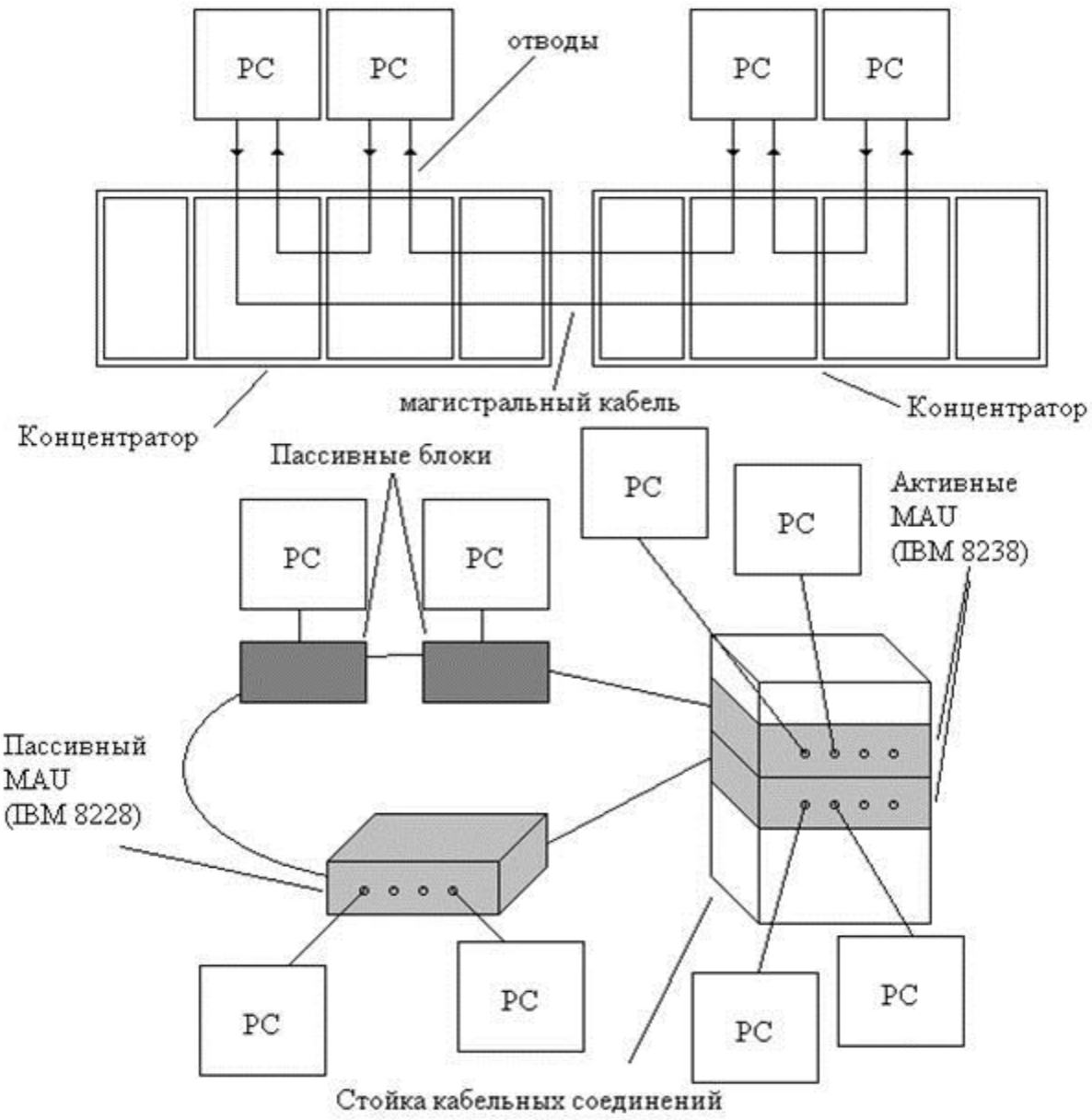


Рис. 4.10. Топология сети Token Ring

В отводах две пары проводов: одна – для приема, вторая – для передачи данных. Подключение со стороны сетевого адаптера осуществляется через разъемы DB9 или RJ-45. Адаптеры автоматически различают скорости 4 и 16 Мбит/с.

Подключение к магистрали может осуществляться с помощью одиночного пассивного блока с нормально замкнутыми релейными контактами, которые питаются от сетевого адаптера. Если станция выключается, контакты замыкаются и восстанавливают целостность магистрали.

Но, как правило, используются не одиночные блоки, а так называемые MAU (Multistation Access Unit). MAU бывают пассивные и активные. Пассивные MAU – это практически объединенные в группы одиночные блоки. Активные MAU выполняют

также функции регенерации сигналов. Они выполняются в виде концентраторов или контроллеров, имеющих дополнительные функции управления сетью.

Обычно активные и пассивные MAU размещаются в одной или нескольких стойках кабельных соединений, а к стойкам подключаются станции. Для отводов и магистралей используется экранированная витая пара STP Type-1 или неэкранированная витая пара UTP 3-й категории; может также использоваться оптоволоконная или неэкранированная пара UTP шестой категории.

Максимальное количество станций и максимальная длина кольца определяется в основном временем оборота маркера и временем его удержания.

Сравнительная характеристика спецификаций технологии Token Ring приведена в таблице 4.2.

Таблица 4.2. Основные характеристики сетей Token Ring

Кабель	**STP T1**	**UTP T3**
Максимальное число узлов	260	72
Максимальная длина кольца	4000 м	4000 м
Максимальное длина отводов	100 м	45 м
Максимальное расстояние между пассивными MAU	100 м	45 м
Максимальное расстояние между активными MAU	730 м	365 м

В скором времени после появления технологии Fast Ethernet фирма IBM подготовила спецификации High Speed Token Ring на 100-155 Мбит/с и предполагала создание стандарта со скоростью в 1 Гбит/с.

Однако к этому времени стоимость коммутаторов значительно уменьшилась и приблизилась к стоимости концентраторов. А алгоритм полнодуплексной передачи данных коммутаторами одинаков для всех технологий ЛВС. Следовательно, преимущества метода доступа к разделяемой среде передачи утрачивают своё значение.

Итак, сети Token Ring по сравнению с Ethernet имеют:

- лучший механизм управления доступом более равномерное распределение пропускной способности сети между рабочими станциями – каждая из них в течении времени оборота маркера гарантированно получает право на передачу своей порции данных;
- более высокий коэффициент использования пропускной способности сети (0.6);
- лучший механизм определения и исправления ошибок на канальном уровне управление с помощью активного монитора, мониторинг сети и квитанции от получателя по обратной связи кольца;
- лучшее соотношение между объемами полезных данных и служебной информации;
- существенно уступают в сложности и стоимости.

Как показало время именно эти недостатки в сочетании с широким распространением и удешевлением коммутаторов определили победу Ethernet на рынке технологий ЛВС.

4.4. Технология FDDI

Сокращение FDDI расшифровывается как Fiber Distributed Data Interface (оптоволоконный распределенный интерфейс данных). Эта технология была разработана в середине 80-х годов американским институтом национальных стандартов ANSI и была впоследствии положена в основу международного стандарта ISO 9314. Основным назначением технологии было создание магистрами для объединения сетей на основе Ethernet и Token Ring.

Из этого назначения вытекают и основные цели, которые ставились перед данной технологией:

- Увеличение скорости обмена до 100 Мбит/с.
- Высокая отказоустойчивости сети, обеспечиваемая за счет введения процедур восстановления после отказа оборудования (повреждений кабеля, некорректной работы станций или концентраторов, помех на линиях).
- Повышение расстояния между узлами.
- Одинаково эффективная работа при передаче как синхронного (чувствительного к задержкам трафика), так и асинхронного (нечувствительного к задержкам) трафика при большой загруженности сети (0.7).

Сеть строится на основе двух оптоволоконных колец: основного (primary) и резервного (secondary). Данные по кольцам передаются в противоположных направлениях. Обычно используется основное кольцо, а при повреждениях участков выполняется переключение на резервное кольцо средствами концентраторов и сетевых адаптеров. При обрыве кабеля в одном месте длина кольца увеличивается в 2 раза. При множественных повреждениях магистрали, сеть распадается на несколько независимых работающих сетей.

Большое расстояние обеспечивается тем, что каждая станция работает как активный повторитель.

Эффективная работа в условиях повышенной нагрузки достигается благодаря усовершенствованию метода доступа разделяемой среде.

Максимальное количество рабочих станций ограничивается максимальной задержкой при передаче данных в кольце T_{max}.

4.4.1. Метод доступа FDDI

Метод доступа технологии FDDI во многом основан на методе доступа Token Ring с алгоритмом раннего освобождения маркера, но имеет и ряд преимуществ перед ним.

Основные отличия состоят в следующем:

1. Трафик делится не на 8 приоритетов, а на 2 класса: синхронные данные (например, мультимедиа реального времени), которые необходимо передавать небольшими порциями с фиксированными задержками; асинхронные данные (например, файлы), которые не критичны к задержкам между кадрами данных, их желательно передавать реже, но большими порциями. Тип трафика задается протоколами верхних уровней.
2. Время удержания маркера не фиксированная величина. Оно позволяет обеспечить требования синхронного трафика, а для асинхронного трафика является адаптивным к загруженности сети и хорошо регулирует её, притормаживая передачу несрочных асинхронных кадров.
3. В сети нет станции–«активный монитор», все станции принимают участие в управлении кольцом.

Во время инициализации кольца станции договариваются о T_{max} – *максимально допустимое время оборота маркера по кольцу*. Процесс инициализации запускается при подключении или удалении станции из сети, а также при изменении значения T_{max}. При этом каждая станция предлагает свое значение T_{max}, исходя из предельно допустимого времени между передачей своих кадров. Процедура похожа на выборы активного монитора в Token Ring. В соревновании побеждает станция с минимальным значением T_{max} (для учета потребностей самого чувствительного к задержкам передачи синхронного трафика). Эта станция становится собственником маркера. Она посылает всем станциям сети управляющее сообщение о необходимости установить у себя новое значение T_{max}. Исходя из T_{max}, определяется <u>фиксированное</u> малое *время удержания маркера* для передачи синхронных кадров $Tc_{удержания}$ и <u>начальное время</u> для передачи асинхронных кадров $Ta0_{удержания}$. Эти значения выбираются таким образом, чтобы в течении T_{max} каждая станция кольца успевала передать по порции синхронных данных, и оставался определенный запас времени для передачи некоторыми станциями асинхронных данных. Потом станция – собственник маркера передает свою порцию синхронных данных и отдает маркер следующей станции. Во время первого прохода маркера по кольцу разрешается передавать только синхронные данные.

В дальнейшем, если станция передает синхронные данные, то при поступлении к ней маркера, она всегда имеет право его захватить и передавать данные в течение $Tc_{удержания}$.

Если станция передает асинхронные данные, то при приходе маркера она измеряет *время фактического оборота маркера* T_{rial}, т.е. время, которое прошло от предыдущего прихода маркера, и может передавать свои кадры в течение времени удержания равного $Ta_{удержания} = Ta0_{удержания}. + (T_{max} - T_{rial.})$. Если кольцо не перегружено (мало станций на прошлом круге передавало данные), то $T_{rial} < T_{max}$ и $Ta_{удержания}$ у станции возрастает по сравнению с $Ta0_{удержания}$. По мере увеличения передачи асинхронных данных в кольце T_{rial} будет увеличиваться, а $Ta_{удержания}$ - соответственно уменьшаться. Наконец, когда $T_{rial} \geq Ta0_{удержания}. + T_{max}$, станция потеряет право захватывать маркер для асинхронного трафика. До конца круга будут передаваться только синхронные данные.

Если все станции хотят передавать асинхронный трафик, а маркер прошел по кольцу слишком медленно, тогда все станции его пропустят, он быстро обернется по кругу и в следующем цикле станции будут его захватывать.

4.4.2. Протоколы. Формат кадра

Рис. 4.11. Протоколы FDDI

Уровень SMT – Station Management организует управление и мониторинг сети средствами протоколов FDDI. В отличие от Token Ring, в FDDI нет активного монитора. В управлении кольцом принимают участие все станции, которые в соответствии с протоколом SMT обмениваются кадрами (на уровне MAC) и сигналами (на физическом уровне) для управления и контроля над сетью. Например, при первоначальном подключении узла (станции или концентратора) к сети под управлением протокола SMT выполняется процедура физического соединения, которая состоит в последовательном тестировании правильности соединения и качества новых связей.

Кроме SMT в обеспечении отказоустойчивости играют роль и другие протоколы. Так протоколы физического уровня обеспечивают реконфигурацию сети из-за физических отказов, а протокол MAC-уровня – после логических отказов (например, потеря внутреннего пути между портами концентратора при передаче кадров данных или маркера).

Формат кадра FDDI аналогичен Token Ring. Отличие состоит в размере поля данных, максимальный размер которого составляет 4478 байт. Максимальный размер кадра 4500 байт. Преамбула состоит из 16 единиц для синхронизации, а в поле управления отсутствуют поля приоритета. Вместо них указывается тип трафика (синхронный или асинхронный).

4.4.3. Физический уровень

В технологии есть 2 спецификации физического уровня (2 типа PMD):

- для оптоволоконного кабеля — основная ;
- для витой пары категории 5 — называется TP -PMD.

<u>Спецификация для оптоволоконного кабеля</u>

На уровне логического кодирования используются избыточные коды 4B/5B, для физического кодирования используется потенциальный код NRZI, который обеспечивает более узкий спектр передаваемого сигнала, чем у манчестерского кода.

Логическое кодирование применяется для улучшения физического потенциального кода (обеспечения самосинхронизации и отсутствия постоянной составляющей). Для 4-х битовых информационных символов необходимы 16 комбинаций; а поскольку 5-битный код дает 32 комбинации, то остальные 16 комбинаций используются для служебных целей. Например, символ простоя Idle постоянно передается в интервалах между передачей кадров для тестирования связности. Если поток символов между портами отсутствует, то выполняется реконфигурация внутреннего пути станции или концентратора.

При скорости передачи данных в 100 Мбит/с частота работы передатчика FDDI составляет 125 Мгц. Это необходимо для компенсации времени на передачу избыточных бит, образовавшихся при логическом кодировании.

Спецификация для витой пары

Для физического кодирования используется потенциальный трехуровневый код MLT-3. Для получения равномерного по мощности спектра этого кода в качестве предварительного логического кодирования применяется скремблирование.

Сравнительная характеристика спецификаций технологии FDDI приведена в таблице 4.3.

Таблица 4.3.Общие характеристики физического уровня технологии FDDI

Среда передачи /параметры сети	Кабель многомодовый оптический 62.5/125 мкм, источник — светодиод с λ=1300нм	Неэкранированная витая пара категория 5
Максимальная длина сети	100 км на 1 кольцо	50 км
Максимальное расстояние между узлами	2 км (не более 11 Дб потерь между узлами)	100 м от концентратора до узла
Максимальное количество узлов	500 двойных подключений или 1000 единичных соединений	500 двойных подключений или 1000 соединений

4.4.4. Подключение устройств к сети

В FDDI предусмотрено 2 вида подключения конечных узлов (станций, концентраторов) к двойному кольцу:

- SA-Single Attchment (одинарное подключение);
- DA-Double Attachment (двойное подключение).

Соответственно различаются SAS (Single Attachment Station), DAS (Double Attachment Station) и SAC, DAC(то же самое с концентраторами). Общая схема организации сети показана на рис. 4.12.

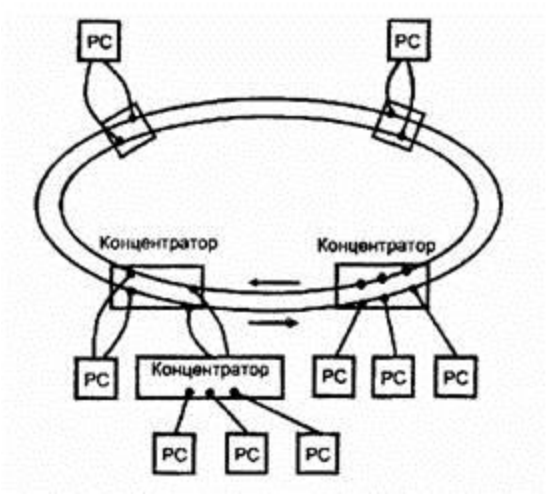


Рис.4.12. Общая схема подключения устройств к сети FDDI

На магистрали для повышения надежности используются концентраторы и мощные дорогие станции с двойным подключением, а рабочие станции подключаются к магистральным концентраторам одинарными связями, что существенно дешевле.

К характерным особенностям технологии, обеспечивающим ее повышенную надежность, относится следующее:

- В станциях DAS необходимы оптические обходные переключатели, которые создают обходной путь для светового потока при отключении питания от станции. Они же организуют реконфигурацию внутренних путей в концентраторах и сетевых адаптерах.
- Протоколы SMT организуют слежение станции и концентраторов за интервалами времени циркуляции маркера и кадров, а также за наличием физического соединения между портами. Все узлы равноправны и в случае обнаружения неисправности начинают процесс повторной инициализации сети, а затем ее реконфигурацию.

Процесс реконфигурации кольца, к которому подключены 3 станции DAS и один концентратор DAC (к нему, в свою очередь, подключены 3 станции SAS) показан на рис.4.13. На рисунке показан случай повреждения одного из двойных подключений DAS PC3 к кольцу. Реконфигурация выполняется средствами протоколов физического уровня, реализованных в соседних с поврежденным участком устройствах. В данном случае — это сетевой адаптер станции PC3 и концентратор DAC. Если бы обрыв произошел в соединении одной из станций PC4 — PC6, то эта станция осталась бы отключенной от сети, а концентратор просто замкнул бы обходной переключатель порта, сохраняя целостность основного кольца без реконфигурации.

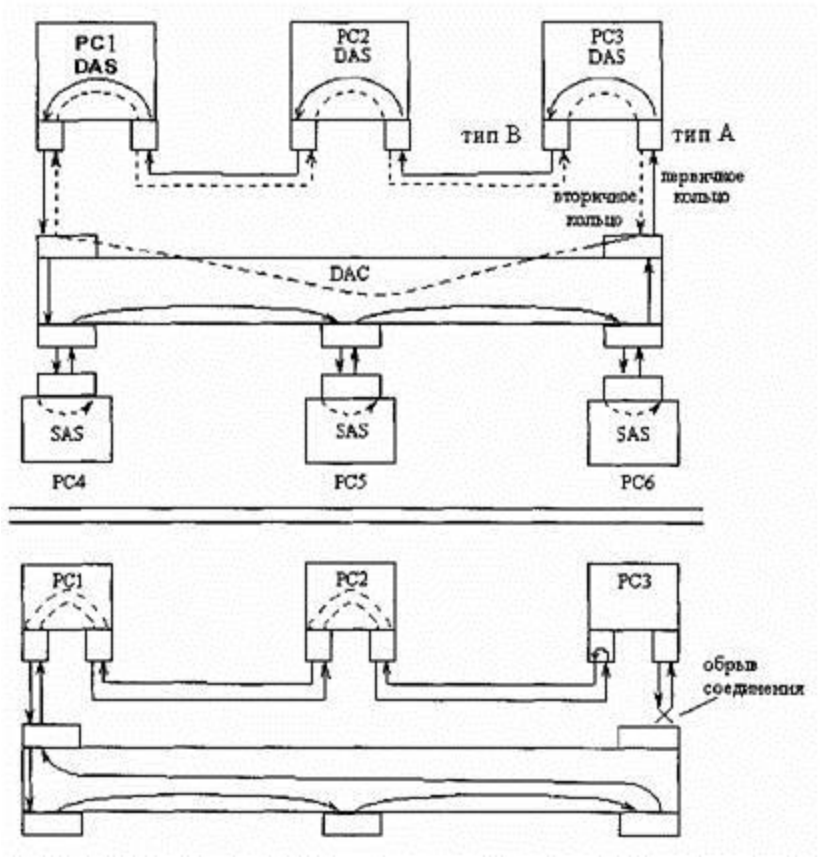


Рис. 4.13. Организация реконфигурации сети при обрыве соединения

Технология FDDI самая отказоустойчивая технология ЛВС. Отказоустойчивость обеспечивается на уровне основных протоколов. Это и самая дорогая технология LAN, и даже созданный позднее вариант реализации на витой паре не особенно её удешевил.

Областью применения технологии были магистрали между крупными сетями, например, зданиями в сети предприятия, где к кольцу FDDI подключаются отдельные сети зданий и мощные серверы, а также сети городского масштаба. И хотя технология FDDI ушла в прошлое по тем же причинам, что и Token Ring, работающие сети на её основе успешно сохранились до наших дней. Идеи по обеспечению отказоустойчивости на основе двойного кольца сейчас реализованы в ряде технологий глобальных сетей.

4.5. Технология Fast Ethernet

При переходе от процессоров Intel 286, 386 с шинами ISA (8 Мбайт/сек) и EISA (32 Мбайт/сек) к более мощным станциям с шиной PCI (133 Мбайт/сек) пропускная способность Ethernet стала недостаточной. Если раньше пропускная способность сети составляла 1/8 или 1/32 канала «память-диск», то это хорошо согласовалось с отношением объема данных передаваемых по сети и обрабатываемых на PC. Когда соотношение стало 1/133, сегменты Ethernet стали перегружаться, а реакция серверов в них значительно упала. Возникла необходимость в 100-мегобитной технологии для ЛВС, т.к. технология FDDI имела другую область применения и для ЛВС была неоправданно дорогой.

Сравнение Fast Ethernet и Ethernet

1. Уменьшился диаметр сегмента сети. Это связано с ограничением, которое налагается временем двойного оборота, поскольку скорость передачи данных увеличилась в 10 раз, значит, в 10 раз уменьшилось время передачи кадра минимальной длины. Ограничение на длину сегмента снимается при использовании коммутаторов в полнодуплексном режиме вместо концентраторов. При использовании коммутаторов ограничения на длину соединения типа адаптер-коммутатор и коммутатор-коммутатор связаны только со степенью затухания сигнала в кабеле.

2. Формат кадров не изменился.

3. Все временные параметры пропорционально уменьшаются в 10 раз (межкадровый интервал стал равен 0.96 мкс, битовый интервал — 10 нс, т.е.), но соотношение между ними не изменилось, следовательно, протокол уровня MAC не претерпел изменений.

4. Признаком свободной среды стала передача символа Idel из соответствующего избыточного кода, а не отсутствие сигнала, как в 10 Base X.

Таким образом, отличия между обычным Ethernet (802.3) и Fast Ethernet (802.3U) сосредоточены на физическом уровне.

4.5.1. Физический уровень Fast Ethernet

В качестве сред передачи в технологии Fast Ethernet используется витая пара и оптоволокно. Коаксиальный кабель был исключен по ряду причин:

- витая пара UTP 5 обеспечивает на небольших расстояниях такую же скорость передачи, как и коаксиальный кабель, но стоит дешевле;
- оптоволокно имеет полосу пропускания больше, чем коаксиальный кабель, а стоит не на много дороже, если учесть затраты на поиск и устранение неисправностей в сложной коаксиальной системе (нужно специальное оборудование для обнаружения неисправностей).

Физический уровень был разделен на несколько подуровне с дополнительными функциями. В частности, к единственному ранее уровню физического кодирования добавился уровень логического кодирования и уровень автопереговоров.

Подуровень логического кодирования преобразует поступающие от MAC уровня двоичные байты в два кода: 4B/5B и 8B/6T, которые используются для последующего физического кодирования сигналов соответственно потенциальными кодами NRZI (двух уровневый) и MLT-3 (трех уровневый). Напомним, что потенциальные коды обеспечивают наиболее узкий спектр сигналов, а это позволяет при высокой скорости передачи использовать более дешёвый кабель (с более узкой полосой пропускания).

Подуровень автопереговоров является необязательным. Он позволяет двум портам договариваться о наиболее эффективном режиме работы.

Спецификации 100 Base FX/TX

Спецификация **FX** — использует многомодовое оптоволокно 62.5/125 мкм (62.5 — внутренний диаметр, 125 — внешний диаметр).

Спецификация **TX** — использует неэкранированную витую пару пятой категории UTP 5 или экранированная витая пара STP Type 1.

Спецификации были заимствованы из технологии FDDI, которая хорошо зарекомендовала себя на практике. в ней используется метод логического кодирования 4B/5B для улучшения последующего потенциального физического кода. Избыточные запрещенные коды способствуют отбраковке ошибочных символов и увеличению отказоустойчивости.

На уровне физического кодирования при передаче по оптоволоконному кабелю используется потенциальный код NRZI (инверсный без возвращения к “0”), а для UTP категорий 5 и STP Type 1 — используется трехуровневый потенциальный код MLT – 3.

- NRZI - “+V”, “-V”;
- MLT-3 - “+V”, “-V”,“0”.

Обе спецификации предусматривают топологию – «звезда» с концентратором. Узел подключается к повторителю (так в этой технологии называют концентраторы) двумя оптоволоконными проводниками (рис. 4.18.) или двумя витыми парами (рис. 4.17.). Один проводник или пара используются для приема данных, а другой – для передачи. Приемо-передатчики заимствованы из FDDI.

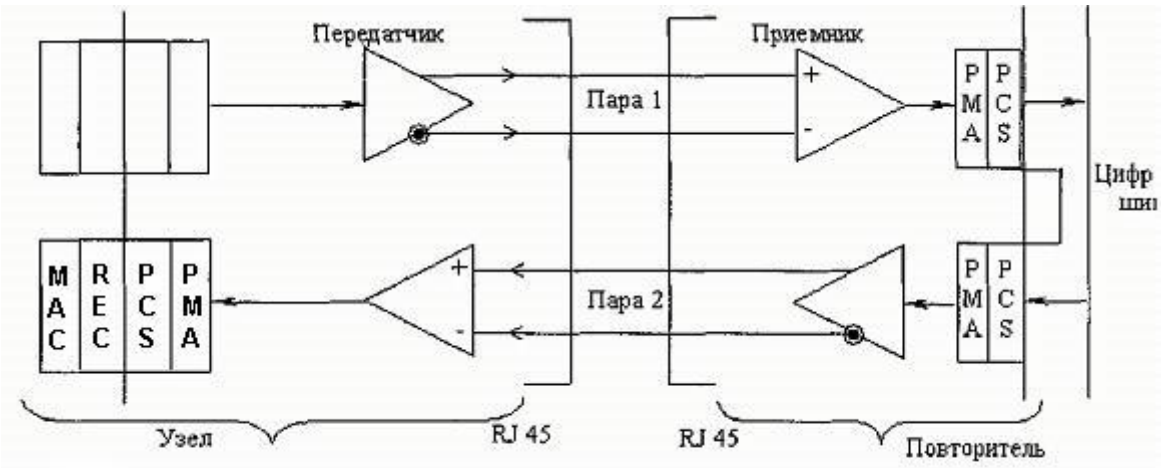


Рис. 4.17. Соединение 100Base TX

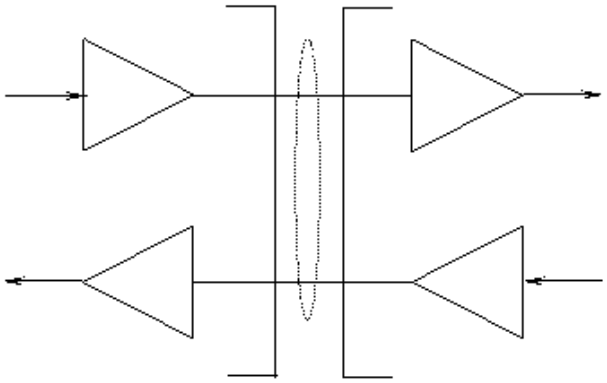


Рис. 4.18. Соединение 100Base FX

Для минимизации наводок и искажений сигналов, передаваемых по витым парам, сигналы передачи и приема для каждой витой пары поляризованы: один проводник передает положительный, а второй — отрицательный сигнал. Стандартный кабель содержит 4 витые пары. Из соображений помехозащищенности для передачи данных могут использоваться только две пары. Оставшиеся 2 витые пары данного кабеля не используются для передачи данных, а могут использоваться для передачи голоса (телефон).

Спецификация 100 Base T4

В этой спецификации используется пара категории 3 с целью применения уже проложенного в здании телефонного кабеля и кабеля 10 Base T (рис.4.19.). Может использоваться также витая пара категории 4 и 5. Поначалу спецификация получалась более дорогой, чем TX, поскольку была сложнее. И вообще, спецификация оказалось не слишком популярной из-за низкой помехозащищенности, большей зависимости от неисправностей кабеля.

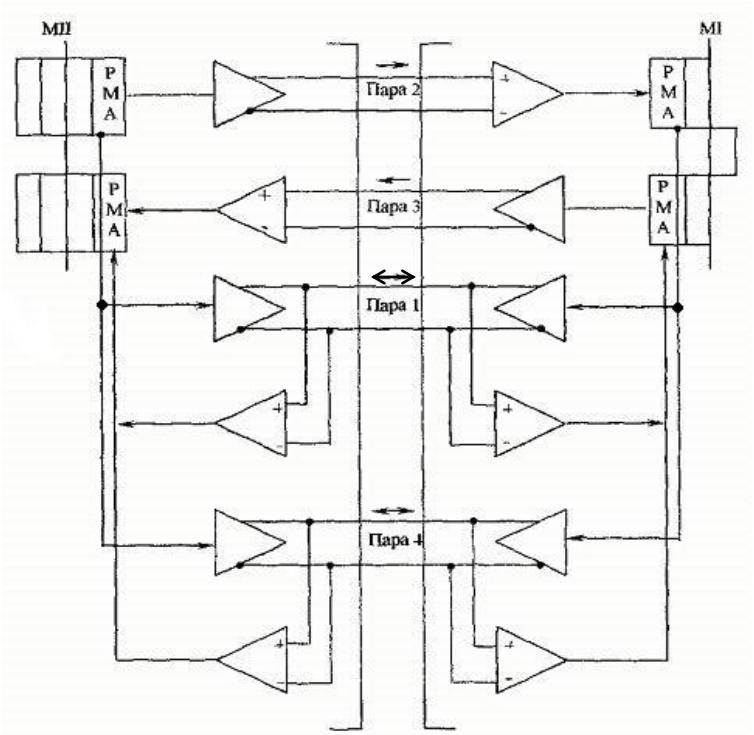


Рис. 4.19. Соединение 100Base T4

Функции обнаружения коллизий реализуются с помощью одной из однонаправленных пар, а 3 пары определяются для передачи данных в каждом направлении. Это позволяет уменьшить частоту передачи сигнала для каждой пары до получения 33,33 Мбит/с, что в сумме дает 100 Мбит/с. При этом частота синхронизации превышает 30 Мгц, которая является верхней границей полосы пропускания данного кабеля (витой пары категории 3). Поэтому в качестве метода физического кодирования используется трехуровневый код 8В/6Т. Это означает, что каждые 8 двоичных бит преобразуются в 6 троичных символов, которые используют три уровня сигнала ±3.5 V и 0. Таким образом, вместо передачи по одной витой паре 8 бит с тактовой частотой генератора 33,33МГц теперь будет передаваться 6 троичных символов с частотой 25 МГц.

Автосогласование

Процедура позволяет сетевому адаптеру, который работает на скоростях 10 и 100 Мбит/с при подключении его к концентратору или коммутатору устанавливать наиболее эффективный режим работы. Все новые коммутаторы обладают подобной способностью. Это позволяет реализовать режим Plug and Play. Выбор режима осуществляется по убыванию приоритетов:

1. полнодуплексный 100 Base TX/FX;

2. 100 Base 4T;

3. 100 Base TX;

4. полнодуплексный 10 Base T;

5. 10 BaseT.

Переговоры начинаются при включении питания, а также могут в любой момент быть запущены модули управления.

Устройство, которое начинает процесс, посылает порцию импульсов совместимых с 10 Base T, в которой содержится 8-битовое слово. Слово кодирует предлагаемый режим, начиная с самого высокого, который данное устройство может поддержать.

Если отвечающий узел может поддержать этот режим, он отвечает такой же пачкой импульсов или указывает в ответе менее приоритетный режим, но самый приоритетный из всех, которые он может поддержать. Этот режим и выбирается в качестве рабочего и переговоры заканчиваются.

Если параметр поддерживает только 10 Base T, то он не понимает запроса, а просто каждые 16 мкс посылает манчестерские импульсы проверки целостности линии связи. Интеллектуальный узел, который в ответ на свой запрос получил такие импульсы, понимает, «с кем имеет дело», и устанавливает для себя такой же режим 10 Base T.

4.5.2. Правила построения сегментов

Сегменты всех спецификаций используют физическую топологию «звезда» и логическую — «общая шина».

При построении определяется понятие **DTE** (Data Terminal Equipment) — это источник новых кадров для сегмента разделяемой среды. Это может быть адаптер, порт коммутатора или маршрутизатора, которые передают кадры в данный сегмент из другого сегмента. Повторитель передает кадр, который уже есть в сегменте и поэтому DTE не является.

Определено три типа конфигураций:

1. Соединение DTE — DTE без использования повторителя (таблица 4.4.).

Таблица 4.4. Допустимая длина кабеля в соединении DTE — DTE

Спецификация	Максимально допустимая длина соединения
100 Base Tx	100 м
100 Base Fx	412 (полудуплекс) 2 км (полный дуплекс)
100 Base T4	100 м

2. В сегменте используется один повторитель класса 1 или два класса 2 (рис.4.20.).

Повторители *класса I* поддерживают оба типа кодирования (4B/5B, 8B/6T). Могут осуществлять трансляцию логических кодов и поэтому могут иметь порты всех трех типов: Tx, Fx и T4. Этот повторитель вносит большую задержку при распространении сигнала из-за трансляции кодов.

Повторители *класса II* могут поддерживать или 4B/5B (иметь порты Tx и Fx) или 8B/6T (иметь порты типа T4). Они вносят почти вдвое меньшую задержку, чем повторители класса I. Поэтому в одном сегменте их может быть два (рис.4.21.).

Рис. 4.20. Сегмент на одном повторителе класса I

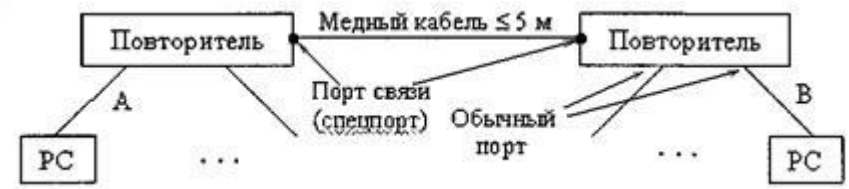


Рис. 4.21. Сегмент на повторителях класса II

Максимально допустимая длина соединений на витой паре в сегментах составляет 100м, и является физическим ограничением её полосы пропускания, связанного с затуханием передаваемого сигнала.

Ограничение длины оптоволоконных соединений в 136м связано с необходимостью устойчивого распознавания коллизий, т.е. с соблюдением PDV – времени двойного оборота кадра по сети. Поэтому существует правило, что если длина самого длинного медного кабеля в сегменте будет меньше 100м, то с каждым уменьшением этой длины на 1м (от 100м) длина самого длинного оптоволокна будет увеличиваться на 1.19м. Для двух оптоволоконных кабелей в сегменте длина кабеля А может увеличиться на столько, на сколько уменьшиться длина кабеля В, а суммарная длина А+В должна оставаться постоянной.

Как и для 10 Base X можно не пользоваться приведенными правилами и значениями, а самостоятельно рассчитывать длину кабеля в сегментах, исходя из расчёта PDV, которое должно соответствовать условию PDV≤512 битовых интервалов. Методика расчета и данные для неё приводятся в стандартах спецификации Fast Ethernet.

Повторители класса II имеют существенный недостаток. Они сложнее в производстве из-за более жестких ограничений задержек на распространение сигнала, и по этой же причине их конструктивные особенности не позволяют объединять эти повторители в стеки, с помощью которых осуществляется наращивание портов. В то же время расстояние между двумя повторителями класса II намного меньше, чем в других технологиях, а в сегменте их может быть не более двух, что во многих случаях явно не достаточно. Поэтому повторители класса II не получили распространения.

Повторители класса I, хотя и вносят большую задержку в передачу сигнала, зато допускают объединение нескольких повторителей в стек, т.е. в один объединённый повторитель (с задержкой, примерно равной задержке одного повторителя), а так же поддерживают порты всех спецификаций. На рис.4.22. показан пример топологии сети с повторителями класса I, объединенными в стек (обычно допускается объединение до 8 повторителей).

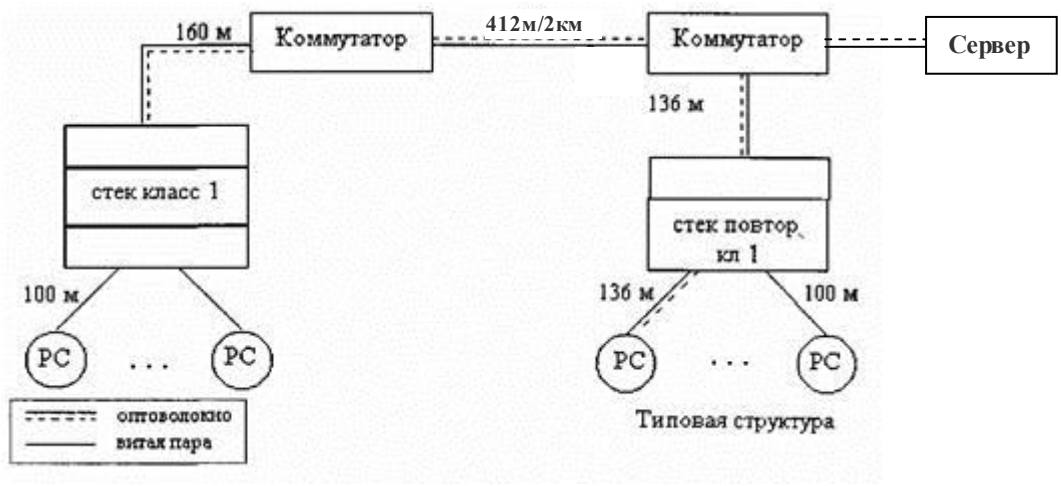


Рис. 4.22. Пример построения сети Fast Ethernet

4.7. Технология Gigabit Ethernet

Достаточно быстро после появления на рынке продуктов Fast Ethernet, сетевые интеграторы и администраторы почувствовали определенные ограничения при построении корпоративных сетей. Во многих случаях серверы, подключенные по 100-мегабитному каналу, перегружали магистрали сетей, работающие также на скорости 100 Мбит/с — магистрали FDDI и Fast Ethernet. Ощущалась потребность в следующем уровне иерархии скорости.

Летом 1996 гола было объявлено о создании группы 802-3z. для разработки протокола, максимально подобного Ethernet, но с битовой скоростью 1000 Мбит/с. Окончательно стандарт 802.3z был принят 29 июня 1998 года на заседании комитета IEEE 802.3. Работы по реализации Gigabit Ethernet на витой паре категории 5 были переданы специальному комитету 802.3ab. Этот стандарт был принят несколько позже (в июне 1999р.).

Новый стандарт старался максимально сохранить преемственность с предыдущими спецификациями 802.3 и 802.3u:

- Сохраняются все форматы кадров Ethernet.
- По-прежнему будет существовать полудуплексная версия протокола, поддерживающая метод доступа CSMA/CD, и полнодуплексная версия, работающая с коммутаторами. Сохранение недорогого решения на концентраторах для разделяемых сред позволит применить Gigabit Ethernet в небольших рабочих группах, имеющих быстрые серверы и рабочие станции.
- Поддерживаются все основные виды кабеля, используемые Ethernet и Fast Ethernet: волоконно-оптический, витая пара категории 5, коаксиальный кабель.

Тем не менее, разработчикам технологии Gigabit Ethernet для сохранения приведенных выше свойств Ethernet пришлось внести изменения не только в физический уровень, как это было в случае Fast Ethernet, но и в уровень MAC. Эти **изменения** заключаются в следующем:

В связи с ограничениями, накладываемыми методом CSMA/CD на длину кабеля, версия Gigabit Ethernet для разделяемой среды допускала бы длину сегмента всего в 25 м при сохранении размера кадров и всех параметров метода CSMA/CD неизменными. Так как существует большое количество применений, требующих диаметра сети хотя бы 200 м, разработчики технологии предприняли достаточно естественные меры, основывающиеся на известном соотношении времени передачи кадра минимальной длины и временем двойного оборота.

Минимальный размер кадра был увеличен (без учета преамбулы) с 64байт до 512байт. Теперь время двойного оборота также можно увеличить, что с учетом скорости распространения сигналов по кабелю и задержки, вносимой одним повторителем, делает допустимым диаметр сети около 200 м.

Для увеличения длины коротких кадров до требуемой в новой технологии величины, сетевой адаптер должен дополнить кадр, полем *расширения (extention)*, заполненным нулями. Это поле помещается после поля контрольной суммы, и является просто продлением времени передачи, необходимым для корректного обнаружения

коллизий. Если станции нужно передать несколько коротких кадров, то она может не дополнять их до 512 байт за счет поля Extention, а передавать несколько кадров подряд до исчерпания предела в 8192 байт (в этот предел входят все байты кадра с учётом преамбулы). Предел 8192 байт называется Burst-Length (длина монопольного режима). Если станция начала передавать кадр, и предел Burst-Length был достигнут в середине кадра, то кадр разрешается передать до конца.

В полнодуплексном режиме поля Extention и монопольный режим не используются, так как распознавать коллизии в этом режиме нет необходимости, такое понятие здесь просто отсутствует.

Структура физического уровня Gigabit Ethernet аналогична Fast Ethernet с введением необходимых измерений в каждый подуровень, включая подуровень автосогласования. Физическая топология сети – «звезда» с одним концентратором. Интерфейс MII Fast Ethernet заменен расширенным интерфейсом GMII.

4.7.1. Спецификации физического уровня

Спецификация физического уровня включают в себя 2 стандарта 802.3 z и 802.3ab.

В стандарте 802.3z определены следующие типы физической среды:

- одномодовый волоконно-оптический кабель;
- многомодовый волоконно-оптический кабель 62,5/125;
- многомодовый волоконно-оптический кабель 50/125;
- двойной коаксиальный кабель с волновым сопротивлением 75 Ом.

В основу стандартов 802.3z были положены спецификации Fiber Channel (скоростной интерфейс компьютера с периферийными устройствами, такими как RAID-массивы, находящимися на небольшом расстоянии). Это сильно ускорило процесс разработки стандартов Gigabit Ethernet и соответствующего сетевого оборудования.

Спецификации 803.z используют схему кодирования 8B/10B, заимствованную из Fiber Channel, в соответствии с которой 8 бит исходного кода представляются 10-разрядным кодом. Не используются кодовые комбинации, содержащие длинной последовательности нулей и единиц. Метод обеспечивает скорость передачи данных всего в 800 Мбит/с (битовая скорость на линии равна в этом случае примерно 1000 Мбит/с, но при методе кодирования 8B/10B полезная битовая скорость на 25% меньше скорости импульсов на линии).

Спецификация 1000 Base-LX

Для спецификации 100Base-LX в качестве источника излучения всегда применяется полупроводниковый лазерный диод с длиной волны 1300 нм (L-от Long Wavelength, то есть длинная волна).

Спецификация 1000Base-LX может работать как с многомодовым, так и с одномодовым кабелем. Предельные значения сегментов для кабелей разного типа приведены в таблице 4.6.

Стандарт 802.3z стал первым использовать на высоких скоростях в качестве источника света лазер для многомодного оптоволокна, а не обычный светодиод. Эффект «дрожания» сигнала, который составляет главную проблему такой реализации, был разрешен при помощи переопределения характеристик лазерных передатчиков, применяемых для генерации сигнала. Этот шаг был очень важен, так, как спецификация только на одномодовом оптоволокне получалась слишком дорогой.

Таблица 4.6. Диапазоны значений длины сегментов кабеля в стандарте 1000Base - LX

Тип кабеля	Полоса пропускания, МГц/км	Диапазон, м
62,5 мкм MMF	500	2-550
50 мкм MMF	400	2-550
50 мкм MMF	500	2-550
10 мкм SMF (одномодовый)	Не определено	2-5000

Стандарт предназначен для прокладки магистралей внутри зданий (по многомодному кабелю) или магистралей между зданиями в пределах кампуса по одномодному кабелю.

Спецификация 1000 Base-SX

В 1000 Base-SX оптический сигнал генерируется с помощью коротковолнового лазерного диода с длиной волны 850 нм.(S означает Short Wavelength). Спецификация ориентирована только на многомодовый кабель, хотя затухание сигнала с длиной волны 850 нм более чем в 2 раза превышает затухание сигнала с длиной волны 1300 нм на многомодовом оптоволокне (что уменьшает допустимую длину кабеля). Зато, такие диоды значительно дешевле. Они аналогичны диодам, применяем в приводах CD-ROM и проигрывателях компакт – дисков.

В таблице 4.7 приведены предельные значения диапазонов длины сегментов волоконно-оптического кабеля разного типа для стандарта 1000Base-SX:

Таблица 4.7. Длина сегментов кабеля в стандарте 1000Base-SX

Тип кабеля	Погонная полоса пропускания, МГц/км	Диапазон, м
62,5 мкм MMF	160	2-220
62,5 мкм MMF	200	2-275
50 мкм MMF	400	2-500
50 мкм MMF	500	2-550

Приведенные в таблице расстояния рассчитаны для худшего по стандарту случая полосы пропускания многомодового кабеля, находящегося в пределах 160 до 500 МГц/км. Реальные кабели обычно обладают значительно лучшими характеристиками, находящимися между 600 и 1000 МГц/км. В этом случае можно увеличить длину кабеля примерно до 800м.

Следует подчеркнуть, что **максимальные значения длина кабеля** в таблицах 4.6. и 4.7. могут достигаться только для полнодуплексной передачи данных. Для

полудуплексной передачи, исходя из времени двойного оборота, длина сегментов оптоволоконного кабеля должна быть **не более 100 м**.

Спецификация 1000 Base-CX

В качестве среды передачи данных используется высококачественный твинаксиальный кабель (Twinax) с волновым сопротивлением 150 Ом (2х75 Ом). Данные посылаются одновременно по паре проводников, каждый из которых окружен экранирующей оплеткой. При этом получается режим полудуплексной передачи. Для обеспечения полнодуплексной передачи необходимы еще две пары коаксиальных проводников. Начал выпускаться специальный кабель, который содержит четыре коаксиальных проводника, — так называемый Quad-кабель. Он внешне напоминает кабель категории 5 и имеет близкие к нему внешний диаметр и гибкость. Максимальная длина твинаксиального сегмента составляет всего 25м, поэтому это решение подходит для оборудования, расположенного в одной комнате. По существу, стандарт направлен на соединение между оборудованием, таким как кластеры серверов или соединения между коммутаторами, т.к. он значительно дешевле и проще в установке, чем оптоволокно.

Однако, поскольку был создан стандарт на витой паре категории 5, интерес к этому стандарту существенно снизился.

Спецификация 1000 Base-T

Эта спецификация определена в стандарте 802.3ab.

Как известно, каждая пара кабеля категории 5 имеет гарантированную полосу пропускания до 100 МГц. Для передачи по такому кабелю данных со скоростью 1000 Мбит/с было решено организовать параллельную передачу одновременно по всем 4-м парам кабеля. Это сразу даёт возможность уменьшить тактовую частоту передатчика до 250 МГц . Для кодирования данных можно применить 4-х уровневый код, и передавать по 2 бита информации за один такт по одной паре, что даст уменьшение тактовой частоты передатчика до 125 МГц. Но и этого недостаточно. Чтобы передавать по 3 бита за такт нужно увеличивать количество уровней кода до 8-ми, и существенно повышать мощность передатчика для компенсации помех.

Тогда поступили следующим образом, применили код PAM5, использующий 5 уровней потенциала: -2,-1, 0, +1, +2, но стали кодировать данные не отдельно на каждой линии, а сразу на всех 4-х. Теперь, если за один такт по всем четырем парам передавать 8 бит данных (по 2 бита на пару), то для их кодирования требуется 2^8 = 256 комбинаций, а код PAM5 будет обеспечивать 5^4 = 625 комбинаций. Из них отобрали 256 комбинаций с невысокой частотой переключения, а оставшиеся комбинации (с частым чередованием уровней) использовали для выделения правильных комбинаций на фоне шума. В результате, спектр сигнала на тактовой частоте 125 МГц уложился в полосу 100 МГц кабеля категории 5.

Следует отметить, что стандарт 1000 Base-T рекомендует использовать кабель UTP категории 5E, который отличается от категории 5, тем, что он более устойчив к определенным типам перекрестных помех.

Для распознавания коллизий и организации полнодуплексного режима разработчики спецификации 802.3ab применили технику, используемую при

организации дуплексного режима на одной паре проводов в современных модемах и аппаратуре передачи данных абонентских окончаний ISDN. Вместо передачи по разным парам проводов или разнесения сигналов двух одновременно работающих навстречу друг другу передатчиков по диапазону частот оба передатчика работают навстречу друг другу по каждой из 4 пар в одном и том же диапазоне частот.

Для отделения принимаемого сигнала от собственного передаваемого приемник вычитает из результирующего сигнала известный ему свой сигнал. Естественно, что это не простая операция и для ее выполнения используются специальные цифровые сигнальные процессоры – DSP (Digital Signal Processor). Такая техника уже прошла проверку практикой, но в модемах и сетях ISDN она применялась на более низких скоростях.

При полудуплексном режиме работы получение встречного потока данных считается коллизией, а для полнодуплексного режима работы — нормальной ситуацией.

4.7.2. Область применения Gigabit Ethernet

Основная область применения технологии Gigabit Ethernet – это магистрали локальных и глобальных сетей. При непосредственном подключении серверов необходимо убедится в том, что они способны поддерживать такую скорость обмена данными. Например, скорости 32-х разрядной шины PCI (33МГц) для этого недостаточно.

Напомним, что достоинством технологии Ethernet является простота, а недостатком – отсутствие в ней механизмов обеспечения качества обслуживания и отказоустойчивости, которые предполагается компенсировать дополнительным применением других средств.

- Для обеспечения хорошего качества обслуживания предполагается, что магистраль сети должна быть недогруженной. А при возрастании загрузки на магистрали для передачи трафика, чувствительного к задержкам передачи, предполагается использовать дополнительный протокол RSVP на маршрутизаторах, который позволяет резервировать полосу пропускания каналов на всём маршруте следования такого трафика. Для коммутаторов предлагается стандарт IEEE 802.1p назначения приоритетов кадрам данных.
- Отсутствие встроенных механизмов обеспечение отказоустойчивости предполагается компенсировать наличием таких механизмов в других протоколах. Например, поиска альтернативных путей в протоколах маршрутизации или поддержки резервных связей (Spanning Tree) в коммутаторах.

4.8. Технология 10G Ethernet

Стандарт определяет только полнодуплексный режим работы и предназначается для использования с коммутаторами, а концентраторы в нём не предусмотрены.

Стандарт 802.3ae описывает несколько новых спецификаций физического уровня на оптоволокне, которые взаимодействуют с уровнем MAC с помощью нового варианта подуровня согласования. Этот подуровень обеспечивает для всех спецификаций единый интерфейс XGMII – расширенный интерфейс независимого доступа к гигабитной среде,

который предусматривает параллельный обмен четырьмя байтами, образующими четыре потока данных.

Существует три группы спецификаций, которые отличаются способом кодирования данных: 10GBase-X (8B/10B), 10GBase-R и 10GBase-W (64B/66B). Например, в группе 10GBase-X в настоящее время одна спецификация 10GBase-LX4. Обозначение указывает, что для передачи данных применяется длинноволновой лазерный диод в диапазоне длин волн 1310 нм. Для организации дуплексной передачи используется 2 оптоволокна. Информация в каждом направлении передаётся на 4-х длинах волн в одном оптоволокне (техника мультиплексирования WDM). Каждый из 4-х потоков интерфейса XGMII передаётся со скоростью 2,5 Гбит/с. Максимальное расстояние между передатчиком и приёмником равно 200–300м для многомодового оптоволокна (в зависимости от полосы пропускания), а для одномодового – 10км.

В 2006г. была принята спецификация 10GBase-T для неэкранированной витой пары категории 6 (максимальная длина кабеля 55м) и 6а (максимальная длина кабеля 100м).

4.9. Беспроводные локальные сети. Стандарт IEEE 802.11

Беспроводные сети сегодня рассматриваются как дополнение, а не замена проводным сетям. Основными областями применения беспроводных сетей являются:

- Организация доступа в ЛВС или Интернет при отсутствии проводного канала от здания;
- Организация доступа в аэропортах, вокзалах, гостиницах и т.д.;
- Организация ЛВС в исторических зданиях с оригинальным интерьером;
- Организация быстрого развертывания временных ЛВС, например, при проведении конференций;
- Организация мобильных ЛВС, когда пользователь перемещается по территории предприятия.

Они имеют следующие преимущества:

- быстрота и легкость разворачивания и модернизации;
- мобильность пользователей.

К недостаткам беспроводных сетей следует отнести:

- действие многочисленных техногенных и атмосферных помех;
- ж/б стены зданий являются препятствием для радио сигнала;
- неустойчивая, динамически меняющаяся зона покрытия.

Для снижения влияния помех на полезный сигнал применяются методы расширения спектра сигнала и прямая коррекция ошибок (FEC), а также методы исправления с помощью повторной передачи данных на канальном уровне.

Совместимость продуктов различных производителей гарантируется независимой организацией, которая называется Wireless Ethernet Compatibility Alliance (WECA). В настоящее время членами WECA являются более 80 компаний, в том числе такие известные производители, как Cisco , Lucent , 3Com , IBM , Intel, Apple, Compaq, Dell , Fujitsu , Siemens , Sony , AMD и пр.

4.9.1 Протоколы стандарта IEEE 802.11

Как и все стандарты локальных сетей IEEE 802, стандарт IEEE 802.11 работает на двух нижних уровнях модели ISO/OSI, физическом и канальном уровне (рис. 4.25).

Рис. 4.25. Уровни модели ISO/OSI и их соответствие стандарту 802.11

Канальный уровень IEEE 802.11, как и у всех технологий ЛВС, состоит из двух подуровней: из общего для всех технологий уровня LLC и специфического для данной технологии уровня MAC. Стандарт IEEE 802.11 поддерживает такую же 48-битовую MAC- адресацию, как и другие технологий ЛВС, что позволяет легко объединять беспроводные и проводные сети.

Уровень MAC IEEE 802.11 выполняет ряд дополнительных функций по сравнению технологиями проводных сетей, которые будут рассмотрены ниже.

На физическом уровне существует несколько спецификаций, отличающихся скоростью и дальностью передачи, что обеспечивается различными (и достаточно сложными) методами кодирования данных. Все спецификации работают с общим уровнем MAC, хотя некоторые временные параметры этого уровня зависят от типа физических спецификаций.

4.9.2 Режимы работы 802.11

Стандарт IEEE 802.11 определяет два типа оборудования – клиент, который обычно представляет собой компьютер, укомплектованный беспроводным сетевым адаптером (Network Interface Card, NIC), и базовую станцию, которая называется в технологии *точкой доступа* (Access point, AP). Точка доступа выполняет роль концентратора для беспроводных станций и роль моста или маршрутизатора между

беспроводной и проводной сетью (аналогично концентратору и мосту/маршрутизатору, которые соединены последовательно).

Стандарт IEEE 802.11 определяет два режима работы сети: режим самоорганизующейся сети – «Ad-hoc» и режим клиент/сервер (или режим инфраструктуры – infrastructure mode).

Режим инфраструктуры

В режиме клиент/сервер беспроводная сеть состоит из одной точки доступа, подключенной к проводной сети, и некоторого количества беспроводных станций. Такая конфигурация носит название базового набора служб (Basic Service Set, BSS).

Два или более BSS, образующих единую подсеть, формируют расширенный набор служб (Extended Service Set, ESS). Точки доступа могут быть связаны между собой либо беспроводной средой (радио или инфракрасной) либо проводной средой. В задачи ESS входит объединение станций, принадлежащих разным BSS. В этом случае станция – отправитель передаёт данные своей точке доступа, которая пересылает их точке доступа станции – получателя. ESS-сеть обеспечивает станциям мобильность – они могут перемещаться из одной BSS в другую. Процедура незаметного для клиента перемещения между точками доступа называется *хэндовером* (hand-over), она обеспечивается функциями уровня MAC рабочих станций и точек доступа.

Поскольку беспроводным станциям чаще всего требуется доступ к ресурсам проводной локальной сети, режиме инфраструктуры является наиболее распространённым.

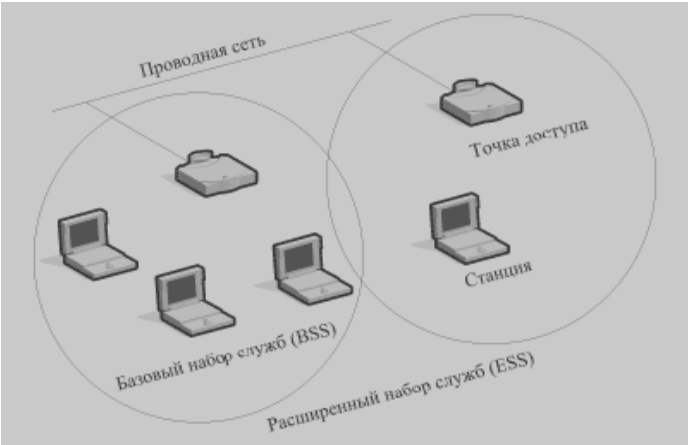


Рис. 4.26. Архитектура сети "клиент/сервер"

Режим "Ad-hoc"

Режим "Ad-hoc" или режим самоорганизующейся сети – это простая сеть, в которой связь между многочисленными станциями устанавливается напрямую, без использования точки доступа (рис. 4.27). Режим полезен в том случае, когда инфраструктура беспроводной сети не сформирована (например, отель, выставочный зал, аэропорт).

Рис. 4.27. Архитектура сети "Ad-hoc"

Режим WDS – распределенная беспроводная сеть

Режим WDS (Wireless Distribution System) является разновидностью режима инфраструктура, в котором точки доступа связаны между собой беспроводной средой. Все точки доступа WDS сети должны быть настроены на использование одного и того же частотного канала, метода шифрования и ключа шифрования. В то же время допускается использование различных имён сетей (Service Set Identifier, SSID).

WDS может обеспечивать два режима для соединения точек доступа:

- режим беспроводного моста;
- режим беспроводного повторителя.

Режим беспроводного моста служит для беспроводного объединения сегментов сети там, где прокладка проводного соединения затруднена (рис. 4.28 и рис. 4.29).

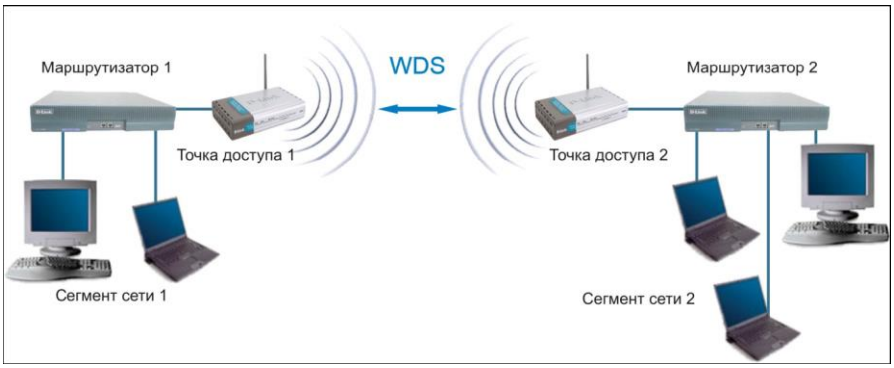


Рис. 4.28. Мостовой режим в пределах здания

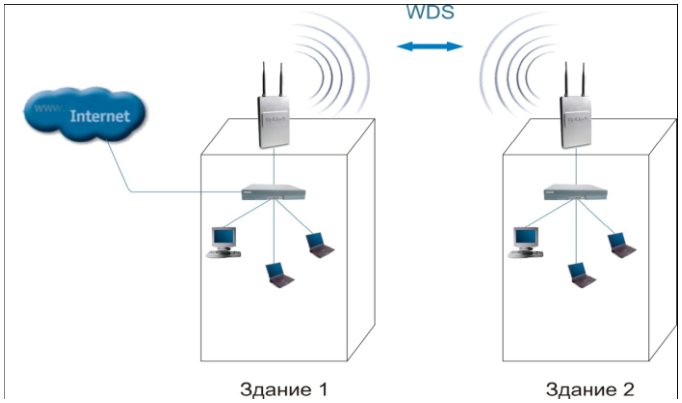


Рис. 4.29. Мостовой режим между зданиями

В режиме беспроводного моста устройства сообщаются между собой и не обеспечивают доступа для других беспроводных станций или клиентов.

Режим беспроводного повторителя (концентратора) позволяет точкам доступа работать как с другими точками доступа, так и с клиентскими адаптерами (рис.4.30). Реализуется схема аналогичная проводному соединению двух сегментов на концентраторах.

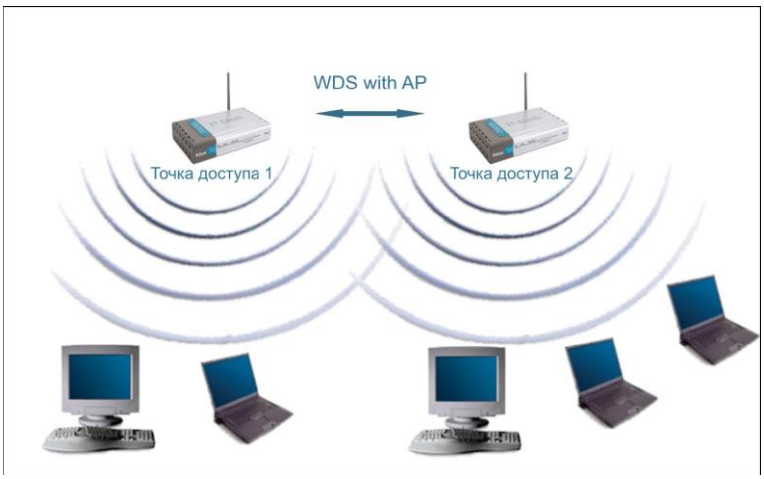


Рис. 4.30. WDS в режиме повторителя

Недостатком режима WDS является уменьшение скорость работы сети в связи с увеличением её загруженности аналогично много сегментной сети на концентраторах Ethernet, так как для связи точек используется один канал.

4.9.2 Уровень MAC IEEE 802.11

Уровень MAC IEEE 802.11 похож на MAC стандарта IEEE 802.3 Ethernet, который также поддерживает метод случайного доступа к общей разделяемой среде. Однако, в беспроводных сетях уровень MAC выполняет больше функций, чем в проводных. Эти функции включают:

- доступ к разделяемой среде передачи данных;
- фрагментация больших пакетов;
- обеспечение мобильности станций при наличии нескольких точек доступа;
- обеспечение безопасности при передаче данных.

Ещё раз отметим, что особенности всех функций, кроме мобильности, связаны с высоким уровнем помех и общедоступностью разделяемой среды передачи.

Фрагментация пакетов. Фрагментация пакетов позволяет разбивать большие пакеты на более маленькие при передаче по радиоканалу, что полезно в загруженных сетях или при наличии значительных помех, так как для коротких пакетов уменьшается вероятность их повреждения и временные затраты на повторную передачу. Каждый пакет получает свою контрольную сумму CRC. Поскольку сборкой фрагментированных пакетов занимается MAC уровень, то для вышележащих протоколов этот процесс не заметен.

4.9.3 Метод доступа к разделяемой среде

В сетях IEEE 802.11 предусмотрено два режима доступа к разделяемой среде: *распределенный режим* DCF (Distributed Coordination Function) и *централизованный режим* PCF (Point Coordination Function).

Распределенный режима доступа DCF

Как было рассмотрено ранее, для сетей IEEE 802.3 Ethernet используется алгоритм случайного доступа CSMA/CD – метод коллективного доступа с опознаванием несущей и **обнаружением коллизий**. Метод определяет способы, с мощью которых станция Ethernet проверяет занятость среды перед доступом к ней, а также способы обнаружения и обработки коллизий, которые возникают при пытке нескольких устройств начать передачу данных одновременно. Чтобы обнаружить коллизию, станция должна обладать способностью и передавать и принимать данные (прослушивать среду) одновременно.

В стандарте IEEE 802.11 подобное невозможно, так как собственный передатчик будет заглушать принимаемый сигнал, т.е. станция не может обнаружить коллизию во время передачи данных. Поэтому распределенный режим IEEE 802.11 использует алгоритм случайного доступа, который называется ***CSMA/CA*** (Carrier Sense Multiple Access with Collision Avoidance) или метод коллективного доступа **с предотвращением коллизий**.

Во-первых, CSMA/CA косвенно обнаруживает коллизию с помощью явного подтверждения пакета (ACK), что означает, что принимающая станция посылает ACK пакет для подтверждения того, что пакет получен неповреждённым. Если передающая станция не получила в течение таймаута квитанцию (пакет ACK), она считает, что произошла коллизия, и будет передавать этот пакет данных снова в следующем цикле доступа.

Во-вторых, CSMA/CA пытается уменьшить вероятность коллизий.

Станция, желающая передать кадр данных, прослушивает среду, и с момента её освобождения ожидает стандартную межкадровую паузу, а затем, если среда ещё свободна, начинает отсчитывать тайм слоты фиксированной длины. Кадр можно начать передавать только в начале тайм слота. Номер тайм слота L для передачи выбирается случайным образом из интервала [0, CW] (CW-Contention Window). В начале каждого тайм слота станция проверяет среду. Если во всех L слотах (например, пяти) среда будет свободна, станция начинает передачу. Если же в начале очередного слота (например, третьего) среда окажется занятой, то станция начнет процедуру доступа заново, но теперь в качестве L выберет то число слотов, которое ей осталось ожидать в прошлом цикле доступа (в нашем примере L=5-2=3). То есть в каждом следующем цикле время ожидания доступа сокращается.

Размер тайм слота зависит от способа кодирования сигнала. Его длительность должна быть больше времени распространения сигнала между двумя наиболее удалёнными станциями сети плюс время, необходимое станции на проверку занятости среды. С помощью введения тайм слотов исключаются ситуации, часто возникающие в Ethernet, когда коллизия происходит потому, что одна станция начала передачу, а до другой он ещё не дошёл, и она считает среду свободной.

Таким образом, в методе CSMA/CA коллизия может произойти только тогда, когда несколько станций случайно выберут одинаковый номер тайм слота для передачи, что маловероятно. Но, если переданный кадр всё же попадёт в коллизию, то отправитель не получит на него квитанцию и будет пытаться передать кадр снова. При каждой повторной попытке передачи одного и того же кадра интервал, из которого выбирается номер слота, увеличивается вдвое, а после N (в стандарте не фиксировано) неудачных попыток передача прекращается.

Для определения того, является ли канал свободным, используется алгоритм оценки чистоты канала (Channel Clearance Algorithm, ***CCA***). Его суть заключается в измерении энергии сигнала на антенне и определения мощности принятого сигнала. Если мощность принимаемого сигнала будет ниже определённого порога, то канал считается свободным.

Таким образом, алгоритм CSMA/CA предоставляет способ разделения среды передачи по радиоканалу. Механизм явного подтверждения эффективно решает проблемы помех, но и добавляет некоторые накладные расходы, которых нет в IEEE 802.3. Поэтому сети IEEE 802.11 всегда будут работать медленнее, чем эквивалентные им локальные сети Ethernet.

Проблема "скрытой точки"

Ещё одна специфичная проблема MAC-уровня – это проблема "скрытой точки", которую иллюстрирует рис.4.31, когда две станции могут "слышать" точку доступа, но не могут "слышать" друг друга. Разновидностью этой проблемы может быть проблема "скрытого терминала", когда две станции могут "слышать" друг друга, но есть третья станция, которая может слышать только одну из них в силу большого расстояния или преград.

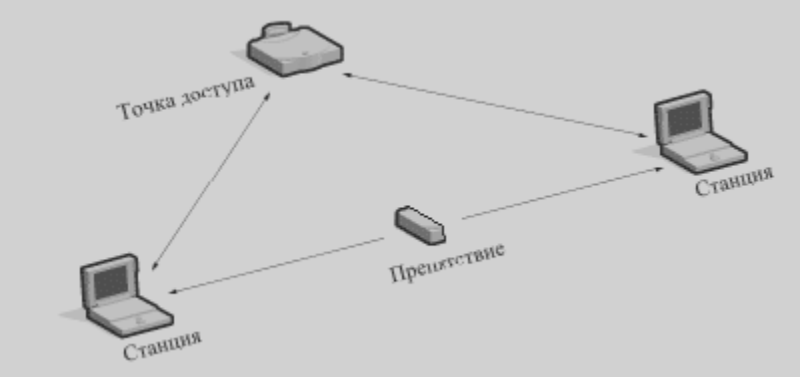


Рис. 4.31. Иллюстрация проблемы "скрытой точки".

Для решения этой проблемы в MAC уровень IEEE 802.11 добавлен необязательный протокол RTS/CTS (Request to Send/Clear to Send). Когда используется этот метод, посылающая станция, начиная передачу кадра в определенном слоте, вместо кадра данных сначала отправляет получателю короткий кадр запроса RTS и ждёт от неё ответа с кадром CTS – подтверждения готовности приёма. После чего станция – отправитель посылает кадр данных. Кадр CTS должен оповестить о захвате среды те станции, которые находятся вне зоны сигнала станции – отправителя (скрытые терминалы), но в зоне досягаемости станции – получателя. Это позволяет передающей станции передать кадр данных и получить на него ACK квитанцию без коллизий.

Аналогичный результат достигается и тогда, когда станции взаимодействуют через точку доступа (рис.4.31), которую «слышат» все терминалы.

Так как протокол RTS/CTS, временно резервируя среду, несколько замедляет обмен данными в сети, он обычно используется только для пакетов самого большого размера, для которых повторная передача становится накладной, или при большой загруженности сети, когда вероятность возникновения коллизий возрастает.

Централизованный режим доступа PCF

Режим может использоваться только при наличии в сети точки доступа и обеспечивает приоритетное обслуживание трафика. Чтобы воспользоваться режимом станция при подключении к сети должна послать соответствующий запрос точке доступа. Обычно приоритетный режим необходим станциям, желающие передавать чувствительный к задержкам синхронный трафик. Точка доступа играет роль арбитра среды.

По общим правилам после освобождения среды каждая станция должна ожидать межкадровую паузу. Пауза имеет 3 значения (рис.4.32)

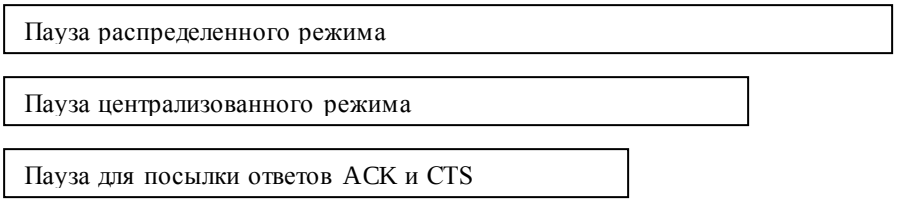


Рис. 4.32 Длительность стандартных межкадровых пауз в стандарте 802.11

Если станция должна отправить квитанцию или подтверждение готовности к приёму данных, она ожидает минимальную паузу и, таким образом, получает наивысший приоритет в захвате среды. Арбитр ожидает более длительную паузу централизованного режима и посылает всем станциям кадр о его начале. Затем арбитр по очереди опрашивает все станции, подписавшиеся на этот режим. Получив кадр опроса, станция отвечает кадром подтверждения и, если имеет данные на передачу, то одновременно посылает кадр данных. После окончания периода работы централизованного режима арбитр посылает всем станциям кадр оповещения. После получения этого кадра, остальные станции ожидают паузу распределенного режима и начинают работать в режиме DCF.

Для того, чтобы станции, желающие передавать асинхронный трафик в режиме DCF, не ожидали слишком долго, максимальное время режима PCF ограничено, т.е. временные промежутки для работы в режиме PCF и в режиме DCF распределяются равномерно. В больших сетях режим PCF становится чрезвычайно неэффективным.

4.9.4 Физический уровень IEEE 802.11

В базовом стандарте IEEE 802.11 на физическом уровне определены: один метод передачи в инфракрасном диапазоне и два широкополосных радиочастотных метода.

Метод передачи в инфракрасном диапазоне (IR)

Реализация этого метода в стандарте IEEE 802.11 основана на излучении ИК передатчиком (лазерным или светодиодом) ненаправленного (diffuse IR) сигнала.

Стандарт предусматривает три варианта распространения излучения: направленную антенну, отражения от потолка и фокусное направление излучения.

Фокусное направленное излучение предназначено для организации двухточечной связи, например, между зданиями. Основной недостаток здесь – зависимость качества передачи от погодных условий (ИК лучи сильно поглощаются туманом, снегом и дождем). Приём отраженных от потолка сигналов является удобным решением, но при этом требуется потолок, отражающий ИК – излучение в заданном диапазоне длин волн 850 – 950 нм. Так как ИК лучи не проникают через стены, область покрытия ЛВС ограничивается зоной прямой видимости (с радиусом в 10 метров).

В стандарте поддерживаются две скорости передачи данных – 1 и 2 Mbps, которые отличаются используемыми методами модуляции и кодирования данных.

Радиочастотные методы

Радиочастотные методы работают в микроволновом диапазоне 2,4 ГГц (в полосе 2,4-2,483 GHz), который в большинстве стран не лицензируется.

Технологии широкополосного сигнала, используемые в этих методах, увеличивают помехоустойчивость передаваемых данных, позволяют снизить мощность передатчиков, позволяют многим несвязанным друг с другом устройствам разделять одну полосу частот с минимальными помехами друг для друга.

Стандарт IEEE 802.11 предусматривал два метода передачи радиосигнала с расширением спектра: *метод прямой последовательности* (Direct Sequence Spread Spectrum ─ DSSS) и *метод частотного расширения спектра* (Frequency Hopping Spread Spectrum ─ FHSS).

При использовании радиочастотных методов сеть может состоять *из сот* (в каждой соте *свой радиоканал*). Каждый радиоканал представляет собой разделяемую среду передачи данных для определённой группы клиентов с рассмотренным ранее методом доступа к ней. Чтобы соседние соты не создавали друг другу помех, их каналы желательно назначать максимально отличающимися по характеристикам каждой спецификации. В одних спецификациях это будут разные частотные диапазоны, в других – разные кодовые последовательности и т.д. (рис. 4.33).

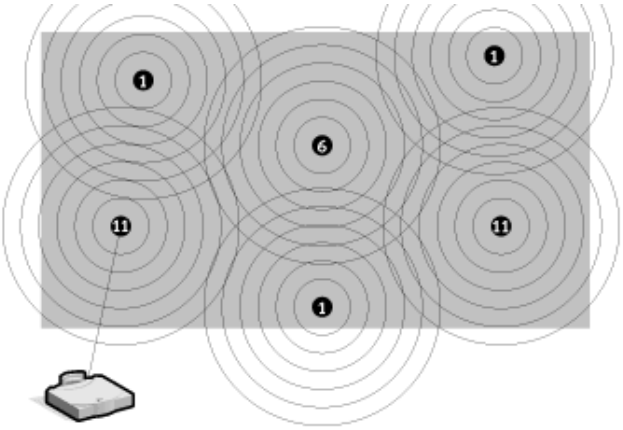


Рис. 4.33. Подключение к соте и иллюстрация правильного назначения каналов для точек доступа

Когда клиент IEEE 802.11 попадает в зону действия одной или нескольких точек доступа, он на основе мощности сигнала и наблюдаемого значения количества ошибок автоматически выбирает одну из них и подключается к ней. Как только клиент получает подтверждение от точки доступа, он настраивается на её радиоканал. Время от времени клиент проверяет все каналы IEEE 802.11, чтобы посмотреть, не предоставляет ли другая точка доступа более качественное обслуживание (вследствие перемещений пользователя, изменения радиочастотных характеристик здания, увеличения загруженности первоначальной точки доступа). Если такая точка доступа находится, то станция подключается к ней, перенастраиваясь на её радиоканал.

Метод FHSS

При использовании метода частотных скачков полоса 2,4 ГГц делится на 79 подканалов по 1 МГц. Отправитель и получатель согласовывают схему переключения подканалов (на выбор имеется 22 таких схемы), и данные посылаются последовательно по различным подканалам с использованием этой схемы. Каждая передача данных в сети IEEE 802.11 происходит по разным схемам переключения, а сами схемы разработаны таким образом, чтобы минимизировать шансы того, что два отправителя будут использовать один и тот же подканал одновременно.

Для исключения взаимовлияния в соседних сотах могут применяться непересекающиеся последовательности частот.

В качестве модуляции применяется двухуровневая (2 частоты) частотная модуляция FSK, что позволяет достичь скорости передачи данных 1 Mbps, или четырехуровневая FSK – для скорости 2 Mbps.

Метод FHSS дешев и прост в реализации, однако ограничен максимальной скоростью 2 Mbps. Это ограничение вызвано тем, что весь диапазон 2,4 ГГц использован под 1 МГц- вые каналы, а с увеличением скорости должно происходить более частое переключение каналов, что, в свою очередь, приводит к увеличению накладных расходов.

Метод DSSS

Метод DSSS делит диапазон 2,4 ГГц на 14 частично перекрывающихся каналов. Для того, чтобы несколько каналов могли использоваться одновременно в одном и том же месте, необходимо, чтобы они отстояли друг от друга на 25 МГц (не перекрывались), для исключения взаимных помех. Таким образом, в одном месте может одновременно использоваться максимум 3 канала.

Данные пересылаются с использованием одного из этих каналов, без переключения на другие каналы. Чтобы компенсировать посторонние шумы, используется 11-ти битная расширяющая последовательность Баркера – {10110111000}. Каждый бит данных пользователя преобразуется в 11 бит (называются чипами) передаваемых данных, так что тактовая частота передатчика, а, следовательно, и спектр сигнала увеличивается в 11 раз. Двоичная «1» заменяется прямой последовательностью (10110111000), а «0» – инверсной (01001000111). Приемник, сравнивая известную последовательность с поступающими данными, легко находит в них начало последовательности. Действительно, если сравнивать последовательность Баркера с

такой же последовательностью, но сдвинутой на 1 бит влево или вправо, то будет получено меньше половины совпадающих значений битов. Значит, даже при искажении нескольких битов приемник с большой долей вероятности правильно определит начало последовательности, а значит правильно прочитать полученную информацию.

Высокая избыточность для каждого бита позволяет также, не снижая надёжность передачи, значительно уменьшить мощность передаваемого сигнала. Даже если часть сигнала будет утеряна (помеха обычно искажает только определенные частоты спектра сигнала), он в большинстве случаев всё равно будет восстановлен. Тем самым минимизируется число повторных передач данных.

При передаче последовательности чипов для достижения скорости 1 Mb/s применяется двухпозиционная фазовая манипуляция (BPSK), т. е. один фазовый сдвиг на каждый чип. Для достижения скорости 2 Mb/s применяется квадратурная фазовая манипуляция (QPSK) – с помощью четырех сдвигов фаз два исходных чипа передаются за один такт.

Спецификация IEEE 802.11b

Основное дополнение, внесённое спецификацией в основной стандарт – это поддержка скоростей передачи данных – 5,5 и 11 Mb/s. Спецификация IEEE 802.11b определяет только один метод передачи – DSSS. Таким образом, сети IEEE 802.11b могут быть совместимы с системами IEEE 802.11 DSSS, но не с IEEE 802.11 FHSS. Для увеличения скорости передачи была использована более совершенная техника кодирования CCK (Complementary Code Keying). Здесь вместо кода Баркера применяется последовательность кодов, называемых дополнительными (Complementary Sequences). Она состоит из 64 8-чиповых кодирующих слов, и позволяет одним словом закодировать до 6 бит. Затем код CCK модулируется с помощью схемы QPSK, точно такой же, как и в методе IEEE 802.11 DSSS. Это добавляет к символу еще два бита. Символы посылаются с частотой 1,375 Msps, что и дает в результате пропускную способность 11 Mb/s.

Стандарт IEEE 802.11b позволяет автоматически изменять скорость передачи данных в диапазоне 11 Mb/s – 1 Mb/s в зависимости от свойств радиоканала (повышение уровня помех, или удаление пользователя на большое расстояние).

Спецификация 802.11a

Спецификация IEEE 802.11a предусматривает увеличение скорости передачи данных до 54 Mb/s, но, для этого задействуется более ёмкий информационный канал в другом диапазоне частот (полоса 5,15–5,825 GHz). Кроме этого применяется принципиально другой метод передачи, называемый *ортогональным частотам мультиплексированием* (Orthogonal Frequency Division Multiplexing – OFDM) и прямая коррекция ошибок FEC. Схемы последующей фазовой и амплитудно-фазовой модуляции с разным количеством состояний одного (фаза) и двух (амплитуда и фаза) информационных параметров сигнала обеспечивают скорости передачи 6 Mb/s (BPSK), 12Mb/s (QPSK), 24Mb/s (16QAM),…, 54 Mb/s (64QAM).

Как легко видеть, стандарт IEEE 802.11a оказался не совместимым ни с вариантом IEEE 802.11b, ни с базовым беспроводным стандартом IEEE 802.11, кроме того, оборудование для данного диапазона частот оказалось существенно дороже и сам диапазон в ряде стран подлежит лицензированию.

Метод OFDM

При использовании этого метода битовый поток делится на подпотоки. Каждый подпоток модулирует определенную несущую частоту, которая обычно выбирается по принципу: f0, 2f0, 3f0, и т.д. Модуляция выполняется с помощью обычных методов PSK или FSK. Перед передачей все несущие сворачиваются в общий сигнал путем быстрого преобразования Фурье. Спектр такого сигнала примерно соответствует спектру сигнала, получаемого на одной несущей. После передачи из общего сигнала путем обратного преобразования Фурье выделяются несущие подканалы, а из них – битовые подпотоки. Выигрыш в разделении исходного битового потока на несколько низкоскоростных подпотоков проявляется в том, что увеличивается временной интервал между отдельными символами кода. А это ведёт к уменьшению эффекта межсимвольной интерференции, которая проявляется из-за многолучевого распространения электромагнитных волн (отраженная от некоторого препятствия и запоздавшая волна предыдущего сигнала может наложиться на прямую волну следующего сигнала и исказить его).

Стандарт IEEE 802.11g и IEEE 802.11n

Стандарт IEEE 802.11g использовал частотный диапазон 2,4 ГГц и схему мультиплексирования OFDM, что позволило достичь пропускной способности 54 Mb/s. Для обеспечения совместимости с сетями IEEE 802.11b он предусматривал поддержку механизма кодирования CCK/Barker и сразу же был благосклонно принят рынком.

Целью нового стандарта IEEE 802.11n является достижение реальной скорости передачи данных пользователя со скоростью 100Mb/s и выше. Такая скорость достигается за счёт использования *технологии множественных антенн* (MIMO), ортогонального частотного мультиплексирования (OFDM) и использования частотного диапазона 5ГГц. MIMO (Multiple Input, Multiple Output — много входов, много выходов) предусматривает одновременную передачу и приём нескольких информационных потоков данных по одному радио каналу, а также многолучевое отражение, которое уменьшает вероятностью влияния помех и потерь данных. Количество одновременно передаваемых и принимаемых потоков зависит от конфигурации антенн для передачи и приёма информации. Максимальная теоретическая скорость 600Mb/s может быть достигнута с конфигурацией антенн 4×4 при использовании техники *пространственного мультиплексирования* (ПМ). Техника ПМ состоит в том, что несколько передатчиков и несколько приёмников, благодаря определённому пространственному разнесению их антенн, создают несколько относительно уникальных каналов распространения внутри одного частотного диапазона, называемых пространственными потоками.

В таблице 4.8 приведены основные характеристики стандартов IEEE 802.11

Таблица 4.8. Основная характеристика стандартов IEEE 802.11

Стандарт	802.11			802.11a	802.11b	802.11g	802.11n
Максимальная скорость передачи, Мбит/с	1 и 2	1 и 2	1 и 2	54	11	54	150(1x1)-600(4x4)
Рабочая частота, ГГц	2.4	2.4	ИК волны 850 нм	5	2.4	2.4	2.4 и 5
Реальная пропускная способность на расстоянии 6–18 м,	Нет данных	Нет данных	Нет данных	15 – 20	4 – 6	15 – 20	80 и >

Mb/s							
Типичный радиус покрытия в помещении, м	≤ 100	≤ 100	10 – в помещении	45	23	45	Около 250
Схема кодирования	Метод частотных скачков FHSS	Широкополосная модуляция с прямым расширением спектра (DSSS)		Мультиплексирование с разделением по ортогональным частотам (OFDM)	Широкополосная модуляция с прямым расширением спектра (DSSS с CCK)	Мультиплексирование с разделением по ортогональным частотам (OFDM)	Мультиплексирование с разделением по ортогональным частотам (OFDM)
Совместимость	Несовместим с другими	Совместим с продуктами 11b/g,	Не совместим с другими	Не совместим с другими	Совместим с продуктами 11g, если они работают в смешанном режиме	Обратно совместим с 11b	Обратно совместим с 802.11a/b/g.

4.9.5. Обеспечение безопасности

В беспроводных сетях данные передаются с помощью радиосигналов, и всё, что нужно для их перехвата в незащищённой системе – это компьютер, оснащённый беспроводным адаптером и свободно доступным ПО. Не обязательно даже входить в здание, где расположена беспроводная ЛВС. Ввиду очевидности этого факта для защиты данных в стандарте IEEE 802.11 был предусмотрен механизм WEP (Wired Equivalent Privacy), который базировался на шифровании. WEP работал на канальном уровне модели OSI и использовал для шифрования 40/64-разрядный ключ, что оказалось явно недостаточным. Другая проблема заключалась в том, что когда беспроводный клиент обращался к шлюзу для доступа к беспроводной ЛВС, протокол выполнял аутентификацию (определение) устройства, а не пользователя. Протокол WEP постоянно подвергался критике и был абсолютно неприемлем для корпоративных сетей.

Недостатки WEP были устранены в новом протоколе WPA (Wi-Fi Protected Access) и в принятом в последствие стандарте IEEE 802.11i.

В WPA были устранены такие недостатки WEP, как слабое шифрование и отсутствие механизма аутентификации пользователя.

В спецификацию WPA добавлено динамическое распределение ключей, уникальные главные ключи для каждого пользователя и каждой сессии, а также уникальные ключи шифрования для каждого пакета. Этот подход предусматривает использование для аутентификации центрального сервера, такого, как RADIUS (Remote Access Dial-In User Service). Спецификация использует средства надёжного шифрования с помощью 128-разрядных ключей и протокола TKIP (Temporal Key Integrity Protocol – протокол временного обеспечения целостности важнейших данных). Такое сочетание технологий защищает конфиденциальность и целостность (защита от подмены или подделки перехваченных пакетов) пересылаемых по беспроводной сети данных, дополнительно гарантируя, что только авторизованные пользователи получают доступ к сети.

Наконец, в 2004 г. был принят стандарт IEEE 802.11i, который включает в себя многие из возможностей спецификации WPA. Некоторые существенные изменения стандарта IEEE 802.11i в сравнении с WPA приводят к улучшению передачи и качества

шифрования. Стандарт IEEE 802.11i также предлагает кэширование ключей, для ускорения повторного подключения к серверу при возвращении пользователя. Более того, он предоставляет средства предварительной идентификации для обеспечения быстрого хендовера между точками доступа в сети.

Достаточно новый протокол WPS («синяя кнопка») был призван оказать помощь неопытным пользователям при осуществлении настроек сети. WPS автоматически обозначает имя сети и задает параметры шифрование для обеспечения безопасности. Но сам протокол оказался уязвимым местом в системе безопасности. Если в точке доступа активирован WPS с PIN (который по умолчанию включен в большинстве беспроводных маршрутизаторов), то подобрать PIN-код для подключения можно за считанные часы. Защититься от атаки можно пока одним способом — отключить WPS в настройках маршрутизатора. Некоторые производители вводят таймаут на блокировку пользователя, например, после 5 неудачных попыток ввода PIN-кода, что существенно усложняет полный перебор, или допускают использование в PIN не только цифр, но и букв, что существенно увеличивает время подбора.

Кроме встроенных протоколов канального уровня в сетях IEEE 802.11 можно использовать те же стандарты для контроля доступа и шифрования (например, IPSec VPN), что и в других сетях.

5. Структурирование, как средство построения больших сетей

Небольшие сети, которые состоят из 10-40 PC, целесообразно строить в виде сегмента одной из базовых технологий ЛВС. Такая однородная структура делает простой процедуру наращивания число компьютеров в небольших пределах, облегчает обслуживание и эксплуатацию сети.

Однако в таких сетях есть ряд ограничений, важнейшими из которых являются:

1. ограничение на длину связей между узлами;
2. ограничение на количество узлов в сети;
3. ограничение на интенсивность графика, который порождается узлами сети.

Для снятия перечисленных ограничений применяются методы структурирования сети (физического и логического), которые реализуется с помощью коммутирующего оборудования: повторителей, концентраторов, мостов, коммутаторов и маршрутизаторов.

5.1. Физическое структурирование сети

Ограничения на длину связей между узлами и количеством узлов в сегменте сети, которые связаны с затуханием сигналов в передающей физической среде, позволяют снять методы физического структурирования сети. Для этого используются повторители и концентраторы. Они позволяют выполнить усиление (восстановление мощности и амплитуды) и регенерацию (восстановление формы и интервалов следования) сигналов.

Простейшее из коммутирующих устройств — **повторитель** (repeater). Это устройство выполняет свои функции на физическом уровне модели OSI. Повторители используются для физического соединения нескольких сегментов в локальной сети.

Многопортовый повторитель называется **концентратором** (hub). Концентраторы встречаются во всех базовых технологиях. Их основной функцией является усиление и формирование сигналов и передача их в соответствии с логической топологией (логический путь передачи потока данных), принятой в базовой технологии сети. Например, в технологии Ethernet – это «общая шина», и концентратор передает сигналы, пришедшие на один из портов, на все остальные порты, в технологиях Token Ring и FDDI – это «кольцо»», и концентратор передает сигналы с одного из портов на соседний порт в логическом кольце.

Концентратор всегда изменяет физическую топологию сети (во всех приведенных примерах она становится «звездой»), но при этом логическая топология сети остается неизменной.

Однако повторители и концентраторы не позволяют преодолеть ограничения, которые накладываются на общую длину сети и количество узлов в ней методами доступа к разделяемой среде всех технологиях ЛВС. Например, в сетях Ethernet – это

время двойного оборота, в сетях Token Ring и FDDI – это максимально допустимое время оборота маркера по кольцу.

Но практически максимальное количество рабочих станций, которое позволяет использовать каждая из технологий, никогда не достигается в виду того, что при интенсивном обмене данными необходимо обеспечить каждому компьютеру приемлемую долю пропускной способности сети.

Наиболее важной проблемой, которую не решает физическая структуризация, остается проблема перераспределения передаваемого трафика между различными физическими сегментами сети с целью снижения ее загруженности.

Рассмотрим пример сети Ethernet, построенной на концентраторах (рис.5.1).

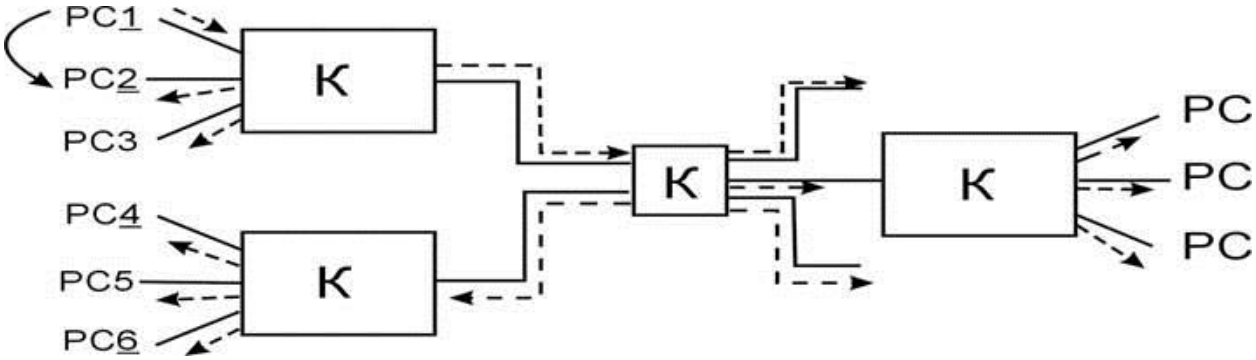


Рис. 5.1. Передача данных концентраторами Ethernet

Если PC1 надо передать данные PC2, то эти данные будут передаваться по всей сети, т.к. повторитель – аналог «общей шины», и в этот момент никакая из других PC ничего передавать не может, т.к. будет ожидать освобождение разделяемой среды.

5.2. Логическое структурирование сети

Итак, основной проблемой, которую не решает физическая структуризация сети, является перераспределение передаваемого трафика между сегментами.

Хотя базовые технологии допускают до нескольких сотен компьютеров в общей разделяемой среде, практически это число гораздо меньше (несколько десятков), т.к. при интенсивном обмене информацией необходимо обеспечить каждому компьютеру приемлемую долю пропускной способности сети. Из-за случайного фактора, который присутствует во всех методах доступа ЛВС, при значительной загруженности сети средняя доля пропускной способности (Cmax/N, где Cmax – максимальная скорость протокола, N- количество компьютеров) рабочей станции часто не достается.

На рис. 5.2 показана зависимость задержек доступа к среде передачи данных в сетях Ethernet, Token Ring и FDDI от коэффициента использования сети ρ, который также часто называют коэффициентом нагрузки сети.

$$\rho = \frac{\sum_{i=1}^{N} T_{pi}}{C_{max}} 100\%$$, где

Cmax – максимальная скорость протокола, т.е. максимальная пропускная способность сети;

Tpi – среднестатистическая интенсивность трафика, генерируемого каждым компьютером сети, т.е. в числители формулы – среднестатистическая интенсивность трафика, который должна передавать сеть;

N - количество рабочих станций в сети.

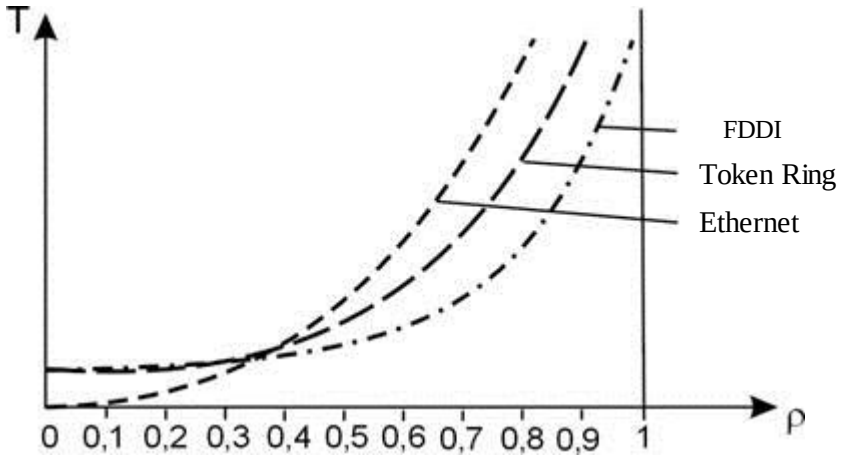


Рис. 5.2. Задержки доступа к среде передачи данных для технологий Ethernet, Token Ring и FDDI

Как видно из рисунка, всем технологиям присущ экспоненциальный рост величины задержек доступа при увеличении коэффициента использования сети, отличается только порогом, при котором наступает резкий перелом в поведении сети, когда почти прямолинейная зависимость переходит в крутую экспоненту. Для всего семейства технологий Ethernet — это 30-40%, для технологии Token Ring – 60 %, для технологии FDDI – 70 %.

Наиболее чувствительна к перегрузкам разделяемого сегмента технология Ethernet из-за её случайного метода доступа. При повышении интенсивности генерируемого узлами трафика до величины, когда ρ превышает 30%, увеличивается количество «коллизий» и повторных передач данных. А, следовательно, полезная пропускная способность сети (передача данных пользователя) уменьшается. При значении ρ близком к 1 наступает момент, когда сеть полностью занята обработкой «коллизий» и перестает передавать данные пользователя, так называемый «крах Ethernet» (рис. 5.3.).

Этот эффект хорошо известен на практике и исследован путем имитационного моделирования. Поэтому сегменты Ethernet не рекомендуется загружать так, чтобы среднее значение коэффициента использования превосходило 30 %. Именно поэтому во многих системах управления сетями пороговая граница для индикатора коэффициента загрузки сети Ethernet по умолчанию устанавливается на величину 30%.

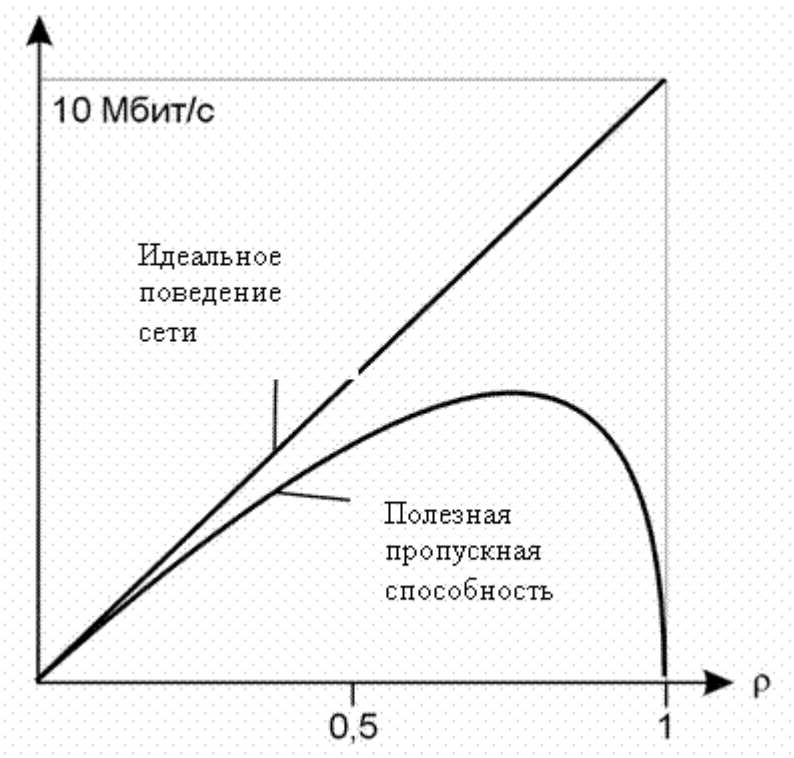


Рис. 5.3. Зависимость полезной пропускной способности сети Ethernet от коэффициента использования

Для решения перечисленных выше проблем необходимо **отказаться от использования общей разделяемой среды для всей сети** и разделить ее на несколько сегментов, соединенных между собой такими устройствами как мосты, коммутаторы или маршрутизаторы.

Распространение трафика, который предназначен PC некоторого сегмента сети, только в пределах этого сегмента, называется *локализацией* трафика. *Логическое структурирование сети* это процесс ее разбиения на сегменты с локализованным трафиком.

Сейчас часто справедливо соотношение локального трафика к межсегментному 50% к 50% и даже 20% к 80% (когда усиленно используются общие данные предприятия в отделе). Но все равно, если при разбиении на сегменты локальный трафик отсутствует, то разбиение наверно, т.е. необходимо стремится к максимальной локализации трафика при разделении сети на сегменты.

Большинство крупных сетей строится на основе структуры с общей магистралью, к которой через мосты, коммутаторы, маршрутизаторы присоединены подсети (сегменты) разных отделов. Подсети отделов могут делиться на сегменты для обслуживания рабочих групп.

Логическая сегментация, кроме локализации трафика, дает следующие преимущества:

4. Увеличивается гибкость сети: в разных подсетях могут использоваться разные базовые технологии и разные ОС, а их пользователи могут обмениваться данными друг с другом.

5. Увеличивается безопасность данных. Для пользователей одних сегментов легко ограничить доступ к ресурсам других сегментов. В мостах, коммутаторах, маршрутизаторах устанавливаются логические фильтры данных, чего не позволяют делить повторители. Кроме того, данные передаются только тем станциям, которым они предназначены.

6. Упрощается управление сетью. Проблемы одной подсети не влияют на другие подсети. Подсети образуют логические домены управления сетью.

7. Снимаются ограничения на длину оптоволоконного кабеля для технологии Ethernet, которая накладывалась временем двойного оборота;

8. Снимаются ограничения на количество коммутирующих устройств в древовидной топологии сети (коммутаторов и маршрутизаторов). Такие ограничения накладывались на количество концентраторов в сети особенностями методов доступа к разделяемой среде (например, временем двойного оборота в технологии Ethernet, максимально допустимым временем оборота маркера в сетях с кольцевой топологией).

Мости и коммутаторы работают на канальном уровне стека протоколов, а маршрутизаторы для решения своих задач привлекают протоколы сетевого уровня. Мосты и коммутаторы выполняют передачу кадров на основе аппаратных адресов (MAC - адресов), а маршрутизаторы на основе составных числовых адресов (номер сети + номер узлов). При этом общая разделяемая среда, созданная концентраторами, делится на несколько частей – сегментов, каждый из которых присоединен к порту моста, коммутатора или маршрутизатора (рис.5.4).

Мосты (bridge) изолируют трафик одной подсети от другой, передавая кадры из подсети в подсеть только в том случае, если адрес станции назначение действительно находится в другой подсистеме. Для этого они строят таблицу коммутации, запоминая через какие порты к ним поступают кадры с MAC – адресами отправителей. В дальнейшем мосты посылают кадры, адресованные этим станциям (теперь они выступают в роли получателей), на уже известные порты.

Мосты последовательно записывают приходящие пакеты в общий буфер и пересылают их в нужные порты.

В настоящее время мосты применяются в глобальных сетях для прозрачного соединения 2 – х удаленных ЛВС в общую сеть, и называются в этом случае удаленными мостами (remote bridge).

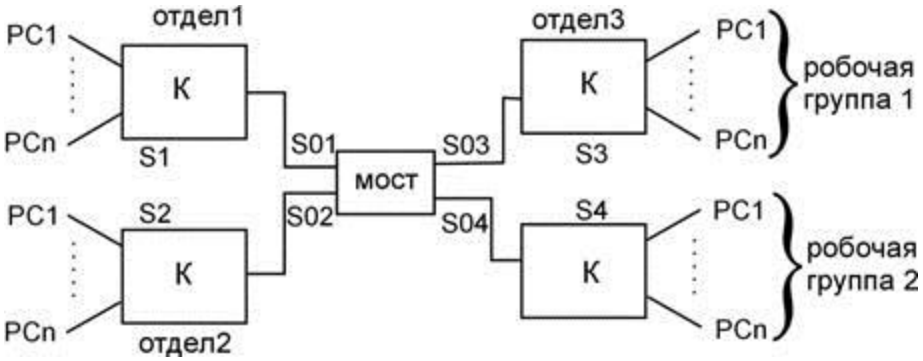


Рис. 5.4. Передача данных мостами/коммутаторами

Пример.

На предприятии есть 3 отдела. Один из отделов включает в себя 2 рабочие группы. Вся сеть разделена мостом на 4 сегмента (подсети).

S1,S2,S3,S4 – локальный трафик подсетей (между станциями подсети).

S01,S02,S03,S04 – межсегментный трафик подсетей, (т.е. тот который данная подсеть отправляет и принимает от всех остальных подсетей).

Трафик подсетей:

Отдел 1 = S1+S01;

Отдел 2 = S2+S02;

Отдел 3:

рабочая группа 1 = S3 + S03;

рабочая группа 2 = S4 + S04;

Если бы вместо моста был концентратор, то трафик для всей сети был бы общим:

Трафик сети = S1+S2+S3+S4+S0,

Где S0 – общий межсегментный трафик, т.е. тот который генерируется станциями, находящимися в одних сегментах для станций, которые находится в других.

(S0<S01+S02+S03+S04, т.к. S01, например учитывает и трафик S12 u S21, также, как S02 учитывает S21 и S12)

Коммутаторы (switch). В отличие от моста, который содержит 1 процессорный блок и обрабатывает кадры данных, поступающие на все его порты, последовательно, каждый порт коммутатора оснащен специализированным процессором, который обрабатывает поступающие на этот порт кадры по алгоритму моста независимо от других портов. Поскольку данные между разными портами коммутатора могут передаваться параллельно, то его производительность намного больше, чем у моста.

Следовательно, межсегментный трафик будет передаваться быстрее. Кроме процессора каждый порт имеет свой входной и выходной буфер памяти, и свой экземпляр адресной таблицы.

Полнодуплексный режим работы коммутатора (это относится и к маршрутизатору) состоит в одновременной передаче данных в противоположных направлениях между портами 2-х коммутаторов или коммутатором и компьютером. Скорость в каждом направлении соответствует скорости протокола порта коммутатора. Использование полно дуплексного соединения позволяет увеличить скорость передачи данных по линии связи почти в 2 раза, если объем трафика в обоих направлениях приблизительно одинаков. При организации дуплексной связи методы доступа к среде передачи всех технологий унифицируются и сводятся к общему простому алгоритму, в соответствии с которым кадры, поступающие в выходной буфер порта, последовательно передаются в линию связи. Такая линия связи в отличие от разделяемой среды является индивидуальной, в любое время находится в распоряжении единственного передатчика. Рекомендованная загруженность каждой из 2-х индивидуальных линий при пульсирующем трафике составляет 70%-80%. Не рекомендуется рассчитывать общий коэффициент загруженности дуплексного соединения, поскольку нередко проходящий по нему трафик может быть сильно несимметричен.

Коммутаторы так же могут выполнять ряд полезных дополнительных функций: приоритезация трафика, поддержка виртуальных сетей и т.д.

Следует отметить, что точная топология связей между логическими сегментами в сети мостам и коммутаторам не известна. Поэтому использование этих устройств налагает ограничения на конфигурацию связей между сегментами – они не должны содержать замкнутых контуров, т.е. от любого узла сети к другому узлу должен существовать только один маршрут.

Маршрутизаторы еще более надежно и эффективно изолируют трафик отдельных сегментов. Они разделяют сеть на подсети. Компьютеры каждой подсети снабжаются в дополнение к аппаратным адресам сетевыми адресами с одинаковой старшей частью – адресом подсети. Задачей маршрутизатора является передача данных между своими портами в соответствии с сетевыми адресами – получателей, которые содержатся в заголовках пакетов сетевого уровня. Выходной порт для пакета маршрутизатор находит в заранее заполненной таблице маршрутизации.

Маршрутизаторы не передают по умолчанию широковещательные кадры данных между подсетями. Широковещательные рассылки часто инициируют сервера и операционные системы, информируя клиентов о своем присутствии в сети или собирая некоторую информацию от них. Такая информация обычно актуальна для ограниченных сегментов крупной сети, в то время как остальные сегменты сильно загружаются ненужным трафиком.

Маршрутизаторы являются удобным средством для фильтрации трафика на сетевом и транспортном уровне. Маршрутизаторы могут работать в сетях с замкнутыми контурами и осуществлять выбор наиболее рационального маршрута из нескольких возможных, обходить поврежденные участки сети. Они могут связывать в единую сеть подсети, построенные по разным технологиям, в том числе LAN и WAN . Однако они не являются прозрачными устройствами сети. Их нужно конфигурировать, а также нужно конфигурировать каждый узел, который хочет

передать данные узлу другой подсети (он должен знать о наличие маршрутизатора и обращаться непосредственно к нему). При соизмеримом быстродействии маршрутизаторы стоят дороже коммутаторов.

Рассмотрим пример. Если в рассмотренном ранее примере (рис. 5.4) мост заменить маршрутизатором, то на загруженность подсетей это не повлияет. Исключением может быть только случай, когда каждая из подсетей генерируют в больших объемах широковещательный трафик, который не предназначен для передачи в другие подсети, но по умолчанию передается мостом или коммутатором.

Т.к. маршрутизатор, работающий на сетевом уровне, выполняет более сложные функции, чем мост или коммутатор, то затрачивает на это больше времени. По производительности маршрутизаторы сильно различаются. Они могут выполнять обработку данных последовательно и программно или параллельно и аппаратно, но в последнем случае их стоимость резко возрастет и значительно превосходит стоимость коммутаторов аналогичной производительности.

В настоящее время для объединения подсетей внутри крупной ЛВС используются коммутаторы третьего уровня, совмещающие в себе преимущества коммутаторов и маршрутизаторов.

Если в нашем примере использовать несколько маршрутизаторов (рис.5.5), то это даст возможность ввести дополнительную связь между М1 и М2.

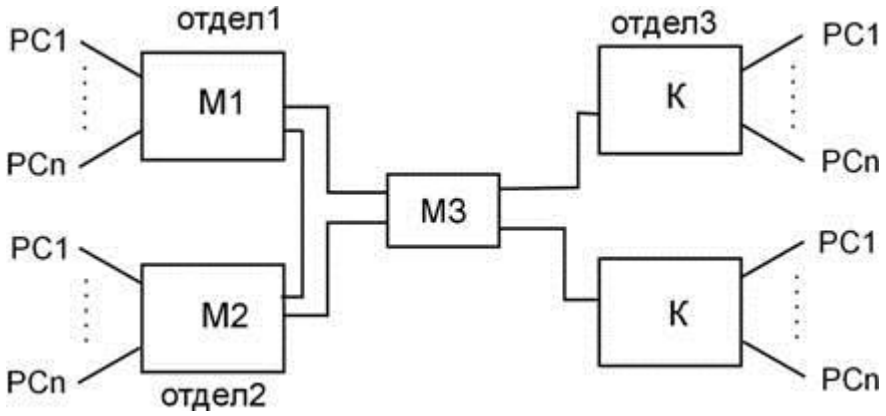


Рис.5.5. Передача данных маршрутизаторами

Дополнительная связь М1–М2 может использоваться для увеличения производительности сети – данные между отделами 1 и 2 могут передаваться параллельно по двум маршрутам. Кроме того, дополнительная связь повышает надежность передачи данных между отдельными подсетями – в случае неполадки на одном из маршрутов данные будут передаваться по другому маршруту.

Кроме перечисленных устройств, для соединения отдельных частей сети может использоваться **шлюз** (gateway). Локализация трафика не является его основной функцией. В основном он используется для объединения сетей с разними типами прикладного и системного программного обеспечения. Шлюз может преобразовать весь поток информации (коды, форматы данных, методы управления и т.д.), работая со всеми семью уровнями модели OSI. К шлюзам можно отнести прокси – серверы, почтовые шлюзы между ПО, которое использует разные почтовые протоколы и т.д.

5.3.Типовые схемы построения ЛВС на коммутаторах и концентраторах

5.3.1. Выбор коммутаторов и концентраторов

При осуществлении выбора надо учитывать функциональные возможности и характеристики устройств, которые будут рассмотрены в главе 6. Остановимся на некоторых моментах, которые нужно учитывать при выборе коммутирующих устройств:

1. Стоимость в расчете на порт.
2. Распределение трафика между узлами. Загруженность сети в целом и ее отдельных узлов не должны превышать предельно допустимые.
3. Возможности роста сети. Хорошее решение — запас по количеству портов 10-20%. Использование устройств с наращиваемым количеством портов. Необходимо предусмотреть возможность дальнейшего сегментирования сети для поддержания производительности сегментов на должном уровне.
4. Возможность удаленного управления. Хорошо, когда коммутирующие устройства поддерживают средства удаленного управления сетью и анализа графика в ней для оценки загруженности сети.
5. Тип протокола — скорость и спецификации физической среды, которые может поддержать концентратор (для него скорости всех портов одинаковы), а для коммутатора необходимо рассматривать варианты разных комбинаций скоростей и спецификаций портов.

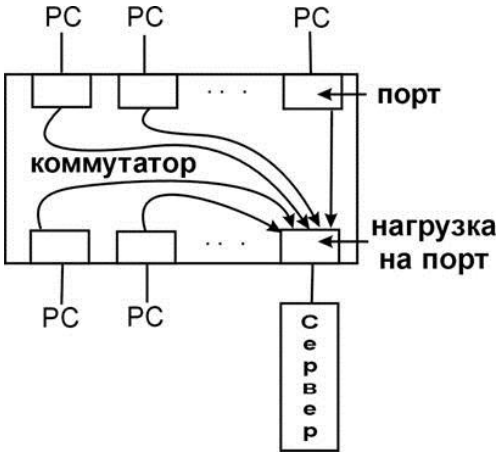


Рис. 5.6. Проблема перегрузки портов коммутаторов

Для эффективной работы в сети с выделенным сервером (рис.5.6.) выпускаются модели коммутаторов с одним высокоскоростным портом 1000Мбит/с (для подключения сервера) и несколькими портами 100 Мбит/с (для подключения рабочих станций). Аналогично, возможно соотношение скоростей портов 100Мбит/с и 10 Мбит/с.

Вообще, к примеру, с коммутатором с одним портом 100Мбит/с и остальными 10Мбит/с мог бы конкурировать концентратор, который поддерживает протокол 100 Мбит/с (Fast Ethernet). Его стоимость в пересчете за порт была бы ниже, чем у коммутатора с одним высокоскоростным портом, а производительность сети в обоих случаях была бы примерно одинаковой. Но в случае концентратора ещё нужно было бы

заменить все сетевые адаптеры компьютеров на 100-Мбитные. А это с одной стороны будет дороже, но с другой – создаст хорошую перспективу роста для новых приложений.

Выбор в пользу коммутатора можно обосновать необходимостью последующей сегментации сети. Кроме того, в сети, построенной коммутаторах, не накладывается ограничений на их количество (хорошая перспектива расширения), и изолируется трафик разных пользователей друг от друга. **С конца 90-х годов началась тенденция снижение стоимости коммутаторов и вытеснения ими концентраторов.** В приведенных в разделе 5.3.2. примерах вместо концентраторов вполне могут использоваться коммутаторы, но их применение не сможет обеспечить в данных условиях существенных преимуществ. Для небольших рабочих групп с небольшой интенсивностью трафика ($\rho \leq 30\%$) и одним выделенным сервером замена концентратора на коммутатор с точки зрения производительности сети останется незаметной.

Сервер с коммутатором соединяется *дуплексной связью*. Поскольку имеется интенсивный график в обоих направлениях, то режим параллельной передачи в обоих направлениях повышает производительность сети. Для подключения мощного сервера можно также использовать *агрегированную связь* с коммутатором, т.е. объединение в одну логическую связь нескольких физических линий. При этом у сервера должно быть несколько сетевых адаптеров, которые соединяются параллельно с несколькими портами коммутатора. И адаптеры, и коммутатор должны поддерживать такую возможность и быть соответствующим образом настроены.

5.3.2. Некоторые типовые решения

Сети рабочих групп

Приведем несколько вариантов организации сетей небольших рабочих групп

Первый вариант:

Сегмент сети построен на простом концентраторе Fast Ethernet с той особенностью, что все его порты концентратора поддерживают протокол 100BaseTX, а один - 100BaseFX для вязи с сетью предприятия, которая находится на расстоянии несколько сотен метров.

Рис. 5.6. Пример сети небольшой рабочей группы.

Второй вариант:

Сегмент сети построен на стековом концентраторе Fast Ethernet. Файловый сервер одновременно выступает в роли маршрутизатора, через который компьютеры сегмента осуществляют доступ в глобальную сеть. Внешний канал может быть подключен, например, к последовательному порту компьютера или порту USB. Современные операционные системы (Windows NT Server и выше, Novell Netware, Unix) поддерживают встроенные протоколы маршрутизации. Это даёт возможность использовать в качестве маршрутизатора соответствующим образом настроенным универсальным компьютером. Такое решение – неплохая альтернатива приобретению отдельного дорогого маршрутизатора для небольшой организации.

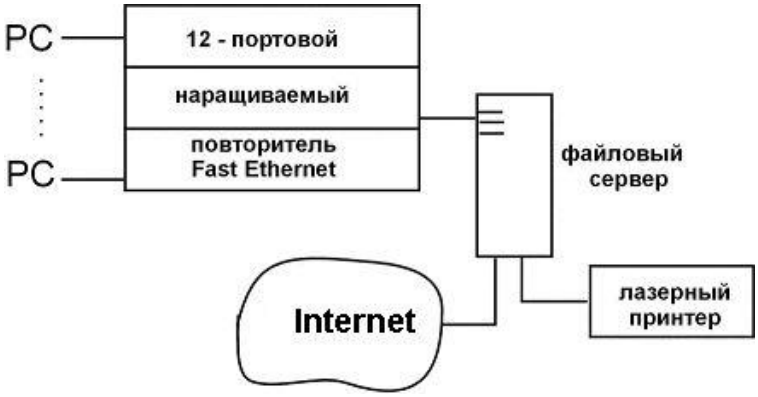


Рис. 5.7. Пример сети средней рабочей группы

Третий вариант:

На рис.5.8. приведена сеть разработчиков технологии Fast Ethernet. Каждая группа имеет свой высоко производительный сервер с большим объемом дисковой памяти и возможность доступа к данным других групп. Интересным решением является то, что у всех рабочих станций есть по два сетевых адаптера: один — для связи с корпоративной сетью, а второй — для сети инженерной группы. Современные операционные системы хорошо поддерживают такую возможность. Внутренняя маршрутизация на компьютерах выключена. Таким образом, группа имеет свою изолированную сеть, которая полностью изолирована от корпоративной сети. Сохраняется высокая степень защищенности информации группы. С другой стороны члены рабочей группы имеют полный доступ к корпоративной сети.

Аналогичным решением может воспользоваться группа руководителей крупной компании, имея отдельную сеть и сервер с особо ценной информацией.

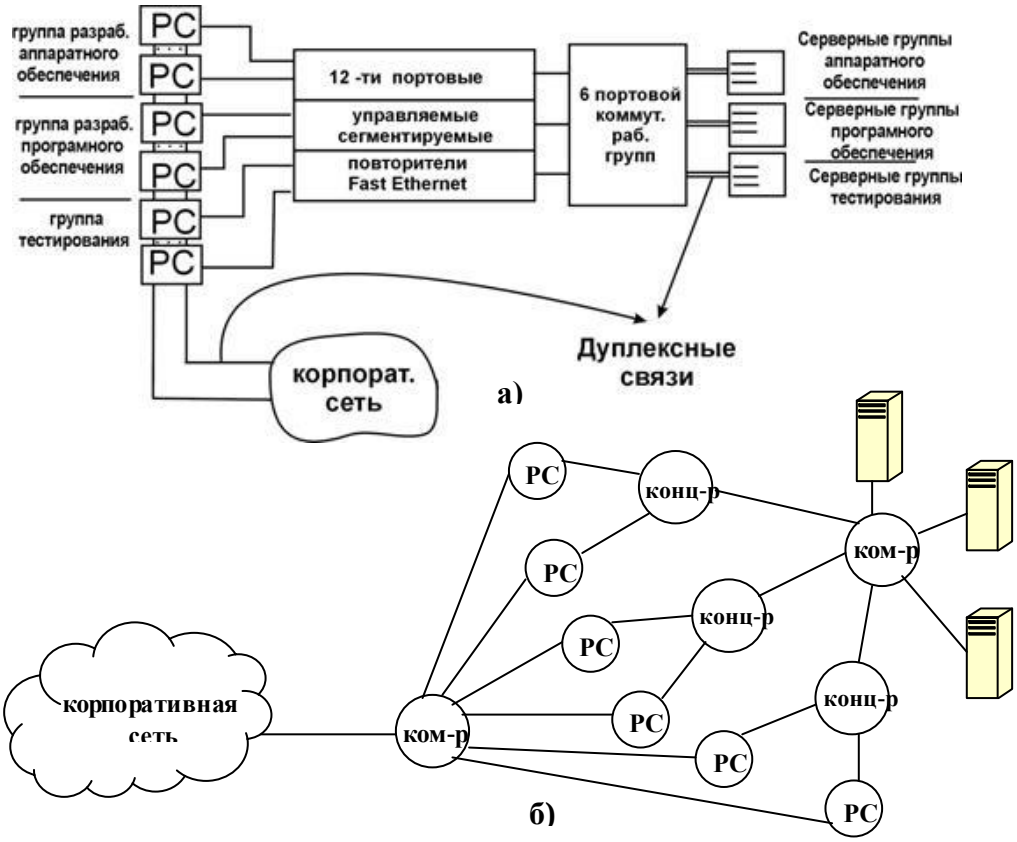


Рис. 5.8. Пример сети инженерной группы (а) и её схематическое представление (б)

Следует отметить, что в настоящее время, стоимость простых коммутаторов сравнялась со стоимостью концентраторов, поэтому в сетях рабочих групп вместо концентраторов обычно используют недорогие коммутаторы. В приведенных выше примерах такая замена будет практически не заметна.

Сеть отдела

В сетях отделов для разделения трафика рабочих групп необходимо сегментирование сети с помощью коммутаторов или маршрутизаторов.

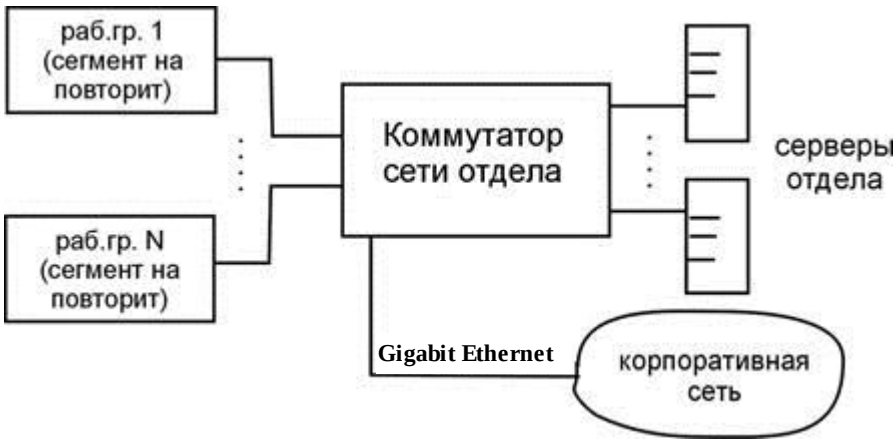


Рис. 5.9. Пример сети отдела

5.3.3. Опорные сети

При всем разнообразии структурных схем сетей на коммутаторах все они используют две базовые структуры:

1. стянутая в точку магистраль;

2. распределенная магистраль.

На основе этих базовых сетей строятся разнообразные структуры конкретных сетей.

Стянутая в точку магистраль

Для объединения сетей отделов с четь здания, а сетей здания - в сеть кампуса необходимо организовать между ними скоростную магистраль.

Внутри здания чаще всего используется решение со стянутой в точку магистралью. Это структура, при которой объединение сегментов, узлов или сетей происходит на внутренней магистрали коммутатора (рис. 5.10).

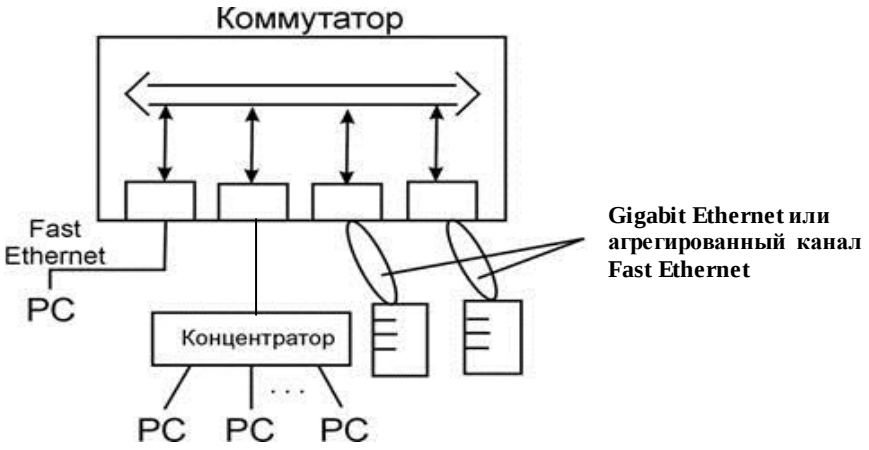


Рис. 5.10. Пример стянутой в точку магистрали

Достоинствами такого решения является высокая скорость магистрали и протокольная независимость. Скорость магистрали в данном случае равна производительности самого коммутатора и для мощного неблокирующего устройства равняется суммарной скорости всех его портов (до нескольких Гб/сек). Подключение узла или сегмента с новым протоколом часто требует не замены коммутатора, а добавления интерфейсного модуля для порта, который поддерживает данный протокол.

Хорошим примером может служить магистраль здания на коммутаторах (рис. 5.11) Наиболее загруженные линии связи могут реализовываться как агрегированные каналы технологии Fast Ethernet (логическое объединение нескольких физических каналов N*100Мбит/с), а могут использовать технологию Gigabit Ethernet.

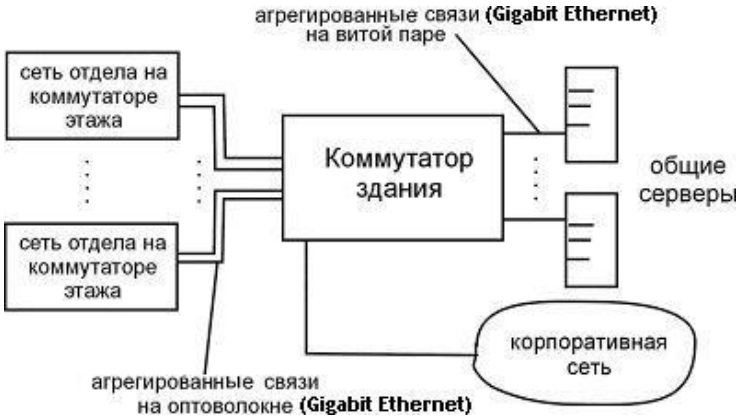


Рис. 5.11. Пример магистрали здания на коммутаторах

Однако структура с мощным центральным модульным коммутатором имеет свои недостатки:

1. высокая плотность и протяженность кабельной системы, следовательно, высокая стоимость;

2. структура не всегда она может быть реализована чисто физически при значительной удаленности подсетей (например, для подсетей зданий уже нельзя использовать кабель на витых парах), поэтому в локальных вычислительных сетях, покрывающих большие территории, часто используется вариант с распределенной магистралью.

Распределенная магистраль

В качестве магистральной обычно используются технологии: Fast и Gigabit Ethernet. Распределенная магистраль упрощает связь между этажами, уменьшает стоимость кабельной системы, преодолевая ограничения на расстояния. Однако скорость магистрали ограничена скоростью протокола, поддерживаемого портами коммутатора, которая всегда меньше, чем у стянутой в точку магистрали. Поэтому необходимо учитывать интенсивность трафика между этажами и зданиями, а также стоимость реализации самой технологии.

Пример сети с распределенной магистралью показан на рис 5.12.

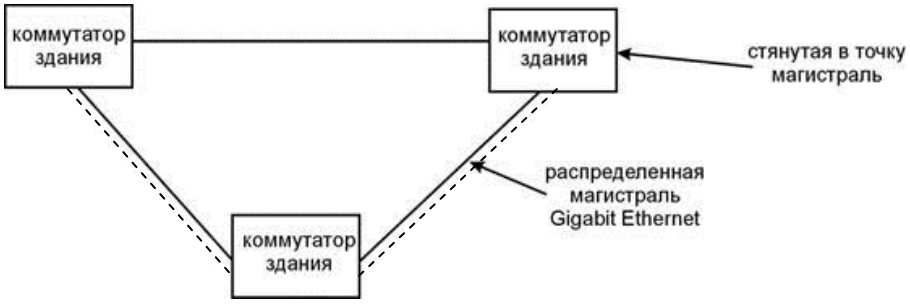


Рис. 5.12. Пример распределенной магистрали на коммутаторах Ethernet, поддерживающих резервные связи

В сети, изображенной на рис 5.12, для повышения надежности магистрали в неё введена резервная связь. Для обеспечения нормальной работы такой топологии (коммутаторы не поддерживают замкнутых контуров) необходимо, чтобы объединяемые коммутаторы поддерживали протокол Spanning Tree. Эта функция автоматически переводит одну из связей в отключенное состояние (резервная), а по двум другим будет передаваться данные. В случае отказа основной связи автоматически будет включена резервная.

В принципе, вместо крупных коммутаторов на магистралях могут использоваться маршрутизаторы. При этом нужно принимать во внимание:

- Маршрутизаторы не прозрачны для узлов сети, они сложнее конфигурируются и управляются;
- Операция коммутации всегда быстрее маршрутизации, а стоимость высокоскоростных маршрутизаторов в расчете на порт обычно в 10-ки и 100-ни раз выше, чем у коммутаторов.

В настоящее время в качестве центральных коммутаторов зданий получили распространение коммутаторы 3-го уровня. Для внутрисегментного трафика они работают в режиме коммутации, межсегментный трафик – маршрутизируют. Таким образом, достигается компромисс: внутрисегментный трафик передается быстрее, а для магистрального трафика выполняется необходимая изоляция от внутреннего трафика сегментов. Широковещательный трафик из сегментов в магистраль не поступает, а для межсегментного трафика маршрутизация предоставляет более развитые средства фильтрации трафика, чем коммутация.

6. Коммутаторы и концентраторы

Различные коммутирующие устройства выполняют свои основные функции на разных уровнях модели OSI. Помимо основных они могут выполнять ряд дополнительных функций, а при одинаковых наборах функций устройства могут иметь разные характеристики. Дополнительные функции всегда увеличивают стоимость устройства, часто требуют дополнительной настройки и могут уменьшить скорость выполнения основных функций, поэтому выбирать их нужно с учетом необходимости решения конкретной задачи.

6.1. Концентраторы

6.1.1. Основные функции и дополнительные функции

В каждой базовой технологии есть свои повторители (концентраторы, MAU). Их основной задачей является усиление (восстановление мощности и амплитуды), формирование (восстановление формы и интервалов следования) приходящих в узел сигналов, и передача их в сеть в соответствии с логическим маршрутом, который определяется для каждой технологии методом доступа к разделяемой среде («общая шина», «кольцо» и т.д.). Концентраторы конкретной технологии характеризуются количеством портов, типами протоколов физического уровня, поддерживаемых

портами, конструктивным исполнением и т.д. Кроме основной функции повторения сигнала концентраторы могут поддерживать ряд дополнительных факультативных функций.

Хотя в настоящее время благодаря снижению стоимости коммутаторов, они все чаще заменяют концентраторы в ЛВС, но следует отметить, что для небольших рабочих групп с небольшой интенсивностью трафика ($\rho \leq 30\%$) и одним выделенным сервером замена концентратора на коммутатор с точки зрения производительности сети останется не заметной.

Автоматическое отключение портов (автосегментация). Это способность отключать некорректно работающие порты. Для концентраторов FDDI – эта функция определена в протоколе, следовательно, является основной. Для Token Ring и Ethernet она во многих случаях дополнительная (не задана реакция на ситуацию в протоколе). Основной причиной отключения концентраторами Ethernet является отсутствие ответа на тест связности. Порт временно отключается, а когда тест снова будет проходить, порт автоматически подключается.

Дополнительно для Ethernet:

1. Если интенсивность ошибочных кадров (неправильная контрольная сумма, неверная длина кадра: > max или < min, неправильный заголовок) превышает заданий порог, то порт на некоторое время отключается.
2. Если порт был источником коалиций 60 раз подряд, он на некоторое время отключается;
3. Если время прохождения кадра через порт в три раза больше времени передачи кадра max длины, то порт отключается (Jabber – контроль, дословно, контроль болтливости неисправного адаптера).

Поддержка резервных связей. Как основная функция определена только для FDDI. Для Ethernet замкнутые контура не допускается в топологии сети. Поэтому порты резервных связей должны находиться в отключенном состоянии (рис.6.1.). При конфигурировании концентратора администратор сети определяет основные и резервные порты. В дальнейшем, если основной порт отключается (автосегментация), то автоматически может быть включен резервный порт.

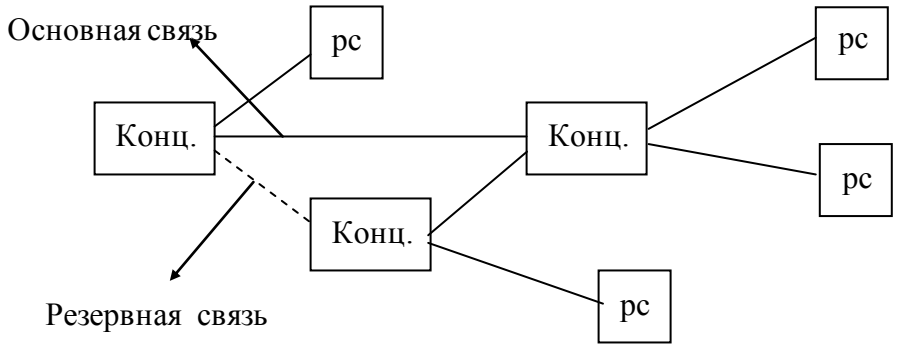


Рис. 6.1 Поддержка резервных связей концентраторами

Защита от несанкционированного доступа. Это защита от подключения постороннего PC к концентратору с целью переписывания сетевого графика. Для

концентраторов Ethernet существует 2 способа реализации данной функции. В обоих случаях концентратор нужно вручную конфигурировать, задавая MAC – адреса PC, которым разрешено подключаться к портам. В результате с каждым портом будет связан адрес PC.

1. Если к порту подключается PC с другим адресом, порт отключается и фиксируется нарушение.
2. Поле данных кадра, который направляется в порты не подключенные к PC – назначения, заполняются нулями.

Управляемость. Сложные концентраторы, выполняющие дополнительные функции, обычно могут управляться централизовано по сети с помощью стандартного протокола (SNMP – обмен сетевыми сообщениями). Эта функция позволяет выполнять удаленную настройку устройства и собирать статистику о проходящем через него трафике с помощью специальной программы – агента, которая в отличие от самого устройства имеет свой сетевой и локальный адрес. Эта функция характерна не только для концентраторов, но и для коммутаторов и маршрутизаторов.

6.1.2. Конструктивное исполнение

Концентраторы, равно как и другие коммутирующие устройства (коммутаторы и маршрутизаторы) могут изготовляться на базе трех основных конструктивов, обладающих различными свойствами: конструкция с фиксированным количеством портов, модульная конструкция на шасси и стековая конструкция. Коммутирующие устройства рабочих групп обычно имеют фиксированное количество портов, отделов – могут иметь стековую структуру, а магистральные – модульную структуру на шасси.

С фиксированным количеством портов

Это наиболее простые и дешевые концентраторы. Количество портов обычно составляет от 4-8 до 24, один порт может быть специально выделен для подключения к другому концентрату. Это простое и дешевое решение. При необходимости подключения дополнительных компьютеров в сегменте можно объдинить несколько таких концентраторов в древовидную топологию. При последовательном объединении нескольких концентраторов, общая задержка передачи данных через них равняется сумме задаржек каждого из концентраторов.

Модульная конструкция

Отдельные модули с фиксированным количеством портов устанавливаются на общее шасси, которое имеет внутреннюю шину для объединения модулей в один повторитель. При этом концентратор, состоящий из модулей, обладает задержкой одного концентратора. Модули могут различаться количеством портов и типом поддерживаемого кабеля среды. Модульные концентраторы поддерживают средства удаленного управления, снабжаются средствами терморегуляции, избыточными источниками питания и т.д. легко и удобно модифицируется, но начальная стоимость велика. Поэтому они используется только в крупных сетях.

Стековая конструкция

Данная конструкция занимает промежуточное положение между модульной и с фиксированным количеством портов. От конструкции с фиксированным количеством

портов она отличается тем, что такой концентратор имеет специальный порт и кабель, с помощью которого он может быть соединен с аналогичным портом другого концентратора. В результате, образуется один общий повторитель с суммарным количеством портов и задержкой примерно равной (чуть большей) задержке одного концентратора. Несколько большая задержка объясняется наличием внешнего соединения. Число, объединяемых в стек корпусов, обычно до 8. Объединяемые концентраторы могут поддерживать различные среды передачи.

Стоимость в расчете на порт у стековых концентраторов ниже, чем у модульных, но больше чем у концентраторов с фиксированным количеством портов. При желании для стековой конструкции можно приобрести корпус с модулем управления, избыточный источник питания и т.д., но корпуса приобретаются по мере необходимости и в нужном количестве, тогда как для модульной конструкции необходимо сразу приобрести шасси со всеми общими модулями (управления, питания и т.д.).

Модульно-стековая конструкция

В этом варианте модульные концентраторы с количеством портов (1-3) объединяются в стек. Конструкция призвана сочетать достоинство конструкций обоих типов.

Многосегментная конструкция

Концентраторы могут быть многосегментными, т.е. образовывать не 1, а несколько независимых повторителей в одном корпусе.

Многосегментная конструкция позволяют делить сеть на физические сегменты программным путем без изменения подключения рабочих станций. Т. е. в одном устройстве реализуется несколько внутренних шин, подключение к которым образует ряд независимых (не связанных между собой) повторителей. На рис.6.2. таких повторителей – 3. Подключение PC к конкретному повторителю задается программно.

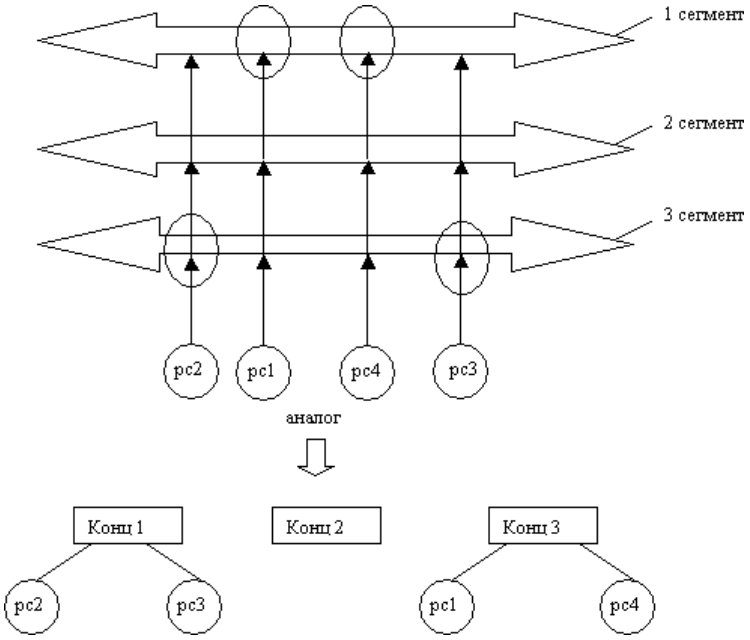


Рис. 6.2 Многосегментная организация концентраторов

6.2. Мосты/коммутаторы

Поскольку мосты и коммутаторы – устройства, которые выполняют свои основные функции на канальном уровне, то в каждой сетевой технологии есть свои коммутаторы. В технологиях LAN– Ethernet Token Ring и FDDI, которые используют общий формат локальных адресов – уникальные MAC-адреса, возможно построение смешанных сегментов на коммутаторах, если коммутаторы обладают дополнительной функцией преобразования формата кадра.

К основным функциям мостов и коммутаторов относится построение таблиц коммутации и передача пакетов между портами устройства на основании построенных таблиц по локальным адресам получателей пакетов.

6.2.1. Алгоритмы работы мостов/коммутаторов

В своей работе мосты/коммутаторы используют 2 типа алгоритмов:

1. Прозрачного моста (стандарт IEEE 802.1D);
2. Мосты с маршрутизацией от источника (IBM для Token Ring).

Алгоритм с маршрутизацией от источника использовался для соединения колец Token Ring и FDDI, хотя и тогда для этих целей разрешалось использовать прозрачные мосты. В настоящее время технологий Token Ring и FDDI ушли в прошлое, а алгоритм прозрачного моста нашел своё применения в коммутаторах технологии Ethernet. Хотя принцип маршрутизации от источника в дальнейшем был принят как один из видов маршрутизации в IPv4.

В дальнейшем все функции мостов и коммутаторов будем рассматривать на примере технологии Ethernet.

Алгоритм прозрачного моста

Прозрачность мостов заключается в том, что такие мосты незаметны для сетевых адаптеров (не влияют на их работу), и если мостам и коммутаторам не задавать дополнительных функций их можно не конфигурировать, а просто правильно подключить.

Мост пассивно наблюдает за трафиком сети. Порты моста работают в так называемом режиме ”неразборчивого захвата кадров”, попадающих на его порты и буферизирует их. В начальный момент, когда мост не знает адресов PC, он просто рассылает захваченный кадр на все свои порты, кроме того, с которого тот кадр получен. **Отличие от повторителя в этом случае состоит в том, что кадр передается не побитно, а с буферизацией.** При этом логика работы “разделяемой среды” разрывается. Когда мост пытается переслать кадр в сегмент, он пытается получить доступ к среде сегмента наравне с любой PC.

Одновременно с рассылкой кадров мост делает также запись в свою адресную таблицу на основании адреса отправителя и номера порта, с которого кадр поступил.

MAC адрес PC	Номер порта моста	t жизни	пользовательский фильтр

В дальнейшем, захватив кадр, мост просматривает таблицу. Если адрес назначения не известен, мост рассылает кадр на все свои порты, аналогично концентратору. Если адрес уже изучен (присутствует в таблице), а PC – адресат и PC – отправитель находятся в разных сегментах, мост получает доступ к среде нужного сегмента и “продвигает” (forwarding) кадр в порт, к которому подключен сегмент. Если бы адреса PC – отправителя и PC – получателя принадлежали одному сегменту, кадр просто был бы удален из буфера. Операция называется фильтрацией (filtering).

Процесс обучения моста продолжается все время, чтобы отслеживать изменения в сети: отключение и включение новых PC, перенесение PC из одних сегментов в другие. Записи в таблице могут быть динамические – создаются автоматически и имеют срок жизни и статические – создаются вручную администратором сети и срока жизни не имеют.

Широковещательные кадры также рассылаются на все порты, как и кадры с неизвестными адресами. Режим называется “затоплением сети” (flood). Однако из-за программных или аппаратных (неисправный адаптер) сбоев PC может долго генерировать широковещательные кадры, что называется “широковещательным штормом” (broadcasr storm). При этом сеть засоряется ненужным трафиком. Хотя администратор может с помощью моста ограничить максимальную интенсивность генерации кадров с широковещательным адресом, но для этого нужно знать их нормальную интенсивность, которая для разных протоколов может существенно отличаться. Поэтому такая возможность практически не реализуется.

6.2.2. Основные отличия коммутаторов от мостов

На рис.6.3. показана общая структура моста. Как уже отмечалось, мосты последовательно записывают приходящие пакеты в общий буфер и пересылают их в нужные порты.

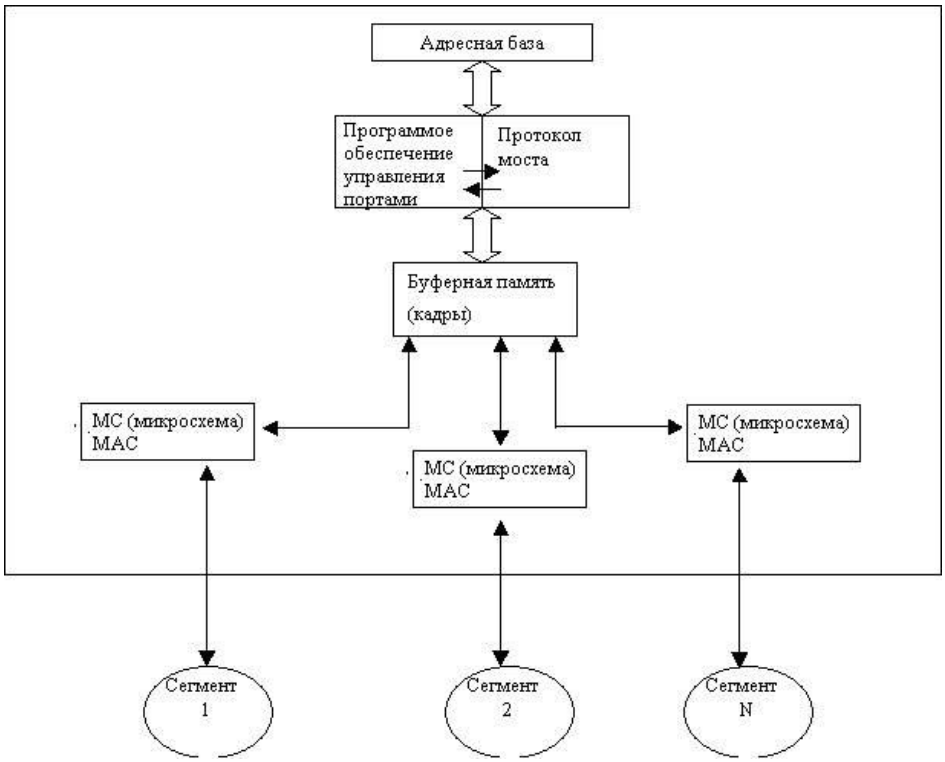


Рис.6.3. Общая структура моста

Коммутаторы обычно имеют общий процессорный блок для координации процессоров портов с некоторым объемом общей памяти. Входные блоки процессоров портов выполняют операции по фильтрации и продвижению кадров, выходные – выполняют доступ к среде сегмента и передачу в него кадров данных. Входные и выходные блоки имеют буфера. Каждый порт имеет свой экземпляр адресной таблицы (со своей информацией). В настоящее время получили распространение 3 основные схемы организации блока обмена данными между портами коммутаторов:

1. коммутационная матрица;
2. скоростная общая шина;
3. разделяемая многовходовая память.

Память должна быть достаточно быстродействующей, чтобы поддерживать скорость перезаписи данных между N портами коммутатора параллельно. Нередко несколько схем комбинируются в одном коммутаторе.

Рассмотрим основные отличия коммутаторов от мостов:

1. у коммутаторов гораздо больше портов (12, 16, 24 и больше), а у моста обычно 2-4.
2. у моста 1 процессор, все кадры, поступающие с разных портов в общий буфер, обрабатываются последовательно, т.е. от любого входного порта до выходного существует только один логический путь. Коммутатор в общем случае имеет отдельный процессор, экземпляр адресной таблицы и буфер в каждом порту, т.е. у коммутатора много логических путей для передачи кадров параллельно между разными парами портов.

3. у коммутатора значительно больше вычислительная мощность, т.к. каждый его порт снабжен специализированный заказной БИС, которая оптимизирована для выполнения основных функций коммутации.

6.2.3. Полнодуплексные протоколы ЛВС

К портам мостов/коммутаторов и маршрутизаторов могут подключаться сегменты на концентраторах. В этом случае порт коммутатора или маршрутизатора поддерживает *полудуплексный режим* и является одним из узлов данного сегмента с разделяемой средой передачи.

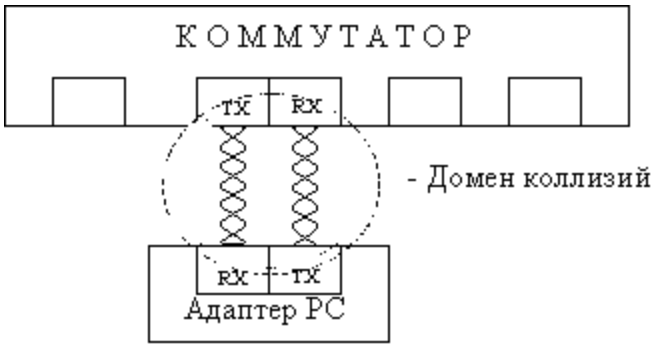


Рис. 6.5. Домен коллизий между компьютером и портом коммутатора

Если к порту коммутатора подключается отдельный компьютер (или порт другого коммутатора), то коммутатор может работать как в обычном полудуплексном, так и в *полнодуплексном режиме*.

В полудуплексном режиме коммутатора Ethernet коллизия возникает, если оба передатчика (порта коммутатора и адаптера) одновременно или почти одновременно начинают передачу, считая, что сегмент из двух проводов (домен коллизий) свободен (рис.6.5).

В полнодуплексном режиме одновременная передача – коллизией не считается, что может существенно увеличить производительность сети. Для реализации дуплексного режима MAC – блоки коммутатора и адаптера должны его поддерживать (все современные модели поддерживают). Изменения в логике работы MAC – блоков минимальны: для Ethernet отменяется фиксация и обработка коллизий, а для маркерных сетей кадры посылаются коммутатору, когда нужно PC без ожидания маркера. Т.е. фактически MAC – блок **не использует протокол доступа к разделяемой среде**. При равновероятной передаче информации в обоих направлениях производительность соединения может возрасти в 2 раза.

6.2.4. Основные характеристики коммутаторов

6.2.4.1. Характеристики производительности

Производительность коммутатора – то свойство, которое сетевые интеграторы и администраторы ждут от этого устройства в первую очередь.

Основными показателями коммутатора, характеризующими его производительность, являются:

1. скорость фильтрации кадров;
2. скорость продвижения кадров;
3. общая пропускная способность;
4. задержка передачи кадра.

Производительность коммутаторов и проблемы их использования

Если входной поток кадров со всех портов коммутатора будет превышать его пропускную способность, т.е. способность по их пересылке в выходные порты, то кадры будут накапливаться **во входных буферах** коммутатора. Если ситуация будет продолжаться достаточно долго, то буфера переполнятся и кадры будут отбрасываться, а время на их восстановление протоколами вышележащих уровней (транспортного или прикладного) велико, поэтому полезная производительность сети вместо улучшения будет ухудшаться.

Поскольку маршрутизаторы по принципу передачи данных похожи на коммутаторы, то всё выше сказанное относится и к ним. Есть данные, что для большой сети на маршрутизаторах (при тайм – аутах восстанавливающих потерянные пакеты протоколов в сотни миллисекунд) при регулярной потере 3% кадров производительность сети может уменьшаться в несколько десятков раз. Таким образом, при номинальной пропускной способности сети в 100Мб/с реальная скорость передача полезных данных будет соответствовать 5Мб/с.

Режим работы коммутатора, при котором он может передавать кадры через свои порты с той же скоростью, с которой они поступают, называется *неблокирующим*.

Для реализации неблокирующего режима работы коммутатора его производительность должна равняться сумме производительностей всех его портов в дуплексном режиме:

$$C = \sum_{i=1}^{N} Cpi, \quad \text{где}$$

C – общая пропускная способность коммутатора;

Cpi – пропускная способность одного порта;

N - количество портов коммутатора.

В полудуплексном режиме сумма производительностей всех портов должна делиться на 2, т.к. порт не может и принимать и передавать данные одновременно, т.е. в каждом обмене данными заняты 2 порта:

$$C = (\sum_{i=1}^{N} Cpi)/2.$$

Коммутаторы, способные работать в неблокирующем режиме, дороги и применяются в основном на магистралях сетей. Для других сегментов сети достаточно, чтобы коммутатор не терял часть передаваемых кадров постоянно. Для этого его общая производительность должна быть больше или равна сумме средних интенсивностей трафика, проходящего через его порты.

$$C \geq \sum_{i=1}^{N} Tpi, \quad \text{где}$$

C – общая пропускная способность коммутатора;

Tpi – среднестатистическая интенсивность трафика, проходящего через один порт;

N - количество портов коммутатора.

Но потеря кадров чаще всего происходит не от недостаточной производительности коммутаторов, а от перегрузки отдельных портов при их ассиметричной нагрузке. Она может возникать как при дуплексном, так и при полудуплексном режиме работы коммутатора (рис.6.6).

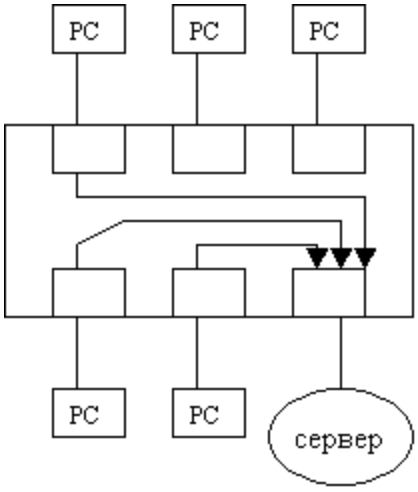


Рис. 6.6. Перегрузка порта коммутатора

Если входной поток кадров в порт будет превышать скорость его выходного протокола, то кадры будут накапливаться **в выходном буфере** порта, а при переполнении буфера отбрасываться.

Чтобы с учетом пульсаций трафика перегрузки не происходило, рекомендуется производительность каждого порта выбирать таким образом, чтобы средний коэффициент его загруженности находился в пределах 0.6-0.8:

$$\rho j = \left(\sum_{i=1}^{M} Tpi\right)/Cpj = 0.6\text{-}0.8,$$

где

ρj – коэффициент загруженности j-го порта;

Cpj – пропускная способность j-го порта;

Tpi – среднестатистическая интенсивность одного потока данных, проходящего через j-й порт;

M – количество потоков данных, проходящих через j-й порт.

Для дуплексного режима работы порта целесообразно рассчитывать коэффициент загруженности соединения в каждом направлении отдельно, поскольку нередко их трафик может сильно отличаться. Например, с одной стороны идет небольшой поток запросов, а с другой – большой поток ответов.

Другие характеристики производительности

Скорость фильтрации (filtering) определяет скорость, с которой коммутатор выполняет следующие этапы обработки кадров:

- приём кадра во входной буфер;
- просмотр адресной таблицы с целью выбора для кадра выходного порта;
- уничтожение кадра, так как входной и выходной порт совпадает, т.е. источник и приёмник находятся в одном логическом сегменте.

Скорость фильтрации практически у всех коммутаторов является неблокирующей – коммутатор успевает отбрасывать кадры в темпе их поступления.

Скорость продвижения (forwarding) определяет скорость, с которой коммутатор выполняет следующие этапы обработки кадров:

- приём кадра во входной буфер;
- просмотр адресной таблицы с целью выходного порта для адреса назначения кадра;
- передача кадра в сеть через найденный по адресной таблице выходной порт.

Как скорость фильтрации, так и скорость продвижения измеряются обычно в кадрах в секунду. По умолчанию считается, что это кадры протокола Ethernet минимальной длины (64 байта без преамбулы). Такие кадры создают для коммутатора наиболее тяжелый режим работы.

Пропускная способность коммутатора изменяется количеством пользовательских данных (в мегабитах в секунду), переданных в единицу времени через его порты.

Максимальное значение пропускной способности коммутатора всегда достигается на кадрах максимальной длинны. Поэтому коммутатор может быть блокирующим для кадров минимальной длинны, но при этом иметь очень хорошие показатели пропускной способности.

Задержка передачи кадра измеряется как время, прошедшее с момента прихода первого байта кадра на входной порт коммутатора до момента появления этого байта на его выходном порту.

Величина вносимой коммутатором задержки зависит от режима его работы. Если коммутация осуществляется «на лету», то задержки обычно невелики и составляют от 5 до 40 мкс, а при полной буферизации кадров – от 50 до 200 мкс (для кадров минимальной длинны).

6.3.4.2. Коммутация «на лету» и с полной буферизацией

При коммутации «на лету» во входной буфер принимается часть кадра, содержащая адрес получателя, принимается решение о фильтрации или ретрансляции кадра в другой порт и, если выходной порт свободен, то сразу же начинается пересылка кадра, пока его остальная часть продолжает поступать во входной буфер. Если выходной порт занят приемом кадра от другого входного порта, то кадр полностью

буферизуется во входном буфере принимающего порта. К недостаткам этого метода относится то, что коммутатор пропускает на передачу ошибочные кадры, т.к., когда возможно проанализировать конец кадра, его начало уже будет передано в другую подсеть. А это ведет к потере полезного времени работы сети.

Полная буферизация принимаемых пакетов, естественно, вносит большую задержку в передачу данных, зато коммутатор имеет возможность полностью проанализировать и при необходимости преобразовать полученный пакет.

В таблице 6.1 перечислены возможности коммутаторов при работе в двух режимах.

Таблица.6.1 Сравнительная характеристика коммутаторов при работе в разных режимах

Функция	**На лету**	**С буферизацией**
Защита от плохих кадров	Нет	Да
Поддержка разнородных сетей (Ethernet, Tokeng Ring, FDDI, ATM)	Нет	Да
Задержка передачи пакетов	Низкая (5-40 мкс) при низкой нагрузке, средняя при высокой нагрузке	Средняя при любой нагрузке
Поддержка резервных связей	Нет	Да
Функция анализа трафика	Нет	Да

Средняя величина задержки коммутаторов, работающих «на лету», при высокой нагрузке объясняется тем, что в этом случае выходной порт часто бывает занят приемом другого пакета, поэтому вновь поступивший пакет для данного порта все равно приходится буферизировать.

Может применяться механизм адаптивной смены режима работы коммутатора. Основной режим такого коммутатора – коммутация «на лету», при этом коммутатор постоянно контролирует контрольные суммы кадров, и когда интенсивность появления испорченных кадров начинает превышать некоторый порог, коммутатор переходит на режим полной буферизации. Через некоторое время он снова может вернуться к коммутации «на лету».

6.3.4.3. Размер адресной таблицы

Размер адресной таблицы обычно приводится в расчете на порт, так как каждый порт содержит свой экземпляр адресной таблицы. Недостаточная емкость адресной таблицы может служить причиной замедления работы коммутатора и засорения сети избыточным трафиком.

Коммутаторы рабочих групп обычно поддерживают всего несколько адресов на порт. Коммутаторы отделов должны поддерживать несколько сотен адресов, а коммутаторы магистралей сетей – до нескольких тысяч, обычно 4000-8000 адресов.

Некоторые производители предлагают полезную возможность дополнительной поддержки общей адресной таблицы в модуле управления коммутатором.

6.3.4.4. Объем буфера обмена

Буферы портов предназначены для предотвращения потерь кадров при кратковременных перегрузках портов из-за пульсаций трафика. Например, для локальных сетей часто встречаются значения коэффициента пульсации трафика в диапазоне 50-100.

Обычно коммутаторы, предназначенные для работы в ответственных частях сети, имеют буферную память в несколько десятков или сотен килобайт на порт. Хорошо, когда эту память можно перераспределять между несколькими портами, так как одновременные перегрузки по нескольким портам маловероятны.

Дополнительным средством защиты может служить общий для всех портов буфер в модуле управления коммутатором. Такой буфер обычно имеет объем в несколько мегабайт.

6.3.4.5. Конструктивное исполнение коммутаторов

В конструктивном отношении коммутаторы, как и концентраторы, делятся на следующие типы:

1. автономные коммутаторы с фиксированным количеством портов;
2. модульные коммутаторы на основе шасси;
3. коммутаторы с фиксированным количеством портов, собираемые в стек.

Первый тип коммутаторов обычно предназначен для организации небольших рабочих групп. Обычно используется коммутационная матрица.

Модульные коммутаторы на основе шасси чаще всего предназначены для применения на магистрали сети. Поэтому они выполняются на основе какой-либо комбинированной схемы, в которой взаимодействие модулей организуется по быстродействующей шине или же на основе быстрой разделяемой памяти большого объема. Модули такого коммутатора выполняются на основе технологии «hot swap», то есть допускают замену на ходу, без выключения коммутатора, так как центральное коммутационное устройство не должно иметь перерывов в работе. Шасси обычно снабжается резервированными источниками питания и резервированными вентиляторами в тех же целях.

С технической точки зрения определенный интерес представляют стековые коммутаторы. Эти устройства представляют собой коммутаторы, которые могут работать автономно, так как выполнены в отдельном корпусе, но имеют специальные интерфейсы, которые позволяют их объединять в общую систему, работающую как единый коммутатор. Говорят, что в этом случае отдельные коммутаторы образуют стек. Обычно такой специальный интерфейс представляет собой высокоскоростную шину, которая позволяет объединить отдельные корпуса подобно модулям в коммутаторе на

основе шасси. Т.к. расстояние между корпусами больше, чем между модулями на шасси, скорость обмена по этой шине ниже, чем у модульных коммутаторов. Стековые коммутаторы занимают промежуточное положение между коммутаторами с фиксированным количеством портов и модульными, и могут применяться в сетях рабочих групп и отделов.

6.2.5. Дополнительные функции коммутаторов

Коммутаторы могут поддерживать помимо основных много полезных дополнительных функций, естественно, это отражается на их стоимости и, в ряде случаев, на производительности. Такие коммутаторы нужно обязательно конфигурировать, для выполнения основных функций коммутатор достаточно только подключить.

6.2.5.1. Управление потоком данных

Управление потоком данных коммутатор может применять с целью предотвращения потерь пакетов данных, которое может происходить при переполнении буферов коммутатора в периоды его временных перегрузок.

В дуплексном режиме, коммутатор использует собственный протокол MAC уровня, поэтому может применяться и любой метод управления. Например, **в стандарте IEEE 802.3x** определена процедура в виде специальных управляющих кадров, в которых указывается время, на которое получивший их узел должен полностью прекратить передачу данных. Такие кадры могут послать порты коммутатора, испытывающие временную перегрузку входных буферов своим соседям. Эта процедура довольно примитивна. Она не позволяет плавно регулировать входной поток коммутатора, указывая насколько его нужно уменьшить. Более эффективным решением является недогруженность линий связи. Обычно выбирается коэффициент загруженности линий связи в пределах 0.6 – 0.8.

В случае полудуплекса к портам коммутатора могут быть подключены PC, которые работают в полудуплексном режиме, или сегменты PC на концентраторах. В этом случае необходимо соблюдать протокол доступа к разделяемой среде сегментов. В этом случае методы управления входным потоком коммутатора, основаны на основном протоколе MAC своей технологии. Например, для Ethernet, используется два метода:

1. *Обратного давления*
2. *Агрессивного поведения порта коммутатора.*

Оба метода основаны на том, что в отличие от адаптера коммутатор может нарушать временные параметры доступа к среде.

1. *Обратное давление:* коммутатор посылает на выход порта, сегмент (или узел) которого слишком интенсивно работает, Jam – последовательность. В сегменте создается искусственная коллизия и передача кадров в нем на некоторое время прекратится.
2. *Агрессивное поведение порта:* после передачи кадра по общей среде каждая PC должна выдержать технологическую паузу прежде, чем она попытается снова захватить среду. Аналогично, после коллизии передающие PC должны выдержать случайную паузу. Если же кадр в сегменте передавал порт коммутатора или в коллизии участвовал кадр от порта коммутатора, то этот порт

перед попыткой следующего захвата общей среды сегмента для передачи очередного кадра может ожидать время, которое будет чуть меньше протокольного. Например, технологическая пауза не 9,6 мкс (Ethernet) а 9,1 мкс. Таким образом, среда компьютерам не достанется. Коммутатор пользуется этим механизмом, адаптивно увеличивая степень своей агрессивности по мере необходимости.

Методы управления потоком, которые используются в полудуплексном режиме, достаточно гибкие. Они позволяют чередовать передачу нескольких кадров с приемом одного.

6.2.5.2. Поддержка алгоритма Spanning Tree

Алгоритм покрывающего дерева – Spanning Tree Algorithm (STA) позволяет коммутаторам автоматически определять древовидную конфигурацию связей в сети при произвольном соединении портов между собой. Для нормальной работы коммутатора требуется отсутствие замкнутых маршрутов в сети. Эти маршруты могут создаваться администратором специально для образования резервных связей или же возникать случайным образом.

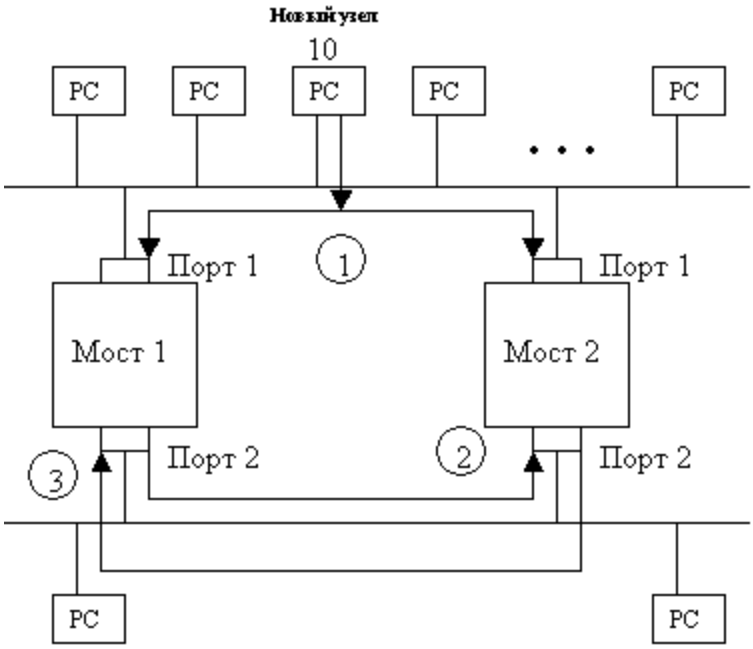


Рис. 6.10. Влияние замкнутых маршрутов на работу мостов

Результаты наличия петли перечислены ниже.

1. «Размножение» кадра с широковещательным, групповым или неизвестным (отсутствует в таблице) адресом получателя, то есть появление нескольких его копий (в данном случае – двух, но если бы сегменты были соединены тремя мостами – то трех и т.д.)
2. Бесконечная циркуляция обеих копий кадра по петле в противоположных направлениях, а значит, засорение сети ненужным трафиком.

3. Постоянная перестройка мостами своих адресных таблиц, так как кадр с адресом источника 10 будет появляться то на одном порту, то на другом. Древовидные структуры гарантируют наличие только одного пути между любыми двумя сегментами. Тогда кадры от каждой станции будут поступать в мост всегда с одного и того же порта, и мост сможет правильно решать со стороны какого порта действительно находится станция.

Алгоритм Spanning Tree описан **в стандарте IEEE 802.1D**, который определяет принципы работы прозрачных мостов. Коммутаторы находят покрывающее дерево адаптивно, с помощью обмена служебными пакетами. Реализация в коммутаторе алгоритма STA очень важна для работы в больших сетях – если коммутатор не поддерживает этот алгоритм, то администратор должен самостоятельно определить, какие порты нужно перевести в заблокированное состояние, чтобы исключить петли. К тому же при отказе какого-либо кабеля, порта или коммутатора администратор должен, во-первых, обнаружить факт отказа, а во-вторых, ликвидировать последствия отказа, переведя резервную связь в рабочий режим путем активации некоторых портов. При поддержке коммутаторами сети протокола Spanning Tree отказы обнаруживаются автоматически, за счет постоянного тестирования связности сети служебными пакетами. После обнаружения потери связности протокол строит новое покрывающее (еще называется ”остовное”) дерево, если это возможно, и сеть автоматически восстанавливает свою работоспособность. Алгоритм Spanning Tree определяет активную конфигурацию сети за три этапа.

1. Сначала в сети определяется корневой коммутатор (root switch), от которого строится дерево. Корневой коммутатор может быть выбран автоматически или назначен администратором. При автоматическом выборе корневым становится коммутатор с меньшим значением MAC – адреса его блока управления (если коммутатор поддерживает удаленное управление, то соответствующий блок имеет свой MAC – адрес, тогда как стандартно ни сам коммутатор, ни его порты MAC – адресов не имеют).
2. Затем, на втором этапе, для каждого коммутатора определяется корневой порт (root port) – это порт, который имеет по сети из коммутаторов кратчайшее расстояние до любого из портов корневого коммутатора. При одинаковом расстоянии выбирается порт с меньшим номером.
3. На третьем этапе для каждого сегмента сети на концентраторах выбирается так называемый назначенный порт (designated), то есть тот порт, который имеет кратчайшее расстояние от данного сегмента до корневого коммутатора. Для каждого узла (коммутатора, маршрутизатора или компьютера), имеющего двух- точечные соединения с коммутаторами сети выбирается designated коммутатор и designated порт у него. В качестве назначенного выбирается тот коммутатор, у которого расстояние от корневого порта до корневого коммутатора будет минимальным, а в качестве назначенного порта – тот порт, который подключен к узлу. При одинаковом расстоянии выбирается коммутатор или порт с меньшим номером. Корневой и назначенный порт могут выбираться не по маршруту с минимальным расстоянием, а по маршруту с максимальной пропускной способностью.
4. После определения корневых и назначенных портов каждый коммутатор блокирует остальные порты, которые не попали в эти два класса портов.

Можно математически доказать, что при таком выборе активных портов сети исключаются петли и оставшиеся связи образуют покрывающее дерево, если оно в принципе может быть построено при существующих связях в сети.

Основным недостатком протокола STA 802.1D является достаточно большое время реконфигурации сети после отказа связи (до 50 секунд). Для ускорения работы протокола (до нескольких секунд) принят новый **стандарт IEEE 802.1D-2004**.

6.2.5.3. Поддержка агрегированных связей

Агрегирование – объединение нескольких физических линий связи в один логический канал между двумя узлами преследует две цели:

- увеличение пропускной способности участка сети;
- повышение надежности участка сети.

На рис. 6.11 коммутаторы 1 и 3 соединены тремя параллельными линиями связи, что повышает производительность этого участка в три раза. Такое решение может быть более эффективным и экономически выгодным по сравнению с заменой линии на более скоростную. Например, объединение 3-х линий по 100 Мбит/с будет выгоднее замены на 1 линию 1Гбит/с в том случае, если замены потребует и сам коммутатор, а более высокая скорость в обозримом будущем не понадобиться.

При отказе одной из составляющих агрегированного канала, который часто называют *транком каналов*, трафик распределяется между оставшимися линиями (рис. 6.11). На рисунке 6.11 примером такой ситуации является транк 2, в котором один из физических каналов (центральный) отказал, так что все кадры передаются по оставшимся двум каналам. Этот пример демонстрирует повышение надежности при агрегировании.

Механизм агрегирования линий связи **стандартизирован в IEEE 802.3ad**.

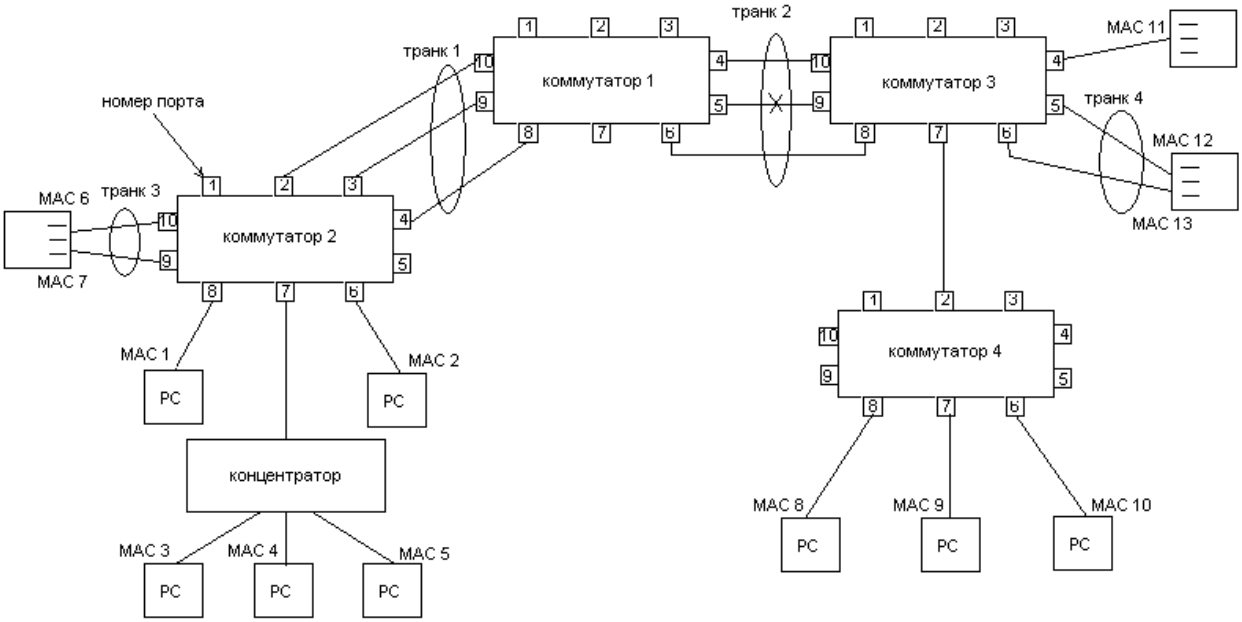


Рис. 6. 11. Агрегирование линий связи

Агрегирование линий связи используется как для связей между портами коммутаторов локальной сети, так и для связей компьютеров с коммутатором. Чаще всего этот вариант выбирают для скоростных и ответственных серверов. В этом случае

все сетевые адаптеры одного компьютера, которые объединяются в транк, разделяют один и тот же сетевой адрес. Поэтому для протокола IP или другого протокола сетевого уровня порты транка неразличимы, что соответствует концепции единого логического канала, лежащей в основе агрегирования.

Между двумя соседними коммутаторами агрегированный канал связи должен быть сконфигурирован в качестве транка с обеих сторон, т.е. на каждом коммутаторе. При этом все порты коммутатора, принадлежащие транку, считаются одним логическим портом, который фигурирует в таблице коммутации данного коммутатора. Например, на рис. 6.11 для коммутатора 2 таблица коммутации может выглядеть так:

MAC адрес	№ порта
MAC 1	8
MAC 2	6
MAC 3	7
MAC 4	7
MAC 5	7
MAC 6	AL-11
MAC 7	AL-11
MAC 8	AL-11
MAC 9	AL-12
MAC 10	AL-12

AL-11-логический порт объединяет физические порты 2,3,4

AL-12-логический порт объединяет физически порты 9,10

После конфигурирования коммутаторов не будет возникать размножение и зацикливание кадров с неизвестными, широковещательными и групповыми адресами в линиях транка, которые иначе воспринимались бы как петля. Теперь любой кадр, который нужно послать в агрегированный порт (с известным адресом или широковещательным) будет послан только в один из физических портов транка.

Если администратор сети хочет использовать все её топологические возможности, то технику агрегирования линий связи ему необходимо применять одновременно с алгоритмом покрывающего дерева. Для STA транк должен выглядеть как одна линия связи. Тогда топология сети кроме транков может содержать и одинарные резервные линии связи.

6.2.5.3. Трансляция протоколов канального уровня

Коммутаторы могут выполнять трансляцию одного протокола канального уровня локальной сети в другой, например Ethernet в FDDI, Tokeng Ring в Fast Ethernet и т.п. При этом они работают по тем же алгоритмам, что и транслирующие мосты, то есть в соответствии со **спецификациями IEEE 802.1H и RFC 1042**, определяющими правила преобразования полей кадров разных протоколов. Это возможно, так как все конечные узлы локальных сетей имеют уникальные адреса одного и того же формата независимо от поддерживаемого протокола (Ethernet, FDDI, Tokeng Ring).

Есть только одно ограничение – кадры с размером поля данных, превышающим максимально допустимое в технологии Ethernet (>1500 байт), в сеть Ethernet из других сетей (например, Tokeng Ring и FDDI) передаваться не могут. Они отбрасываются. Для осуществления возможности такой передачи коммутатор и узлы всей сети должны были бы поддерживать протокол сетевого уровня IP, который может фрагментировать

пакеты. Поэтому данная задача выходит за пределы компетенции коммутаторов и решается маршрутизаторами.

6.2.5.4. Дополнительные возможности коммутаторов по фильтрации трафика

Многие коммутаторы позволяют администраторам задавать дополнительные условия фильтрации кадров наряду со стандартными условиями их фильтрации по таблице коммутации (только в определённые порты). Такие дополнительные фильтры называются пользовательскими или списками доступа (access list).

Наиболее простыми являются пользовательские фильтры на основе MAC – адресов станций. При этом отбрасываются кадры с определенными MAC – адресами. Например, пользователю, работающему на компьютере с данным MAC – адресом, полностью запрещается доступ к ресурсам другого сегмента сети или к какому серверу.

Пользовательские фильтры могут быть основаны на содержимом полей протоколов верхних уровней. В последнем случае администратор должен выполнить большой объем ручной работы по заданию положения поля относительно начала кадра и его требуемому значению. Обычно фильтры допускают комбинацию нескольких условий с помощью логических операторов AND и OR. Наложение дополнительных условий фильтрации может снизить производительность коммутатора, так как вычисление булевых выражений требует проведения дополнительных вычислений процессорами портов. Поэтому такие виды фильтрации целесообразнее поручить маршрутизаторам.

6.2.5.5. Приоритетная обработка кадров

Построение сетей на основе коммутаторов позволяет назначать приоритеты пакетам данных, причем делать это независимо от технологии сети. При этом коммутатор может быть сконфигурирован, например, так, чтобы передавать один низкоприоритетный пакет на каждые 10 высокоприоритетных пакетов. Для трафика разных приоритетов в коммутаторах организуются отдельные очереди.

Наиболее распространенный способ – приписывание приоритета портам коммутатора. Способ простой, но недостаточно гибкий. Так как, если к порту подключен не отдельный узел, а сегмент, то все узлы сегмента получат одинаковый приоритет.

Более гибкий способ назначения приоритета кадрам определён в **стандарте IEEE802.1p**. Стандарт определяет дополнительное поле из трех бит для хранения приоритета кадра независимо от технологии сети. Существует протокол, по которому сетевой адаптер может запросить у коммутатора один из 7-ми уровней приоритета для своего кадра. В дальнейшем при прохождении следующих коммутаторов кадр будет обрабатываться с этим приоритетом, т.е. такую возможность должны поддерживать все коммутаторы и сетевые адаптеры сети.

Существует возможность резервирования пропускной способности интерфейсов коммутатора для трафика разных приоритетов или индивидуальных потоков. Обычно коммутатор разрешает назначить приоритету или потоку минимальную скорость передачи данных, которая гарантируется в периоды перегрузок. Для коммутаторов ЛВС не существует стандартного протокола резервирования ресурсов. Поэтому, администратор сети должен сконфигурировать каждый коммутатор отдельно.

6.2.5.6. Виртуальные локальные сети

Технология виртуальных локальных сетей (VLAN) позволяет в сети, построенной на коммутаторах, создать изолированные группы узлов, между которыми не передается любой тип трафика, в том числе и широковещательный (рис.6.13.)

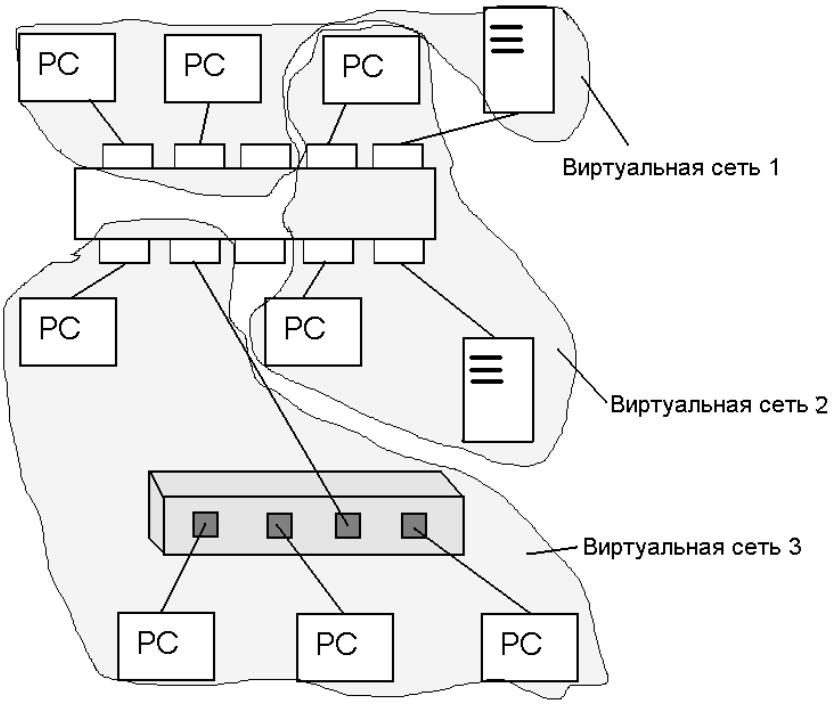


Рис. 6.13. Виртуальные сети, построенные на одном коммутаторе

Виртуальные сети являются основой для создания крупных маршрутизируемых сетей (виртуальные коммутируемые сети объединяются маршрутизатором). Преимуществом такого решения перед физически изолированными сегментами является гибкость состава узлов подсетей, списки которых можно изменять программным путем, не прибегая к физическому переключению. Один компьютер (чаще сервер) может быть отнесён сразу к нескольким подсетям. Принцип конструктивного построения таких коммутаторов аналогичен принципу построения многосегментных концентраторов (рис. 6.2).

Сегодня считается, что любая крупная сеть должна включать маршрутизаторы, иначе потоки ошибочных и широковещательных кадров будут периодически затапливать всю сеть через прозрачные для них коммутаторы, приводя ее в неработоспособное состояние. Вообще считается, что когда доля нормального широковещательного трафика в общем сетевом превосходит 20%, его необходимо изолировать. Широковещательные кадры активно генерируют, например, локальные сервера подсетей. Эта информация является не нужной для других подсетей.

При использовании технологии VLAN на коммутаторах одновременно решаются две задачи:

1. изоляция сетей друг от друга для управления правами доступа пользователей;
2. создание защитных барьеров на пути широковещательных штормов.

Для объединения виртуальных сетей в общую сеть требуется привлечение сетевого уровня. Он может быть реализован в отдельном маршрутизаторе, а может работать и в составе программного обеспечения коммутатора, который тогда становится комбинированным устройством – так называемый *коммутатором 3-го уровня* (см. 7.5.2.). Например, три изолированные виртуальные сети на рис.6.13 могут быть объединены в общую сеть как показано на рис.6.14.

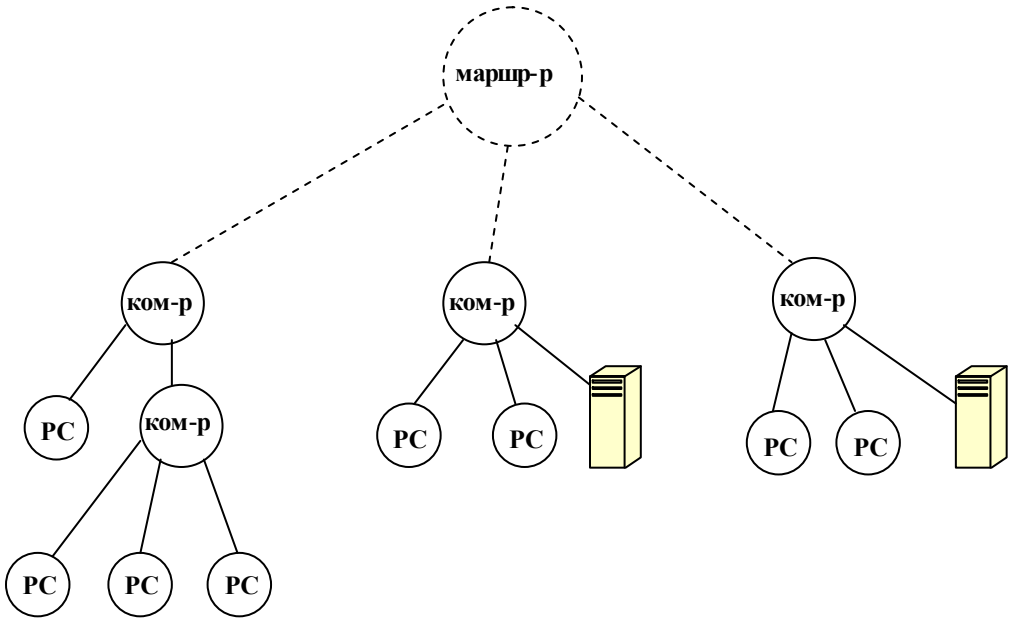


Рис. 6.14. Объединение виртуальных сетей

Технология VLAN долго реализовывалась разными производителями на основе фирменных стандартов пока в 1998г. не появился **стандарт IEEE 802.1Q.**

7. Объединение сетей на основе сетевого и транспортного уровня

Еще раз отметим **ограничения мостов и коммутаторов,** которые выполняют свои функции на канальном и физическом уровне:

1. Не допускаются петлевидные связи в сети, которые могут использоваться как для повышения надежности сети (резервные), так и для повышения пропускной способности сети (параллельная передача).

2. Слабая защита от широковещательных штормов. Поскольку коммутаторы передают кадры с широковещательными MAC адресами на все порты (во все подсети), то в большой коммутируемой сети он может занимать значительную часть ее полосы пропускания и снижать производительность сети. При использовании механизма VLAN получаются полностью изолированные подсети, которые не могут взаимодействовать между собой.

3. Сложность создания пользовательских фильтров, осуществляющих фильтрацию на основании полей вышележащих протоколов. При этом необходимо иметь дело с двоичным содержимым полей данных, так как содержимое пакетов сетевого и транспортного уровней на канальном уровне не обрабатывается.

4. Недостаточно гибкая система адресации. MAC- адреса жестко связаны с сетевыми адаптерами.

5. Возможностью трансляции протоколов канального уровня LAN обладают не все коммутаторы, и они не могут фрагментировать кадры со слишком большим полем данных при передаче их в сеть, которая поддерживает только кадры меньшего размера.

В функции сетевого уровня, на котором работают **маршрутизаторы, входит решение следующих задач**:

1. Передача пакетов между узлами в составных сетях, построенных на разных технологиях канального уровня (в том числе LAN и WAN).

2. Выбор для передачи пакетов одного из нескольких активных маршрутов, который был бы наилучшим по некоторому заданному критерию.

3. Фрагментация и последующая сборка пакетов, которые передаются из подсети с большей допустимой длиной поля данных в подсеть с меньшей допустимой длиной (например, из сети FDDI в сеть Ethernet).

4. Фильтрация пакетов по полям сетевого и транспортного уровня.

5. Изоляция широковещательного трафика внутри подсетей. Считается, что если широковещательный трафик в сети превышает 20% от общего трафика, то подсети необходимо разделить маршрутизатором.

Протоколы сетевого уровня обычно реализуются в виде программных модулей на конечных узлах (хостах) и промежуточных узлах - маршрутизаторах.

Маршрутизаторы могут быть реализованы в виде самостоятельных специальных устройств и на базе универсальной PC с несколькими сетевыми картами и соответствующим программным обеспечением (хотя сейчас оно входит в стандартные поставки популярных ОС).

7.1. Составная сеть (Internetwork)

Чтобы передать пакет от узла А к узлу В в составной сети (рис.7.1.), необходимо использовать средства сетевого уровня.

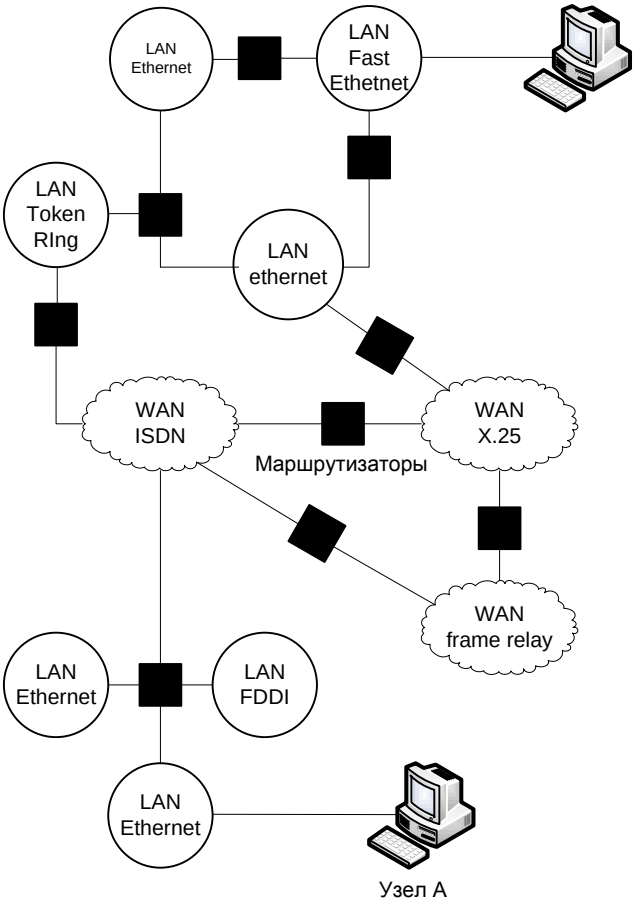


Рис. 7.1. Составная сеть, соединенная маршрутизаторами (черные прямоугольники)

Данные пользователя помещаются в поле данных пакета сетевого протокола, который передают маршрутизаторы между подсетями составной сети. Основная следующая служебная информация, которая содержится полях сетевого пакета:

1. Числовые адреса отправителя (А) и получателя (В).
2. Номер фрагмента пакета, если он разбивается на части при передаче между сетями с разными максимальными размерами пакетов.
3. Время жизни пакета (для уничтожения «заблудившихся» пакетов).
4. Качество услуги – критерий выбора маршрутизатора (с максимальной пропускной способностью, задержкой, надежностью и т. д.).

Все LAN-технологиях используют плоские MAC-адреса. WAN-технологии используют другую систему адресации – разную для разных типов сетей. Числовые

адреса вводят универсальную адресацию независимо от локальных адресов – номер сети и номер узла. Для стека TCP/IP назначаемыми являются и номер сети и номер узла. Поэтому этот способ подходит сетей, построенных на основе любых технологий. К примеру, для стека IPX/SPX номер узла – это его MAC-адрес, то есть такая адресация подходит только для сетей, построенных на основе LAN-технологий.

При передаче данных по составной сети маршрутизатор:

- извлекает пакет сетевого уровня из канального кадра сети – отправителя;
- если сеть получателя не подключена к данному маршрутизатору, то он определяет *сетевой адрес* следующего маршрутизатора в пути к сети получателя;
- по известному сетевому адресу определяет *локальный адрес* либо следующего маршрутизатора либо получателя, если сеть получателя подключена к данному маршрутизатору;
- вкладывает тот же сетевой пакет в новый кадр, соответствующий технологии следующей сети в маршруте или сети получателя (в кадре указывается локальный адрес следующего маршрутизатора или получателя);
- пересылает сформированный кадр в следующую промежуточную сеть или в сеть получателя.

7.2. Реализация межсетевого взаимодействия средствами стека TCP/IP

Благодаря огромной популярности сети Интернет стек протоколов TCP/IP приобрел доминирующее положение как в глобальных так и в локальных сетях. Поэтому организацию межсетевого взаимодействия мы будем рассматривать на примере его протоколов.

7.2.1.Типы адресов стека TCP/IP

В стеке TCP/IP используются три типа адресов:

- *локальные*, или аппаратные, которые используются для доставки данных в пределах подсети, построенной по определенной сетевой технологии (для LAN технологий это будут MAC-адреса);
- *сетевые,* или IP-адреса, которые используются для однозначной идентификации узлов в пределах всей составной сети;
- *символьные* доменные имена используются для идентификации узлов, к которым часто обращаются пользователи.

Все эти типы адресов присваиваются узлам составной сети независимо друг от друга. Один сетевой интерфейс в общем случае может иметь несколько адресов каждого типа.

В разных подсетях допустимы разные сетевые технологии, поэтому при создании стека TCP/IP предполагалось наличие разных типов локальных адресов. Если подсетью интерсети является локальная сеть, то локальный адрес — это MAC-адрес. Локальные адреса назначаются сетевым адаптерам и сетевым интерфейсам маршрутизаторов.

IP-адреса адреса состоят из 4 байт, например 107. 32. 17. 123. IP-адрес состоит из двух частей: номера сети и номера узла. Номера сетей назначаются либо централизованно, если сеть является частью Internet, либо произвольно, если сеть работает автономно. Маршрутизатор по определению входит сразу в несколько сетей. Поэтому каждый порт маршрутизатора имеет собственный IP-адрес. Конечный узел также может входить в несколько IP-сетей. В этом случае компьютер должен иметь несколько IP-адресов, по числу сетевых связей. Таким образом, IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение.

Для определения границы, отделяющей номер сети от номера узла, реализуются два подхода. Первый основан на понятии класса адреса, второй — на использовании масок.

- Класс адреса определяется значениями нескольких первых бит адреса. Например, в адресах класса А под номер сети отводится один байт, а остальные три байта — под номер узла, поэтому они используются в самых больших сетях, в адресах класса С номер сети занимает три байта, а для нумерации узлов используется только один байт.
- Другой способ определения, какая часть адреса является номером сети, а какая номером узла, основан на использовании маски. Маска — это число, которое используется в паре с IP-адресом; двоичная запись маски содержит единицы в тех разрядах, которые в IP-адресе должны интерпретироваться как номер сети. Маски являются эффективным средством структуризации IP-сетей. Они позволяют разделить одну сеть на несколько подсетей. Маски одинаковой длины используются для деления сети на подсети равного размера, а маски переменной длины — для деления сети на подсети разного размера. Использование масок подразумевает, что протоколы маршрутизации (построения таблиц маршрутизации) и сами маршрутизаторы их поддерживают.

В стеке TCP/IP применяется доменная система имен, которая имеет иерархическую древовидную структуру, допускающую использование в имени произвольного количества составных частей (рис.7.2).

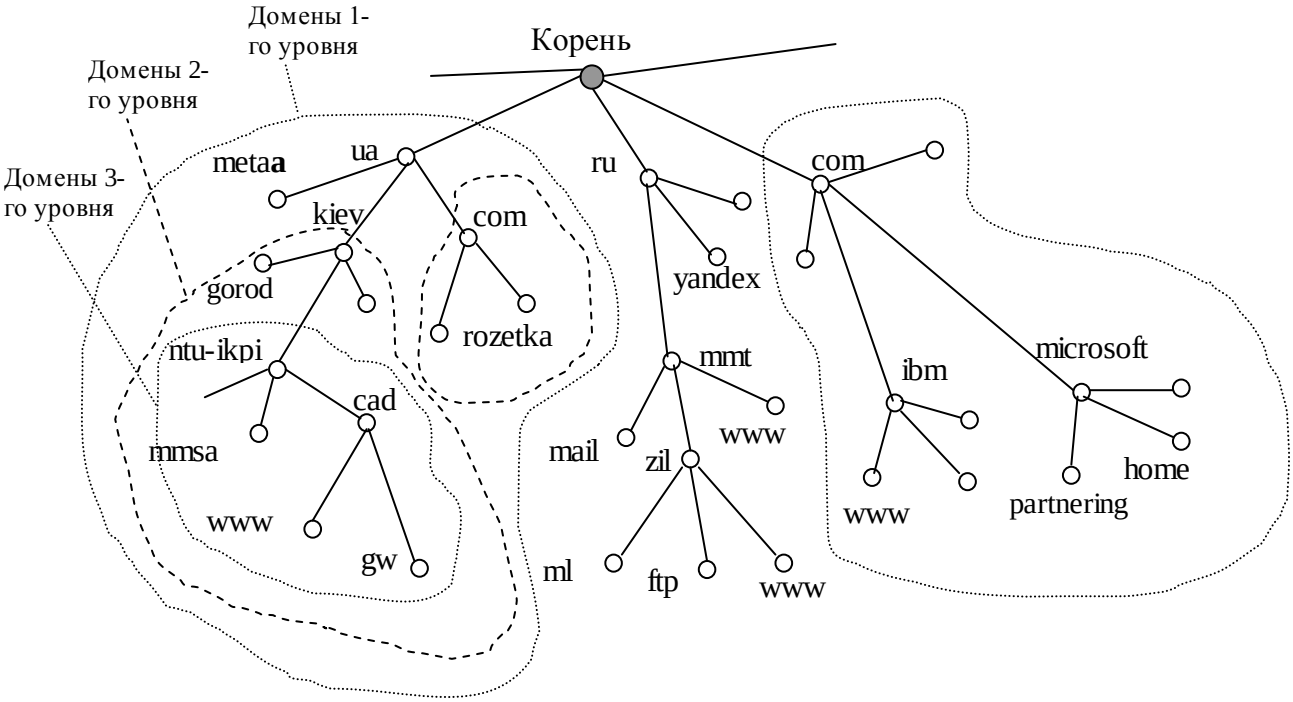


Рис. 7.2. Пространство доменных имен

Дерево имен начинается с корня. Составляющие полного символьного имени разделяются точкой и перечисляются в следующем порядке: сначала простое имя конечного узла, затем имя группы узлов (например, имя организации - домена уровня N), затем имя более крупной группы (домена уровня N-1) и так до имени домена уровня 1. Домены 1-го уровня объединяются в корневой домен.

Совокупность имен, у которых несколько старших составных частей совпадают, образуют домен имен (domain). Например, в один из доменов 2-го уровня на рис.7.2. входят имена, у которых две старшие части всегда равны kiev.ua. Если один домен входит в другой домен как его составная часть, то такой домен могут называть поддоменом (subdomain). Хорошей аналогией домена является каталог файловой системы. (Понятие доменов имен стека TCP/IP не следует путать с доменами Windows NT).

Имена назначаются централизованно, если сеть является частью Internet, в противном случае — локально. В Internet корневой домен управляется центром InterNIC. Домены верхнего уровня назначаются для каждой страны (например, us– США, uk-Великобритания), а также на организационной основе (com— коммерческие организации, net — организации, поддерживающие сети, edu — образовательные организации и т.д.). Имена этих доменов должны следовать международному стандарту ISO 3166.

Каждый домен администрируется отдельной организацией, которая обычно разбивает свой домен на поддомены и передает функции администрирования этих поддоменов другим организациям. Чтобы получить доменное имя, необходимо зарегистрироваться в какой-либо организации, которой InterNIC делегировал свои полномочия по распределению имен доменов. Таким образом, разделение имени на части позволяет *разделить административную ответственность* за назначение уникальных имен между различными организациями в пределах своего уровня иерархии.

7.2.2. Разрешение адресов

В IP-сетях разные типы адресов используются на разных этапах передачи данных. Поскольку никакого алгоритмического соответствия между разными типами адресов одного узла нет, то необходимо использовать дополнительные таблицы или службы, чтобы узел сети однозначно определялся по каждому из них. Процедура нахождения соответствия между разными типами адресов называется процедурой разрешения адресов.

Отображение доменных имен на IP-адреса

Соответствие между **доменными именами и IP-адресами** может устанавливаться как средствами локального компьютера с использованием файла hosts, так и с помощью централизованной службы DNS.

DNS (Domain Name System)— это централизованная служба, основанная на распределенной базе отображений «доменное имя — IP-адрес». Служба DNS использует в своей работе протокол типа «клиент-сервер». DNS-серверы поддерживают распределенную базу отображений, а DNS-клиенты обращаются к серверам с запросами о разрешении доменного имени в IP-адрес.

Для каждого домена имен создается свой DNS-сервер. Обычно сервер домена хранит только имена своего первого уровня. Например, DNS-сервер домена ua на рис.5.11 будет хранить отображения для имен meta.ua , kiev.ua, com.ua , и др., а сервер домена kiev.ua – ntu-ikpi.kiev.ua, gorod.kiev.ua и т.д. Каждый DNS-сервер кроме таблицы отображений имен содержит IP-адреса DNS-серверов своих поддоменов. Эти ссылки связывают отдельные DNS-серверы в единую службу DNS. Для обслуживания корневого домена выделено несколько дублирующих друг друга DNS-серверов, IP-адреса которых являются широко известными.

Процедура определения IP-адреса по доменному имени заключается в последовательном просмотре DNS-серверов доменов, которые входят в имя хоста, начиная с корневого домена. При этом предварительно проверяется кэш и текущий каталог.

Чтобы определить IP-адрес по доменному имени компьютер сначала просматривает свой файл hosts. Не найдя искомого адреса, он обращается к своему DNS-клиенту, который по наиболее распространенной схеме перепоручает эту работу локальному DNS-серверу. Например, компьютеру a1.mmt.ru на рис.7.2 нужно найти IP-адрес компьютера gorod.kiev.ua.

- DNS-клиент запрашивает локальный DNS-сервер, то есть сервер поддомена (mmt.ru), к которому принадлежит имя клиента (a1.mmt.ru);
- если локальный DNS-сервер знает ответ, то он сразу же возвращает его клиенту; это может соответствовать случаю, когда запрошенное имя входит в тот же поддомен, что и имя клиента, а также может соответствовать случаю, когда сервер уже узнавал данное соответствие для другого клиента и сохранил его в своем кэше;
- если же локальный сервер не знает ответ, то он выполняет к корневому DNS-серверу;
- корневой сервер отвечает адресом DNS-сервера, который обслуживает домен, заданный в старшей части запрошенного имени (ua);
- локальный сервер делает запрос следующему DNS-серверу, который отсылает его к DNS-серверу нижнего поддомена (kiev.ua), и т. д., пока не будет найден DNS-сервер, в котором хранится нужное соответствие. Этот сервер и дает окончательный ответ (ответ даст сервер домена kiev.ua).
- получив ответ, локальный DNS-сервер передает его клиенту.

Отображение IP-адресов на локальные адреса

Для определения **локального адреса по IP-адресу** используется протокол *ARP (Address Resolution Protocol).* Необходимость в обращении к протоколу ARP возникает каждый раз, когда модуль IP передает пакет нижележащему канальному протоколу, например, Ethernet. IP-адрес узла назначения известен модулю IP. Требуется на его основе найти MAC-адрес узла назначения.

Работа протокола ARP в локальных и глобальных сетях имеет свои особенности. Рассмотрим работу протокола в локальных сетях.

Каждый сетевой адаптер и порт маршрутизатора знает свои MAC и IP адрес, а также поддерживает ARP-таблицу для определения соответствия между IP- адресами и MAC-адресами других узлов той же сети.

Записи в таблице могут быть динамическими и статическими. Статические записи создаются вручную с помощью утилиты arp и не имеют срока жизни. Динамические записи создаются модулем протокола ARP и имеют срок жизни. Если запись не обновлялась в течение определенного времени (порядка нескольких минут), то она исключается из таблицы. Поскольку такой способ хранения информации называют кэшированием, ARP-таблицы иногда называют ARP-кэш.

Итак, после того как модуль IP обратился к модулю ARP с запросом на разрешение адреса, сначала происходит поиск в ARP-таблице. Если искомый IP- адрес в таблице отсутствует, то IP-пакет, для которого нужно определить локальный адрес, ставится в очередь, а протокол ARP формирует ARP-запрос. Запрос вкладывается в кадр канального протокола и рассылается широковещательно по сети. В запросе указывается MAC и IP адрес отправителя и искомый IP- адрес, для которого нужно определить соответствующий MAC- адрес.

Все узлы локальной сети получают ARP-запрос и сравнивают искомый IP-адрес с собственным. Узел, опознавший свой IP-адрес, присылает ответ непосредственно отправителю. Если в сети нет машины с искомым IP-адресом, то ARP-ответа не будет. Протокол IP просто уничтожает IP-пакеты, направляемые по этому адресу. (Заметим, что протоколы верхнего уровня не могут отличить случай повреждения сети Ethernet от случая отсутствия машины с искомым IP-адресом).

Получив ARP-ответ, модуль ARP делает динамическую запись в своей таблице. ARP-таблицы пополняются не только за счет ARP-ответов, но и за счет чужих ARP-запросов, поскольку в них содержится IP и MAC- адрес отправителя.

7.2.3.Краткая характеристика протоколов стека TCP/IP

В стеке TCP/IP определены четыре уровня. Каждый из этих уровней ориентирован на решение ряда задач по организации надежной и производительной работы составной сети, части которой построены на основе разных сетевых технологий. Так как стек TCP/IP был разработан до появления модели взаимодействия открытых систем OSI, то соответствие уровней стека TCP/IP уровням модели OSI не совсем точно (рис.7.3).

Уровень OSI	**Названия протоколов**	**Уровень TCP/IP**
Прикладной	Telnet, FTP, SMTP, HTTP, SNMP, DNS, SSH, и др.	Прикладной
Представительный	SSL	
Сеансовый	TCP,	Основной уровень
Транспортный	UDP	
Сетевой	IP, RIP,OSPF,ARP,ICMP	Уровень Межсетевого взаимодействия
Канальный	Ethernet, Token Ring, FDDI, SLIP, PPP, HDLC, Frame relay, ATM	Уровень сетевых интерфейсов (конкретные протоколы стеком не регламентируется)
Физический	Спецификации для разных типов кабеля (например, 100Base TX)	

Рис. 7. 3. Соответствие уровней стека TCP/IP семиуровневой модели OSI

Прикладной уровень

Прикладной уровень объединяет все службы, предоставляемые системой пользовательским приложениям. За долгие годы использования в сетях различных стран и организаций стек TCP/IP накопил большое количество протоколов и служб прикладного уровня. Прикладной уровень реализуется программными системами, построенными в архитектуре клиент-сервер, базирующимися на протоколах нижних уровней. В отличие от протоколов остальных трех уровней, протоколы прикладного уровня занимаются деталями конкретного приложения и «не интересуются» способами передачи данных по сети. Этот уровень постоянно расширяется за счет присоединения к старым, прошедшим многолетнюю эксплуатацию сетевым службам типа Telnet, FTP, TFTP, DNS, SNMP, HTTP сравнительно новых служб таких как, например, IMAP4, DHCP и др.

Краткая справка:

HTTP (Hypertext Transfer Protocol) – используется клиентами и серверами WEB для обмена запросами на передачу файлов и самими файлами. Браузер клиента устанавливает TCP -соединение с сервером и отправляет запрос на передачу определенного файла. В ответ сервер посылает файл, который отображается браузером в виде WEB –страницы. HTTP – сообщения также содержат разнообразные поля с информацией о системах, между которыми установлено соединение.

HTTPS или S-HTTP (Secure Hypertext Transfer Protocol) – используется в транзакциях между клиентами и серверами WEB для авторизации пользователей и шифрования передаваемых данных. Протокол HTTPS работает поверх протокола SSL.

FTP (File Transfer Protocol) – применяется для передачи файлов между TCP/IP – системами. Клиент FTP просматривает структуру каталога на сервере, к которому подключен, и выбирает файлы для пересылки. В работе протокола применяются 2 отдельных порта. Подключаясь к серверу, клиент FTP использует для установки управляющего соединения TCP – порт 21. Это соединение остается пока клиент его не прервет. При попытке загрузки файла программа открывает второе TCP –соединение с портом 20 для передачи данных, которое закрывается после завершения передачи файла. Особенность FTP еще и в том, что в большинстве TCP/IP –систем он представляет собой не просто протокол, которое используют другие приложения, а является самостоятельным приложением.

TFTP (Trivial File Transfer Protocol) – сокращенная версия FTP. Вместо TCP в нем используется UDP. Этот протокол не в отличии от полного не поддерживает авторизацию и интерфейсные функции. Первоначально он разрабатывался для бездисковых станций, которым необходимо копировать исполняемые загрузочные файлы с сетевого сервера.

SMTP (Simple Mail Transfer Protocol) – применяется почтовыми серверами для обмена сообщениями по сети.

POP3 (Post Office Protocol) – один из протоколов, применяемых клиентами электронной почты для доставки сообщений с почтового сервера.

IMAP4 (Internet Mail Access Protocol) – почтовый протокол, с помощью которого клиенты получают сообщения с почтового сервера. Протокол обладает большими возможностями, чем POP3. Он, например, позволяет пользователю создавать отдельные папки для хранения сообщений на сервере.

NTP (Network Time Protocol) – служит для синхронизации часов компьютеров в сети.

DNS (Domain Name System) – используется в TCP/IP системах для преобразования доменных имен хостов в IP – адреса.

DHCP (Dynamic Host Configuration Protocol) – применяется в сети для получения рабочими станциями от сервера информации о параметрах конфигурации стека TCP/IP.

SNMP (Simple Network Management Protocol) – протокол управления сетью, который используется сетевыми администраторами для сбора информации о различных узлах сети. С помощью сообщений SNMP встроенные в узлы программы – агенты собирают статистические сведения и передают их дистанционно на центральную консоль управления сетью.

Telnet – программа для эмуляции командной строки терминала, позволяющая пользователю подключиться к удаленному компьютеру и запускать на нем команды и программы.

Уровень сетевых интерфейсов

Идеологическим отличием архитектуры стека TCP/IP от многоуровневой организации других стеков является интерпретация функций самого нижнего уровня — *уровня сетевых интерфейсов*. Протоколы этого уровня должны обеспечивать интеграцию в составную сеть сетей разных технологий. Отсюда следует, что этот уровень нельзя определить раз и навсегда. Уровень сетевых интерфейсов в протоколах TCP/IP не регламентируется, но он поддерживает все популярные стандарты физического и канального уровней: для локальных сетей это Ethernet, Token Ring, FDDI, Wi-Fi, для глобальных сетей — протоколы соединений «точка-точка» SLIP, PPP, протоколы территориальных сетей с коммутацией пакетов X. 25, frame relay, ATM и др. Обычно при появлении новой технологии локальных или глобальных сетей она быстро включается в стек TCP/IP.

Уровень межсетевого взаимодействия

Стержнем всей архитектуры является уровень межсетевого взаимодействия, который реализует концепцию передачи пакетов в режиме без установления соединений, то есть дейтаграммным способом. Именно этот уровень обеспечивает возможность перемещения пакетов по сети по наиболее рациональному маршруту. Этот уровень также называют уровнем internet, указывая тем самым на основную его функцию — передачу данных через составную сеть.

Основным протоколом сетевого уровня (в терминах модели OSI) в стеке является протокол IP (Internet Protocol). IP протокол изначально проектировался как протокол передачи пакетов в больших составных сетях. Поэтому он хорошо работает в сетях со сложной топологией, рационально используя наличие в них подсетей и экономно расходуя пропускную способность низкоскоростных линий связи. **Главной задачей IP протокола** является передача пакетов между конечными узлами (хостами) через промежуточные маршрутизаторы на основании их таблиц оптимальных маршрутов.

Так как протокол IP является дейтаграммным протоколом, он не гарантирует доставку пакетов до узла назначения и не занимается повторной отправкой испорченных и потерянных пакетов, при необходимости это делает протокол транспортного уровня TCP.

Важное свойство IP протокола – способность фрагментировать пакет с длинным полем данных при передаче через сеть, допускающую только кадры с меньшим полем данных. Сборка исходного сетевого пакета происходит у получателя, т.к. фрагменты пакета могут следовать разными маршрутами. При потере или искажения одного из фрагментов все остальные отбрасываются, поскольку за надежность доставки IP протокол не отвечает.

Контрольная сумма вычисляется только по заголовку, а не по всему IP пакету. Это повышает скорость обработки. Поскольку время жизни, указанное в заголовке пакета, должно модифицироваться каждым промежуточным маршрутизатором, то и контрольная сумма должна каждый раз пересчитываться, а за надежность доставки содержимого пакета IP протокол все равно не отвечает.

К уровню межсетевого взаимодействия относятся также все протоколы, связанные с составлением и модификацией таблиц маршрутизации, такие как протоколы сбора маршрутной информации RIP (Routing Internet Protocol) и OSPF (Open Shortest Path First), протокол разрешения сетевых адресов в локальные ARP, протокол группового управления IGMP, а также протокол межсетевых управляющих сообщений ICMP (Internet Control Message Protocol). Последний протокол предназначен для обмена информацией об ошибках между маршрутизаторами сети и узлом-источником пакета. С помощью специальных пакетов ICMP сообщает о невозможности доставки пакета, о превышении времени жизни или продолжительности сборки пакета из фрагментов, об аномальных величинах параметров, об изменении маршрута пересылки и типа обслуживания, о состоянии системы и т. п.

Основной уровень

За надежность передачи данных между двумя конечными узлами отвечает *основной уровень* стека TCP/IP, называемый также *транспортным.*

На этом уровне функционируют протокол управления передачей TCP (Transmission Control Protocol) и протокол дейтаграмм пользователя UDP (User Datagram Protocol).

Поскольку сетевой уровень не гарантирует, что все пакеты будут доставлены в место назначения целыми и невредимыми или придут в том же порядке, в котором они были отправлены, то эту задачу решает **TCP протокол**. Протокол TCP обеспечивает надежную передачу сообщений между удаленными прикладными процессами за счет образования логических соединений, т.е. это протокол с установлением соединения между получателем и отправителем.

Этот протокол позволяет объектам на компьютере-отправителе и компьютере-получателе поддерживать обмен данными в дуплексном режиме (параллельная пересылка данных в обоих направлениях отправитель – получатель). TCP позволяет без ошибок доставить сформированный на одном из компьютеров поток байт в любой другой компьютер, входящий в составную сеть. TCP делит поток байт, идущих от процесса– отправителя, на части — сегменты, нумерует их и передает ниже лежащему уровню межсетевого взаимодействия IP. Пересылка пакетов в протоколе TCP осуществляется методов скользящего окна: с подтверждением получения пакетов с помощью квитанций от получателя и повторной отсылкой испорченных пакетов отправителем в том случае, если он (отправитель) не получил квитанцию в течении времени таймаута. После того как все сегменты в пакетах будут доставлены средствами протокола межсетевого взаимодействия IP в пункт назначения, протокол TCP восстанавливает их исходную последовательность и выстраивает в непрерывный поток байт.

Как правило, размер окна устанавливается в стартовых файлах сетевого программного обеспечения. Впоследствии, при установлении соединения и в процессе обмена данными обе стороны TCP- соединения могут динамически его изменять. TCP– соединение является дуплексным, и подтверждения для данных, идущих в одном направлении, могут передаваться с данными, идущими в противоположном направлении. Принимающая сторона может объявлять в очередной квитанции новое окно приема исходя из наличия свободного места в своем буфере приема. Но и сторона– отправитель может по собственной инициативе уменьшить размер окна,

запрошенного получателем, если сеть работает ненадежно (часто требуются повторные передачи).

Протокол UDP обеспечивает передачу прикладных пакетов дейтаграммным способом, как протокол IP, и выполняет только функции связующего звена между сетевым протоколом и многочисленными службами прикладного уровня или пользовательскими процессами. Протокол UDP может только обнаруживать ошибки передачи данных (по контрольной сумме, которая вычисляется по всему пакета), но не исправлять их. В случае обнаружения ошибки пакет просто отбрасывается.

Поскольку протокол работает быстрее, чем TCP, но не гарантирует доставки пакетов, он может использоваться для передачи единичных сообщений (например, протоколов DNS, DHCP) или мультимедийного трафика реального времени. Каждый UDP –пакет переносит отдельное сообщение прикладного процесса. Сообщения могут иметь переменную длину, не превышающую длину поля данных нижележащего протокола IP, которая, в свою очередь, ограничена максимально допустимой длиной поля данных нижележащего канального протокола (например, Ethernet). Поэтому, если буфер UDP переполняется, то сообщение приложения отбрасывается.

Порты. Сокеты

В то время как задачей сетевого уровня, к которому относится протокол IP, является передача данных между парами соседних узлов составной сети (компьютером и портом маршрутизатора, между портами двух соседних маршрутизаторов), задача транспортного уровня, которую решают протоколы TCP и UDP, заключается в передаче данных между любыми *прикладными процессами,* выполняющимися на любых узлах сети. Каждый компьютер может выполнять несколько процессов, более того, прикладной процесс тоже может иметь несколько точек входа, выступающих в качестве адреса назначения для пакетов данных. Поэтому, после того как пакет средствами протокола IP доставлен в компьютер-получатель, данные необходимо направить конкретному процессу-получателю. С другой стороны, различные приложения передают в сеть свои пакеты через общий IP протокол. Процедуру приема данных от разных прикладных служб выполняют протоколы TCP и UDP и называется она *мультиплексированием*. Обратная процедура распределения пакетов от сетевого протокола IP по прикладным процессам, выполняемая этими транспортными протоколами, называется *демультиплексированием*.

Протоколы TCP и UDP ведут для каждого порта две очереди: очередь пакетов, поступающих в данный порт из сети, и очередь пакетов, отправляемых данным портом в сеть. Пакеты, поступающие на транспортный уровень, организуются операционной системой в виде множества очередей к точкам входа различных прикладных процессов. В терминологии TCP/IP такие системные очереди называются *портами,* причем входная и выходная очередь одного приложения рассматриваются как один порт. Порты идентифицируются номерами. Таким образом, **номера портов идентифицируют приложения и прикладные процессы** (рис.7.4.). Для серверных модулей общедоступных служб, таких как FTP, HTTP, DNS и т.д., назначаются хорошо известные стандартные номера портов (например, номер 21 закреплен за службой удаленного доступа к файлам FTP, а 23 — за службой удаленного управления telnet). *Назначенные номера* являются уникальными в *пределах Интернета* и назначаются приложениям *централизованно* в пределах 0 – 1023. Для серверных модулей менее распространенных приложений номера могут назначаться их разработчиками *локально*. Эти номера являются *статическими*, т.е. постоянными. Для других приложений, в том числе и для клиентов известных служб FTP, HTTP, telnet и т.д. ОС в ответ на поступление запроса от приложения выделяет ему *динамически* первый свободный номер из диапазона 1024 – 65535. После завершения работы приложения, номер его

порта освобождается и может быть назначен другому приложению. Номера портов *в пределах одного компьютера* должны быть уникальными отдельно для TCP –протокола и отдельно для UDP – протокола. Два приложения, которые используют разные транспортные протоколы, могут получить одинаковые номера портов (например, одно – 1520 TCP, другое – 1520 UDP). Приложению, которое может обращаться по выбору к протоколу TCP или UDP (например, DNS) могут назначаться совпадающие номера TCP- и UDP- портов.

Аналогично, могут совпадать номера портов, которые выделяют приложениям разные компьютеры одной сети.

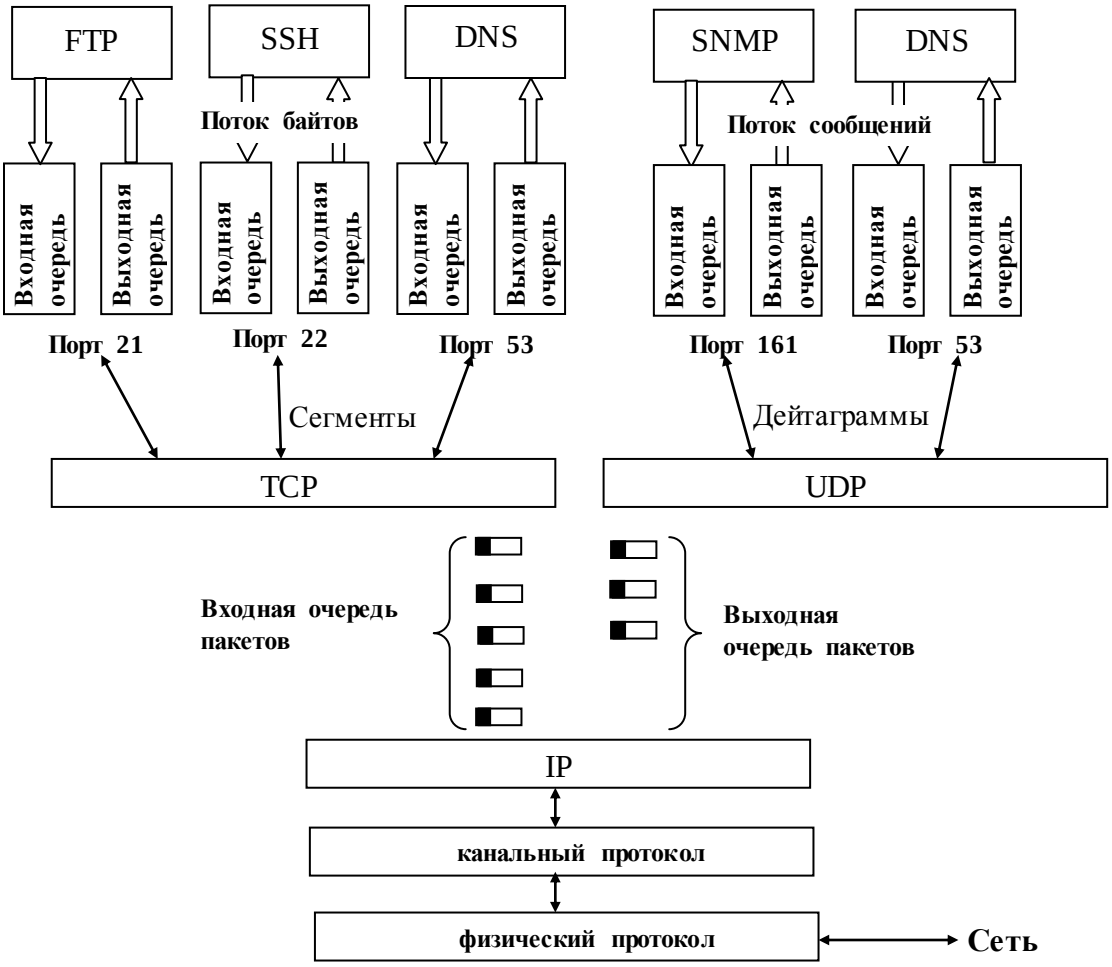


Рис. 7.4. Функции протоколов TCP и UDP

Прикладной процесс однозначно идентифицируется парой (IP – адрес, номер порта), которая называется сокет (socket). Если используется номер порта TCP, сокет называется TCP - сокетом, если используется номер порта UDP, сокет называется UDP-сокетом. В каждом сетевом взаимодействии участвует пара сокетов, а TCP– соединение идентифицируется парой сокетов взаимодействующих процессов

7.2.4 Основные принципы маршрутизации

Маршрутизатор имеет несколько портов, каждый из которых включается в другую подсеть и по логике доступа к среде каждой подсети является ее независимым узлом. Поэтому каждый порт маршрутизатора имеет свой MAC –адрес и свой сетевой адрес, а

само устройство в целом адресов не имеет (исключение составляет случай, когда маршрутизатор поддерживает удаленное управление, тогда адреса имеет его блок управления).

Функции маршрутизаторов могут выполнять как специализированные устройства, так и универсальные компьютеры с соответствующим программным обеспечением, которое обычно входит в состав современные ОС.

Задачу выбора наилучшего маршрута из нескольких возможных решают маршрутизаторы и конечные узлы. Маршрут выбирается на основании имеющейся у устройств информации о топологии сети, а также на основании указанного критерия (*метрики*) выбора маршрута. Обычно в качестве критерия выступает время прохождения маршрута отдельным пакетом или средняя пропускная способность маршрута для серии пакетов. Часто также используется весьма простая метрика, учитывающая только количество пройденных в маршруте промежуточных маршрутизаторов.

Информация о наилучших маршрутах хранится в *таблице маршрутизации*. Таблицы разных маршрутизаторов и компьютеров в зависимости от особенностей их ОС могут выглядеть по-разному, но во всех таблицах обязательно будут присутствовать следующие поля:

Сеть назначения	Сетевой адрес следующего маршрутизатора	Идентификатор собственного выходного порта	Метрика (например, расстояние до сети назначения в количестве промежуточных маршрутизаторов)

Ко всем узлам определенной сети в таблице указан общий маршрут, который задается как один шаг до следующего маршрутизатора в пути от выходного порта данного узла до сети назначения.

Для уменьшения размеров таблиц маршрутизации в больших сетях вводят *путь по умолчанию*. При этом в таблицу данного маршрутизатора включаются непосредственно подключенные к нему сети, сети, расположенные поблизости, и тупиковые ветви сети, а остальные части сети адресуются маршрутом по умолчанию. В некоторых случаях возникает необходимость задать для некоторого узла *специфический маршрут,* который отличается от маршрута для остальных узлов той же сети (например, из соображений безопасности). Для этого в таблицу помещается строка, где поле сети назначения указывается полный адрес узла (и номер сети и номер узла).

Например, записи в таблице маршрутизатора M4 на рис.7.5. говорят о том, что сеть S2 подключена непосредственно (количество промежуточных маршрутизаторов 0) к его первому порту M4(1), а сеть S5 – ко второму порту M4(2). Пути к сетям S1, S3, S4 идут через маршрутизатор M1(2), который подключен к M4(1), путь к сети S6 начинается там же, но расстояние до этой сети больше (в маршруте 2 промежуточных маршрутизатора – M2 и M6). Ко всем остальным сетям ведет маршрут по умолчанию через M5(1) и второй порт данного маршрутизатора M4(2).

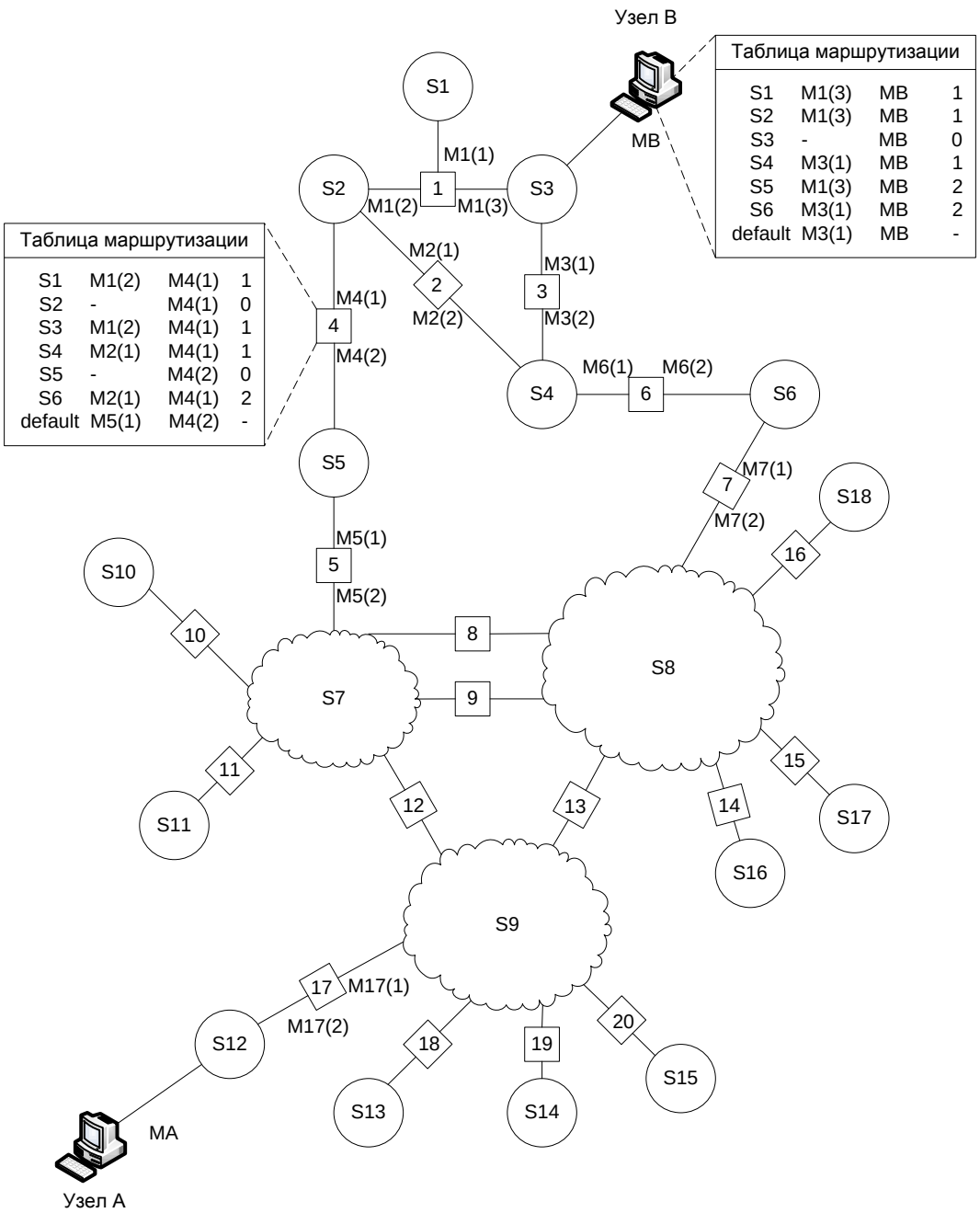


Рис. 7.5. Построение таблиц маршрутизации

Как уже отмечалось, задачу маршрутизации решают не только маршрутизаторы, но и конечные узлы-компьютеры. Протокол IP на конечном узле отправителе прежде всего определяет, находятся ли отправитель и получатель в одной сети (тогда маршрутизация не нужна) или пакет адресован компьютеру в другой сети (тогда нужна маршрутизация). Для этого сравниваются IP адреса отправителя и получателя.

Таблица маршрутизации у компьютера выглядит аналогично таблице маршрутизатора, только меньше по размерам (например, таблица маршрутизации компьютера B на рис. 7.5). Конечный узел вообще может обходиться без таблицы, так как ему достаточно знать только адрес маршрутизатора по умолчанию, из локальной сети во внешнюю обычно ведет только один маршрутизатор. Например, таблица маршрутизации узла A на рис.7.5. может выглядеть примерно следующим образом:

Сети назначения	Сетевой адрес следующего маршрутизатора	Идентификатор собственного выходного порта	Расстояние до сети назначения (число промежуточных узлов)
S12	-	MA	0
Default	M17(2)	MA	-

Из таблицы видно, что компьютер А подключен к сети S12, и может посылать пакеты либо непосредственно другим узлам этой сети, либо направлять их в другие сети через порт 2 маршрушитезатора M17 (запись по умолчанию).

Существует несколько источников, поставляющих записи в таблицу маршрутизации:

Во-первых, при инициализации маршрутизатора или компьютера программное обеспечение стека TCP/ IP заносит в таблицу записи о непосредственно подключенных сетях и маршрутизаторах по умолчанию, информация о которых появляется в стеке при ручном конфигурировании интерфейсов компьютера или маршрутизатора. Кроме того программное обеспечение автоматически вносит в таблицу записи *об особых адресах* типа 127.0.0.0 (используется для локального тестирования стека TCP/IP, пакеты, направленные в сеть с номером 127.0.0.0, не передаются протоколом IP на канальный уровень для последующей передачи в сеть, а возвращаются в источник — локальный модуль IP), адресах широковещательных и групповых рассылок.

Во-вторых, администратор может вносить статические записи в таблицу вручную. Для программных маршрутизаторов это можно сделать с помощью некоторой системной утилиты, например route, имеющейся в ОС Unix и Windows, для аппаратных маршрутизаторов – с помощью специальных команд. Статические записи не имеют срока жизни. Часто администратор вручную вносит записи о маршрутизаторе по умолчанию или о специфичных маршрутах.

В-третьих, *протоколы маршрутизации* (например, RIP, OSPF) автоматически вносят в таблицу динамические записи о имеющихся в сети маршрутах. Эти протоколы обмениваются друг с другом служебной информацией о топологии сети. Динамические записи имеют ограниченный срок жизни. Этот способ используют только маршрутизаторы.

Таким образом, при построении таблиц **маршрутизаторов** могут использоваться все три источника записей. Для **конечных узлов** таблицы маршрутизации либо создаются автоматически программным обеспечением стека TCP/IP, либо вручную – администраторами сети. Для автоматической настройки стека TCP/IP, откуда потом берется информация для таблицы маршрутизации компьютера, существует протокол DHCP.

Протокол прикладного уровня DHCP имеет клиент серверную организацию. Сервер DHCP может назначать клиентским компьютерам постоянные или динамические IP-адреса из общего адресного пула, или (для некоторых компьютеров) те адреса, которые указал администратор сети. В отличие от постоянного динамический адрес назначается компьютеру при его запуске на определенный промежуток времени – время аренды, а по истечении этого времени, если компьютер не активен, адрес снова возвращается в

пул. Помимо IP-адресов протокол DHCP может назначать клиенту и другие параметры стека TCP/IP, например, маску, IP-адрес маршрутизатора по умолчанию, IP-адрес DNS сервера, доменное имя компьютера и т.д.

Особенности таблиц маршрутизации

Некоторые реализации сетевых протоколов допускают наличие в таблицах нескольких строк, соответствующих одному адресу сети назначения, если их метрики одинаковы или разница между ними не превышает заданного значения. В многомаршрутных таблицах должно быть задано правило, по которому выбирается один из доступных альтернативных маршрутов. Чаще всего один путь является основным, а остальные – резервными. Резервные маршруты могут выбираться тогда, когда основной путь по причине технических неполадок становится недоступен.

Наличие нескольких маршрутов к одному узлу делают возможной передачу трафика к этому узлу по нескольким каналам параллельно (поочередная посылка пакетов по каждому маршруту), что повышает пропускную способность и надежность сети. Такая возможность называется балансировкой нагрузки и поддерживается рядом протоколов маршрутизации.

В таблице может содержаться несколько маршрутов по умолчанию. Как правило, в этом случае пакеты направляется по всем перечисленным маршрутам.

Если маршрутизатор поддерживает несколько классов сервиса для пакетов (по разным критериям), то для каждого класса (критерия) составляется отдельная таблица маршрутизации.

7.2.5. Поиск записей в таблицах маршрутизации

Как уже отмечалось ранее, поиск нужной строки в таблице маршратизации выполняется значительно медленнее, чем в таблице коммутации. И связано это не только с большим количеством записей в таблице, но и с самим алгоритмом, который является многопроходным.

Алгоритм просмотра таблиц без использования масок

1. Сначала выполняется первая фаза просмотра таблицы, в которой при последовательном просмотре ее строк ищется *специфический маршрут к узлу назначения*, т.е. полное совпадение IP- адреса получателя (номера сети и номера узла) с полем сети назначения. Если совпадение произошло и нужная строка найдена, из нее извлекается адрес следующего маршрутизатора и идентификатор выходного порта маршрутизатора. На этом просмотр таблицы заканчивается.

2. Если полного совпадения с IP- адресом получателя ни в одной строке не произошло, алгоритм переходит ко второй фазе – *поиску маршрута к сети назначения*. Из IP- адреса получателя выделяется номер сети, и таблица просматривается снова. Если строка, в которой номер сети совпал с искомой частью адреса, найдена, то просмотр на этом заканчивается.

3. Если строка с искомым номером сети не найдена, то выбирается строка с записью о маршруте по умолчанию. А, если такая запись отсутствует, то пакет отбрасывается.

Следует отметить, что последовательность фаз алгоритма строго определена и не зависит от последовательности записей в таблице.

Особенности алгоритма поиска с использованием масок

Рассмотрим алгоритм поиска маршрута в таблице маршрутизации, которая содержит маски подсетей. Из поступившего IP-пакета извлекается IP- адрес получателя, и IP-протокол приступает к просмотру таблицы маршрутизации.

1. Сначала, как и в случае маршрутизации без масок, в таблице ищется *специфический маршрут к узлу назначения* (полное совпадение номера сети и номера узла). Для этого из каждой записи таблицы с маской 255.255.255.255 извлекается адрес назначения и сравнивается с адресом получателя. Если совпадение произошло, то адрес следующего маршрутизатора и номер выходного порта маршрутизатора берется из этой строки.

2. Если специфический маршрут не найден, ищется *неспецифический маршрут к сети назначения* (совпадение только номера сети назначения). Из строк таблицы последовательно берутся маски и умножаются (операция конъюнкции – логическое «И») на адрес назначения, а полученный результат сравнивается с полем сети назначения в данной строке. Если происходит совпадение, IP-протокол отмечает данную строку.

3. Если просмотрены все записи таблицы, включая запись по умолчанию, маршрутизатор анализирует отмеченные строки.

Если не произошло ни одного совпадения и маршрут по умолчанию отсутствует, то пакет отбрасывается. Если произошло одно совпадение, пакет отправляется по найденному маршруту. Если было найдено несколько строк с совпадением, то маршрут выбирается из той строки, в которой количество совпавших разрядов было наибольшим, т.е. в строке с наиболее длинной маской. Это будет соответствовать *наиболее специфическому маршруту*.

В большинстве маршрутизаторов запись по умолчанию имеет в поле адреса сети назначения и в поле маски 0.0.0.0. Любой адрес, будучи умноженным на такую маску, даст 0.0.0.0. и совпадёт с полем сети назначения 0.0.0.0. А поскольку маска имеет нулевую длину, этот маршрут считается самым неспецифическим, и выбираться он будет в самую последнюю очередь, если нет других совпадений.

Пусть, например, на маршрутизатор, который имеет таблицу 7.1, поступает пакет с адресом назначения 129.44.78.200. В первую очередь этот адрес будет сравниваться со строкой 129.44.128.15.(специфический маршрут). Поскольку совпадения не происходит, строки таблицы будут просматриваться снова с целью поиска неспецифического маршрута.

Наложение маски (в данном случае одинаковой) на искомый адрес дает:

11111111.11111111.11000000.00000000 & 10000001.0101100.01001110.11001000=
10000001.0101100.01000000.00000000 =129.44.64.0

Совпадение произойдёт только в одной строке, и пакет будет отправлен на порт 129.44.64.7, к которому непосредственно подключена сеть 129.44.64.0.

Таблица 7.1. Пример таблицы маршрутизации с масками подсетей

Сети назначения	Маска	Адрес следующего маршрутизатора	Номер собственного выходного порта	Расстояние до сети назначения (число промежуточных узлов)
129.44.0.0.	255.255.192.0	129.44.0.1	129.44.0.1	Подключена
129.44.64.0.	255.255.192.0	129.44.64.7	129.44.64.7	Подключена
129.44.128.0.	255.255.192.0	129.44.128.5	129.44.128.5	Подключена
131.54.191.0	255.255.192.0	129.44.192.2	129.44.192.1	2
129.44.192.0	255.255.192.0	129.44.192.1	129.44.192.1	Подключена
0.0.0.0.	0.0.0.0	129.44.192.2	129.44.192.1	-
129.44.128.15	255.255.255.255	129.44.64.8	129.44.64.7	Подключена

7.2.6.Организация межсетевого взаимодействия

На рис.7.6. показано, как процессы, выполняющиеся на двух конечных узлах, передают свои данные через составную сеть.

Протоколы прикладного уровня стека TCP/IP работают на конечных узлах - компьютерах, выполняющих приложения пользователей. Прикладные данные передаются протоколам транспортного уровня, где делятся на сегменты и передаются на сетевой уровень для передачи с помощью маршрутизаторов через составную сеть по сетевым адресам.

Пакеты сетевого уровня упаковываются в кадры канального уровня технологии подсети, лежащей между портами соседних маршрутизаторов, и передаются в пределах этой подсети по локальным, например, MAC – адресам. Таким образом, при передаче из одной подсети в другую неизменные сетевые пакеты упаковываются в разные канальные кадры, которые, в свою очередь, используют разные протоколы физического уровня для передачи своих данных по физической среде передачи.

В пределах одной сетевой технологии (один канальный протокол) возможно использование нескольких физических протоколов, например, одни узлы подключены к коммутатору по витой паре, а другие по оптоволоконному кабелю. В общем случае физический протокол может меняться между любой парой соседних узлов.

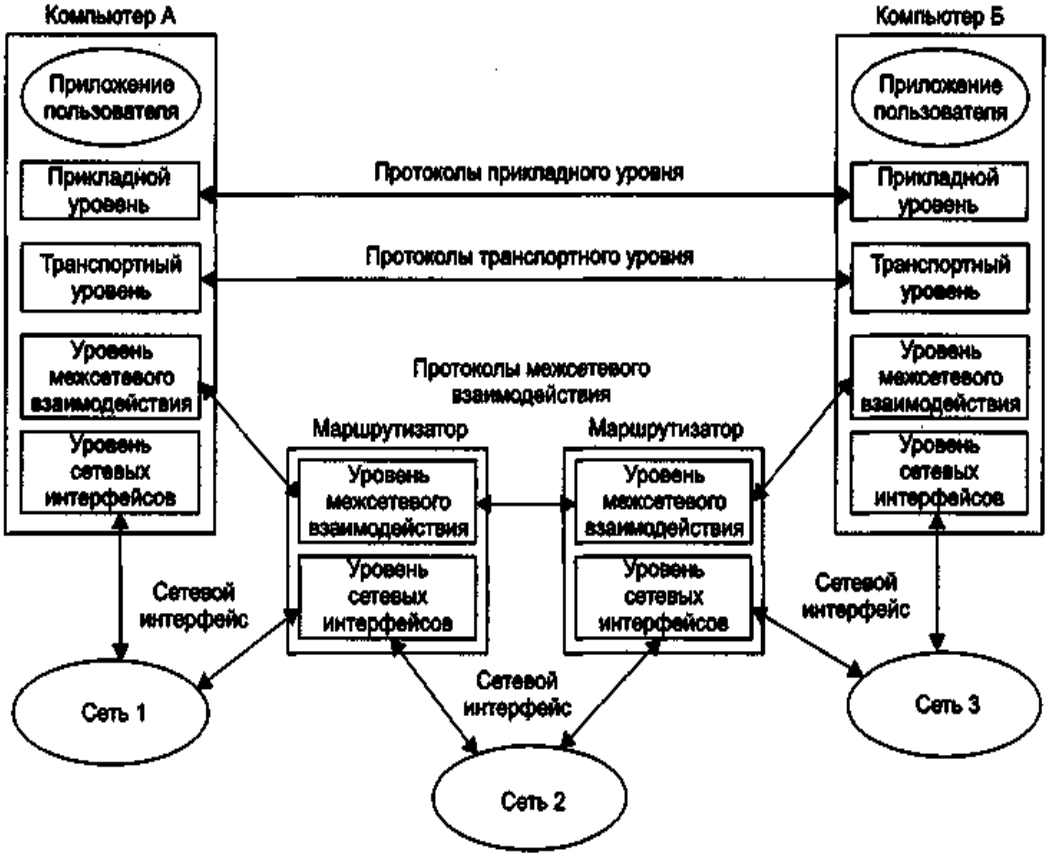


Рис. 7. 6. Передача данных через составную сеть

Протоколы TCP и UDP взаимодействуют через межуровневые интерфейсы с ниже лежащим протоколом IP и с выше лежащими протоколами прикладного уровня или приложениями, аналогично протокол IP взаимодействует через межуровневые интерфейсы с ниже лежащим протоколом канального уровня и с выше лежащими протоколами транспортного уровня TCP и UDP. По межсетевому интерфейсу помимо самого пакета может передаваться дополнительная информация. Например, вышележащие протоколы передают IP – протоколу IP – адрес получателя, а IP – протокол передаёт канальному уровню MAC – адрес следующего маршрутизатора.

7.2.7. Основные функции маршрутизатора

Рассмотрим основные этапы работы маршрутизатора более подробно. Функциональная модель маршрутизатора показана на рис. 7.7.

1. Порт маршрутизатора принимает пакет из LAN. Из кадра извлекает IP-пакет и передает программному обеспечению, реализующему IP-протокол. Проверяется контрольная сумма и время жизни пакета. По ним пакет может быть отброшен. Вносятся коррективы в служебные поля: уменьшение времени жизни пакета, пересчет контрольной суммы.

Может выполняться фильтрация трафика, как по запрещенным сетевым адресам, так и по содержимому полей сетевых и транспортных уровней. Например, в сеть могут не пропускаться пакеты определенных служб (например, telnet).

Пакеты могут образовывать очереди в портах маршрутизатора и отбрасываться при превышении объема буферов, как и в коммутаторах. Алгоритмы обслуживания очередей могут быть разными, в том числе и с учетом приоритетов.

2. Анализируется сетевой адрес назначения пакета, просматривается маршрутная таблица. Если в ней есть адрес указанной сети, то **определяется сетевой адрес следующего маршрутизатора** (точнее, его порта) в пути к сети назначения и **номер собственного порта**, через который проходит маршрут к сети назначения. Если в таблице нет номера нужной сети, используется запись о маршрутизаторе по умолчанию, а если и такой записи нет, то пакет отбрасывается.

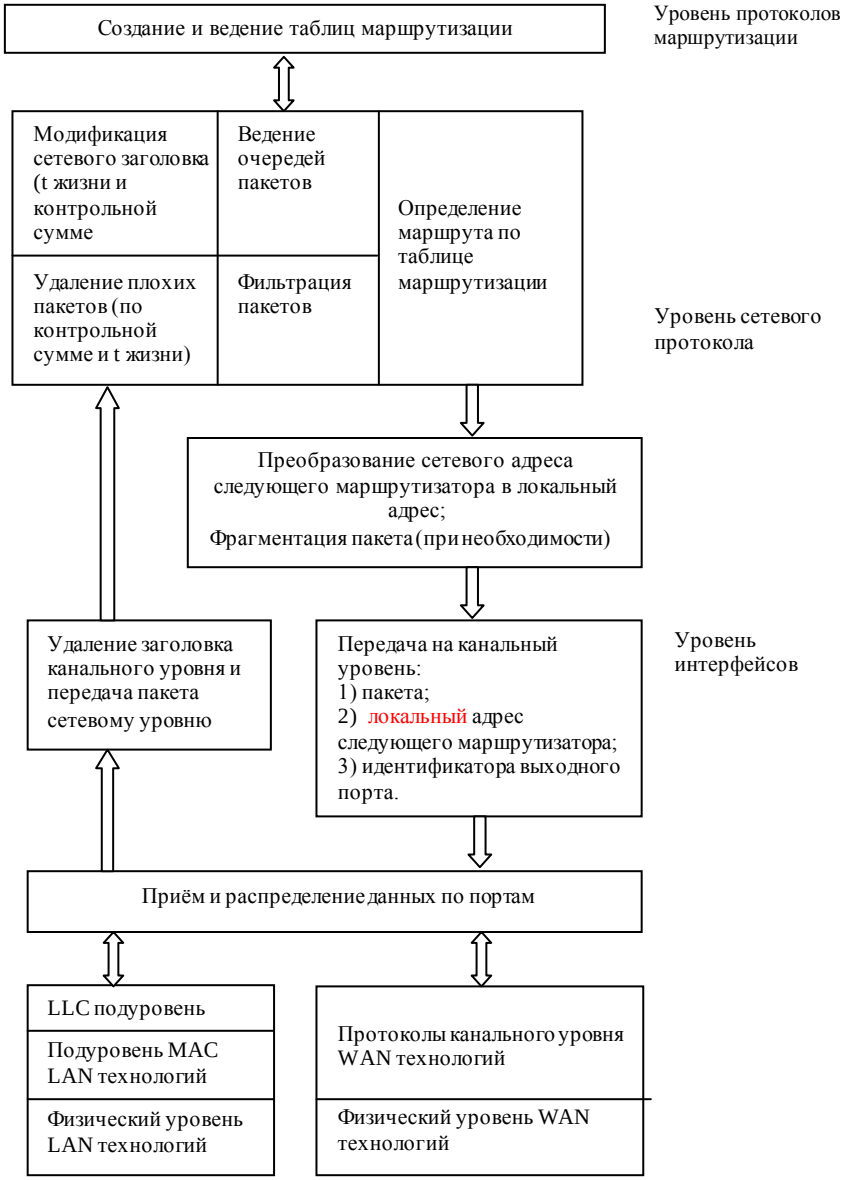


Рис.7.7. Функциональная модель маршрутизатора

3. Маршрутизатор просматривает параметры порта, в который нужно переправить пакет, и определяет технологию подключенной к нему сети. Если длины полей данных в этой технологии меньше, чем у данного пакета, IP-протокол выполняет фрагментацию пакета. Теперь необходимо определить локальный (например, MAC) адрес следующего маршрутизатора по найденному в таблице маршрутизации числовому адресу. Для этого

сетевой протокол обращается к протоколу «разрешения адресов» (например, ARP в стеке TCP/IP). Протокол разрешения просматривает свою кэш-таблицу для данного порта маршрутизатора (сетевого интерфейса). Если там нет нужного адреса, то в подключенную к порту сеть, в которой находится следующий маршрутизатор, посылается широковещательный запрос на опознавание искомого сетевого адреса. Порт следующего маршрутизатора опознает в запросе свой сетевой адрес и посылает ответ, в котором указывает свой локальный адрес.

4. Пакет, локальный адрес следующего маршрутизатора и номер порта выходного порта данного маршрутизатора посылаются на канальный уровень. Пакет переправляется в выходной порт (интерфейс), средствами которого формируется кадр канального уровня нужной технологии. В кадр включается сетевой пакет и снабжается локальным адресом следующего маршрутизатора. Теперь кадр может быть послан в следующую сеть. Перечень интерфейсов, поддерживаемых маршрутизатором – это одна из его важнейших характеристик. Интерфейс выполняет полный набор функций физического и канального уровней данной технологии.

7.2.8. Пример маршрутизации без использования масок

Рассмотрим на примере IP-сети (рис.7.8.) алгоритм работы средств сетевого уровня по продвижению пакета в составной сети. При этом будем считать, что все узлы сети, рассматриваемой в примере, имеют адреса, основанные на классах, без использования масок.

Все маршрутизаторы имеют заполненные таблицы, а на компьютерах проведены настройки стека TCP/IP. ***При настройке стека TCP/IP*** для каждого сетевого адаптера должны быть заданы IP-адрес + маска подсети и IP-адрес маршрутизатора по умолчанию, IP-адрес DNS – сервера (основного и резервного) и доменное имя задается для компьютера в целом.

1. Итак, пусть пользователь компьютера cit.dol.ru, находящегося в сети Ethernet и имеющего IP-адрес 194.87.23.17 (адрес класса C), обращается по протоколу FTP к компьютеру sf.msk.su, принадлежащему другой сети Ethernet и имеющему IP-адрес 142.06.13.14 (адрес класса B).

   Программный модуль FTP – клиента, получив команду >ftp sf.msk.su, передает запрос к работающему на этом же компьютере клиентскому модулю DNS протокола с целью определить IP-адрес узла назначения.

   При конфигурировании стека TCP/IP в компьютере cit.dol.ru был задан его собственный IP-адрес, IP-адрес маршрутизатора по умолчанию и IP-адрес DNS-сервера. Модуль DNS может сделать запрос к серверу DNS, но обычно сначала просматривается локальная таблица соответствия символьных имен и IP-адресов. Если нужного адреса в таблице не оказалось модуль DNS сделает запрос к серверу, упаковав свое сообщение в UDP– пакет, а затем в IP-пакет. В качестве адреса отправителя будет указан IP-адрес 194.87.23.17 (адрес компьютера cit.dol.ru), а получателя – 203.21.4.6 (адрес DNS- сервера). В ответ на запрос клиент FTP получит IP-адрес FTP –сервера sf.msk.su (142.06.13.14).

   Будем считать, что компьютер cit.dol.ru имеет файл hosts, а в нем есть строка 142.06.13.14 – sf.msk.su .Таким образом, разрешение имени выполняется локально.

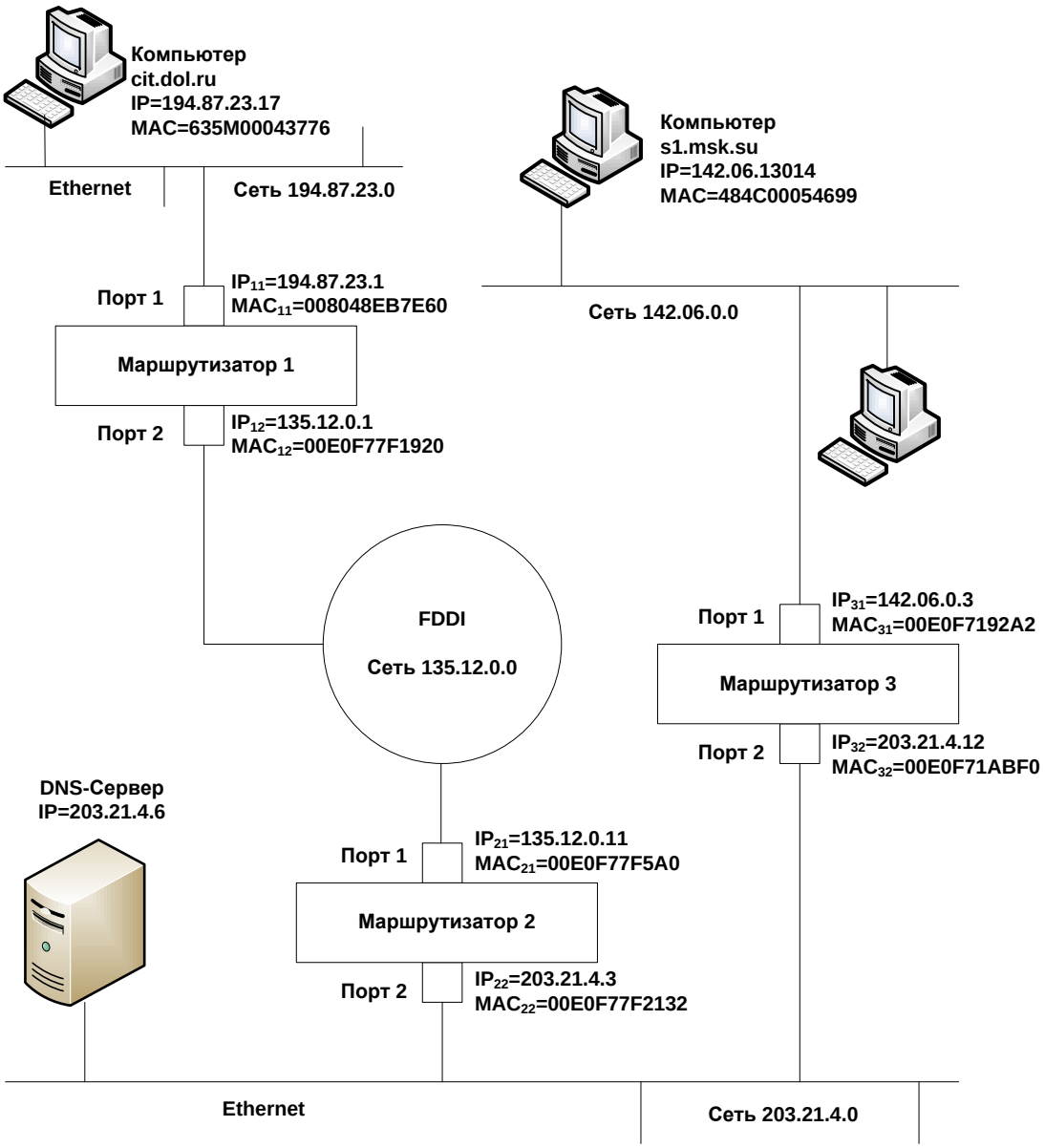


Рис.7.8. Пример взаимодействия компьютеров через сеть

2. Теперь модуль FTP передает свое сообщение и IP-адрес получателя по межуровневому интерфейсу транспортному протокола TCP, который помещает сообщение в свой сегмент и предает его протоколу IP. В заголовке IP-пакета будет указан IP-адрес узла назначения 142.06.13.14.
3. Модуль IP компьютера cit.dol.ru проверяет, нужно ли маршрутизировать пакеты с адресом 142.06.13.14. Так как адрес сети назначения (142.06.0.0) не совпадает с адресом (194.87.23.0) сети, которой принадлежит компьютер – отправитель, то маршрутизация необходима.
4. Теперь IP– пакет должен быть передан на канальный уровень для формирования кадра Ethernet, который нужно отправить по сети Ethernet маршрутизатору по умолчанию. IP– адрес маршрутизатора по умолчанию известен (194.87.23.1), но не известен его MAC– адрес. Для определения MAC-адреса маршрутизатора протокол IP обращается к протоколу ARP, который сначала просматривает ARP-таблицу. Если в последнее время компьютер cit.dol.ru выполнял какие-либо межсетевые обмены, то, скорее всего, искомая запись, содержащая соответствие между IP– и MAC–

адресами маршрутизатора по умолчанию уже находится в кэш-таблице протокола ARP. Пусть в данном случае нужная запись была найдена именно в кэш-таблице:

194.87.23.1 008048EB7E60

Обозначим найденный MAC-адрес 008048EB7E60 в соответствии с номером маршрутизатора и его порта через MAC_{M11}.

5. Протокол IP передает свой пакет и MAC-адрес получателя по межуровневому интерфейсу протоколу Ethernet, который формирует и отправляет по локальной сети кадр со следующими полями:

MAC_{M11} (получ.) 008048EB7E60	MAC_{PCcit} (отправ.) 635F00043776	IP_{PCsf} (получ.) 142.06.13.14	IP_{PCcit} (отправ.) 194.87.23.17	порт TCP (получ.) 21	порт TCP (отправ.) 1027	Поле данных TCP

Заголовок кадра Ethernet — Заголовок пакета IP — Заголовок пакета TCP

Заголовок кадра Ethernet — Заголовок кадра Ethernet — Заголовок кадра Ethernet

6. Кадр принимается портом 1 маршрутизатора 1 в соответствии с протоколом Ethernet, так как MAC– модуль этого порта распознает свой адрес MAC_{M11}. Протокол Ethernet извлекает из полученного кадра IP-пакет и передает его программному обеспечению маршрутизатора, реализующему протокол IP. Протокол IP извлекает из пакета адрес назначения 142.06.13.14 и просматривает записи своей таблицы маршрутизации. Пусть маршрутизатор 1 имеет в своей таблице маршрутизации запись:

142.06.0.0 135.12.0.11 2,

которая говорит о том, что пакеты для сети 142.06.0.0 нужно передавать следующему маршрутизатору 135.12.0.11, который находящемуся в сети, подключенной к порту 2 маршрутизатора 1.

7. Маршрутизатор 1 просматривает параметры порта 2 и находит, что к нему подключена сеть FDDI. Так как сеть FDDI имеет значение MTU большее, чем сеть Ethernet, то фрагментация IP-пакета не требуется. Поэтому маршрутизатор 1 формирует кадр формата FDDI. На этом этапе модуль IP должен определить MAC–адрес следующего маршрутизатора по известному IP-адресу 135. 12. 0. 11. Для этого он обращается к протоколу ARP. Допустим, что нужной записи в кэш-таблице не оказалось, тогда в сеть FDDI отправляется широковещательный ARP-запрос, содержащий наряду с прочей следующую информацию:

MAC (получ.) FFFFFFFFFFFF	MAC_{M12} (отправ.) 00E0F77F1920		00000000000000 Искомый MAC-адрес	135.12.0.11 Известный IP- адрес

Заголовок кадра FDDI — ARP - запрос

Заголовок кадра Ethernet — Заголовок кадра Ethernet

Порт 1 маршрутизатора 2 распознает свой IP-адрес и посылает ARP-ответ по адресу запросившего узла:

MAC_{M12} (получ.) 00E0F77F1920	MAC_{M21} (отправ.) 00E0F77F51A0		00E0F77F51A0 Найденный MAC-адрес	135.12.0.11 Известный IP- адрес

Заголовок кадра FDDI — ARP - ответ

Заголовок кадра Ethernet — Заголовок кадра Ethernet

Теперь, зная MAC– адрес следующего маршрутизатора 00E0F77F51A0, маршрутизатор 1 отсылает кадр FDDI по направлению к маршрутизатору 2. Заметим, что в полях IP-пакета никаких изменений не произошло.

MAC_{M21} (получ.) 00E0F77F51A0	MAC_{M12} (отправ.) 00E0F77F1920	IP_{PCsf} (получ.) 142.06.13.14	IP_{PCcit} (отправ.) 194.87.23.17	Поле данных пакета IP

Заголовок кадра FDDI

Заголовок пакета IP

Заголовок кадра Ethernet

Заголовок кадра Ethernet

8. Аналогично действует модуль IP на маршрутизаторе 2. Получив кадр FDDI, он отбрасывает его заголовок, а из заголовка IP извлекает IP-адрес сети назначения и просматривает свою таблицу маршрутизации. Там он может найти запись о сети назначения:

   142.06.0.0 203.21.4.12 2

   или при отсутствии такой записи использует запись о маршрутизаторе по умолчанию:

   default 203.21.4.12 2.

   Определив IP-адрес следующего маршрутизатора 203.21.4.12, модуль IP с помощью протокола ARP находит MAC-адрес этого маршрутизатора и пересылает пакет на порт 2, где формируется кадр Ethernet. Кадр с неизменным IP– пакетом пересылается по сети Ethernet маршрутизатору 3.

MAC_{M32}(получ.) 00E0F71AB7F0	MAC_{M22}отправ.) 00E0F77F2132	IP_{PCsf} (получ.) 142.06.13.14	IP_{PCcit} (отправ.) 194.87.23.17	Поле данных пакета IP

Заголовок кадра Ethernet

Заголовок пакета IP

Заголовок кадра Ethernet

Заголовок кадра Ethernet

9. Наконец, после того как пакет поступил в маршрутизатор 3, к которому подключена сеть назначения, появляется возможность передачи этого пакета целевому компьютеру. Маршрутизатор 3 определяет, что пакет нужно передать в сеть 142.06.0.0, которая непосредственно подключена к его первому порту. Поэтому он посылает ARP-запрос по сети Ethernet с IP-адресом компьютера sf.msk.su. ARP-ответ содержит MAC– адрес конечного узла, который модуль IP передает канальному протоколу для формирования кадра Ethernet:

MAC_{PCsf} (получ.) 484C00054699	MAC_{M31} (отправ.) 00E0F7192A2	IP_{PCsf} (получ.) 142.06.13.14	IP_{PCcit} (отправ.) 194.87.23.17	Поле данных пакета IP

Заголовок кадра Ethernet

Заголовок пакета IP

Заголовок кадра Ethernet

Заголовок кадра Ethernet

10. Сетевой адаптер компьютера sf.msk.su захватывает кадр Ethernet, обнаруживает совпадение MAC-адреса, содержащегося в заголовке, со своим собственным адресом и направляет пакет модулю IP. После анализа полей IP-заголовка из пакета извлекаются данные, которые содержат сообщение вышележащего протокола. Поскольку в данном примере рассматривается обмен данными по протоколу FTP, который использует в качестве транспортного протокола TCP, то в поле данных IP-

пакета находится TCP-сегмент. Определив из TCP-заголовка номер порта получателя 21, модуль IP переправляет сегмент в соответствующую очередь, из которой данный сегмент попадет программному модулю FTP-сервера.

7.3. Протоколы маршрутизации

Основная работа по составлению таблиц маршрутизации выполняется автоматически с помощью протоколов маршрутизации, которые обмениваются пакетами с информацией о топологии составной сети. Предусматривается также и ручная корректировка таблиц. При обмене маршрутной информацией пакеты протокола маршрутизации помещаются в поле данных пакетов сетевого уровня, или даже транспортного, поэтому формально их следовало бы относить к более высокому уровню, чем сетевой.

Протоколы маршрутизации могут быть построены на основе разных алгоритмов, отличающихся способами построения таблиц маршрутизации, выбора наилучшего маршрута и другими особенностями.

Эти протоколы делятся на следующие группы:

1. С **одношаговыми алгоритмами** маршрутизации. В них маршрутизация выполняется по распределенной схеме. Каждый маршрутизатор выбирает один шаг маршрута, а конечный маршрут складывается в результате работы всех маршрутизаторов, через которые проходит пакет.
2. С **маршрутизацией от источника** (Sonra Routing). Это многошаговый подход. Узел-источник задает в отправляемом пакете полный маршрут, через все промежуточные узлы. При таком подходе не нужны таблицы маршрутизации для промежуточных узлов, их работа ускоряется, но возрастает нагрузка на конечные узлы. Этот способ трудно применять в больших сетях. Возможна угроза безопасности в публичных сетях (если в перехваченном пакете запроса внести коррективы в маршрут, то ответ пойдёт через подставной маршрутизатор злоумышленника).

Одношаговые алгоритмы в зависимости от способа формирования таблиц делятся на три класса:

1. Алгоритмы фиксированной (статической) маршрутизации.
2. Алгоритмы простой маршрутизации.
3. Алгоритмы адаптивной (или динамической) маршрутизации.

В алгоритмах *фиксированной маршрутизации* все записи – статические и делаются вручную администратором сети. Алгоритм подходит для небольших сетей с простой топологией, а также для магистралей крупных сетей, которые имеют простую структуру.

В алгоритмах *простой маршрутизации* таблица маршрутизации либо не используется совсем, либо строится без участия протоколов маршрутизации. Выделяют три типа простой маршрутизации:

1. *Случайная маршрутизация*, когда прибывший пакет посылается в первом попавшемся случайном направлении, кроме исходного направления (аналогично обработке кадров с неизвестным адресом);

2. *Лавинная маршрутизация,* когда пакет широковещательно посылается по всем возможным направлениям, кроме исходного направления (аналогично обработке мостами кадров с неизвестным адресом);

3. *Маршрутизация по предыдущему опыту,* когда выбор маршрута осуществляется по таблице, но таблица строится по принципу моста, путем анализа адресных полей пакетов, появляющихся на входных портах.

Все описанные алгоритмы не подходят для больших сетей.

Самыми распространенными являются алгоритмы *адаптивной* (или *динамической*) *маршрутизации*. Эти алгоритмы обеспечивают автоматическое обновление таблиц маршрутизации после изменения конфигурации сети. В таблицах маршрутизации при использовании таких алгоритмов обычно определяется время жизни маршрута.

Адаптивные алгоритмы обычно носят распределенный характер, хотя в последнее время наметилась тенденция использовать так называемые серверы маршрутов. Сервер маршрутов – это один выделенный маршрутизатор, который собирает информацию о топологии сети от других маршрутизаторов. На основании этих данных выделенный маршрутизатор строит таблицы маршрутизации для всех остальных маршрутизаторов сети, а затем распространяет их по сети, чтобы каждый маршрутизатор получил собственную таблицу и в дальнейшем самостоятельно принимал решение о продвижении пакетов.

Адаптивные протоколы в свою очередь делятся на:

1. Дистанционно-векторные алгоритмы (Distance Vector Algorithms – DVA)
2. Алгоритмы состояния связей (Link State Algorithms – LSA)

При конфигурации каждого маршрутизатора его портам назначаются IP-адреса, а номера IP-сетей, подключенных к этим портам, вносятся в начальную таблицу маршрутизации.

В *дистанционно-векторных* алгоритмах каждый маршрутизатор периодически (через определенные промежутки времени) широковещательно рассылает по сети вектор (экземпляр своей таблицы), компонентами которого являются расстояния от данного маршрутизатора до всех известных ему сетей. Под расстоянием обычно понимается число промежуточных маршрутизаторов, которые необходимо пройти (хопов). Возможна и другая метрика – учет не только числа промежуточных маршрутизаторов, но и времени прохождения пакетов по сети между соседними маршрутизаторами. При получении вектора от соседа маршрутизатор прибавляет к расстояниям до указанных в векторе сетей расстояние от него самого до данного соседа. Если в его таблице еще нет маршрутов до указанных в векторе сетей, маршрутизатор добавляет новые записи в свою таблицу. Если маршруты до каких – то сетей уже есть в таблице данного маршрутизатора, он сравнивает показатели метрики старого и нового маршрута, и либо заменяет старую запись на новую (показатель нового маршрута лучше), либо игнорирует новый маршрут и оставляет старую запись. После этого маршрутизатор формирует новый вектор, в котором указывает информацию об известных ему сетях, о которых он узнал непосредственно (если они подключены к его портам) или из объявлений других маршрутизаторов, и рассылает новый вектор по сети. В конце концов, каждый маршрутизатор получает информацию обо всех входящих в интерсеть сетях и о расстоянии до них через соседние маршрутизаторы.

Дистанционно-векторные алгоритмы просты и хорошо работают в небольших сетях. В больших сетях они засоряют линии связи интенсивным широковещательным трафиком. К тому же изменения топологии сети обрабатываются этим алгоритмом относительно долго и не всегда корректно, так как маршрутизаторы не имеют точного представления о топологии сети, аналогично мостам (но в современных алгоритмах есть приёмы борьбы с потенциальными некорректностями).

Наиболее распространенный протокол описанного типа – RIP, существующий в версиях для протоколов IP и IPX.

Алгоритмы *состояния связей* обеспечивают каждый маршрутизатор информацией, достаточной для построения точного топологического графа сети. Вершинами графа являются как маршрутизаторы, так и объединяемые ими сети. Распространяемая по сети информация состоит из описания *связей* между вершинами графа – маршрутизатор – маршрутизатор или маршрутизатор – сеть. Связи имеют метрики. Чаще всего это пропускная способность, но возможны метрики задержки или надёжности передачи пакетов. В отличие от дистанционно – векторных алгоритмов информация, полученная от других маршрутизаторов, при последующем распространении не модифицируется. В результате чего, все маршрутизаторы сети располагают идентичными топологическими базами данных. Каждый маршрутизатор вычисляет по графу наилучшие маршруты до всех сетей, но вносит в свою таблицу записи только об одном шаге этих маршрутов (до следующего маршрутизатора).

«Широковещательная» рассылка (то есть передача пакетов всем непосредственным соседям маршрутизатора) используется здесь только в начальной фазе обмена топологической информацией и при изменениях состояния связей, что в надежных сетях происходит довольно редко.

Чтобы понять, в каком состоянии находятся линии связи, подключенные к его портам, маршрутизатор периодически обменивается короткими пакетами HELLO со своими ближайшими соседями. Этот служебный трафик также засоряет сеть, но не в такой степени, как, например, пакеты протокола RIP, так как пакеты HELLO имеют намного меньший объем. Записи в топологических базах маршрутизаторов имеют срок жизни. Если запись о некоторой связи устаревает, то маршрутизатор может запросить её новую копию. Ответ на запрос должен прислать маршрутизатор, который непосредственно тестирует эту связь.

Все маршруты работают на основании одинаковых графов, поэтому изменения в конфигурации сети отрабатываются алгоритмом быстро и корректно (маршрутизатор вносит изменения в граф сети, вычисляет новые оптимальные маршруты к некоторым сетям и модифицирует часть записей в своей таблице).

Недостатком алгоритма является его сложность, требующая большой вычислительной мощности маршрутизатора.

В качестве примера протоколов, использующих алгоритм состояния связей, можно привести OSPF (Open Shortest Path First) из стека TCP/IP и IS-IS (Intermediate System to Intermediate System) из стека OSI.

7.4. Внешние и внутренние протоколы маршрутизации. Общая организация сети Internet

Интернет обладает не только организационной структурой, определяющей деление Интернета на сети различных поставщиков услуг (ISP). Интернет состоит также из автономных систем (AS).

Автономная система (AS) — это совокупность IP-сетей под единым административным управлением, обеспечивающим общую для всех входящих в автономную систему маршрутизаторов политику маршрутизации. Обычно автономной системой управляет один поставщик услуг Интернета, самостоятельно выбирая, какие протоколы маршрутизации должны использоваться в некоторой автономной системе и каким образом между ними должно выполняться перераспределение маршрутной информации. Крупные поставщики услуг и корпорации могут представить свою составную сеть как набор нескольких автономных систем. Регистрация автономных систем происходит централизованно, как и регистрация IP-адресов и DNS-имен. Номер автономной системы состоит из 16 разрядов и никак не связан с префиксами IP-адресов сетей, входящих в нее. Он выделяется организацией, учредившей новую автономную систему, InterNIC.

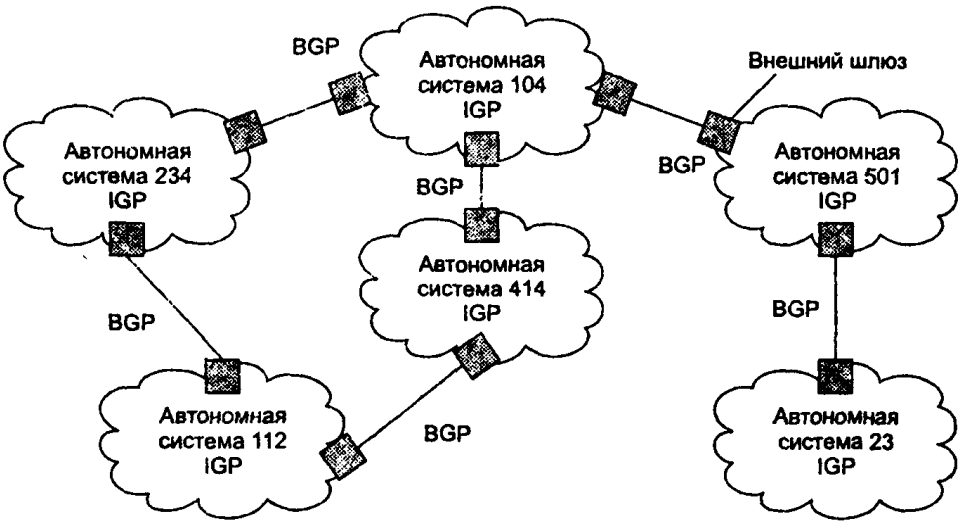


Рис. 7.9. Автономные системы Интернет

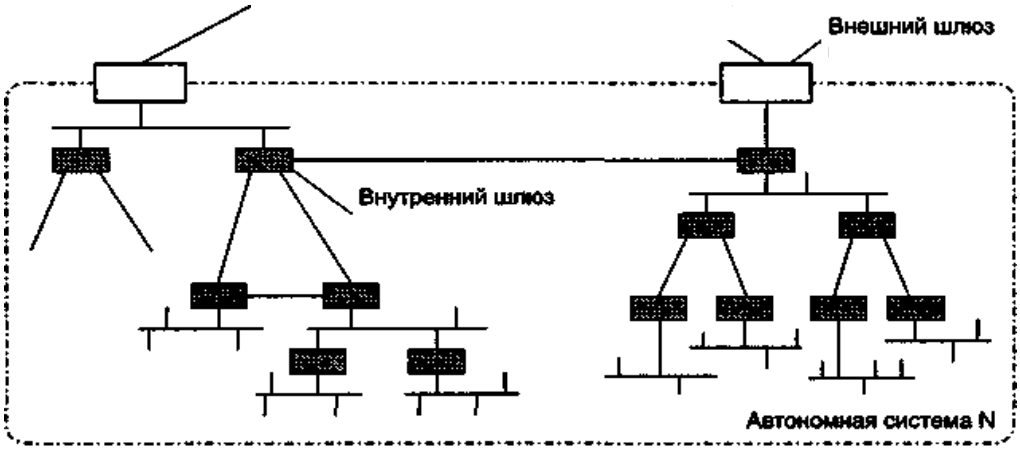


Рис. 7.10. Организация автономной системы

В соответствии с этой концепцией **Интернет выглядит как множество взаимосвязанных автономных систем** (рис. 7.9), **каждая из которых состоит из взаимосвязанных IP – сетей** (рис. 7.10). **Сети и AS соединены между собой маршрутизаторами.**

Основная цель деления Интернета на автономные системы — обеспечение многоуровневого подхода к маршрутизации. До введения автономных систем предполагался двухуровневый подход — то есть сначала *маршрут определялся как последовательность IP– сетей,* а затем вёл непосредственно к заданному узлу в конечной IP – сети.

С появлением автономных систем появляется третий, верхний, уровень маршрутизации — теперь сначала *маршрут определяется как последовательность автономных систем,* затем — *как последовательность IP– сетей,* а уже затем ведет к конечному узлу.

В Интернет сохранилась старая терминология, в соответствии с которой маршрутизаторы называются **шлюзами**.

Автономные системы соединяются внешними шлюзами (маршрутизаторами). Между внешними маршрутизаторами AS разрешается использовать только один протокол маршрутизации, определяющий обмен маршрутной информацией между ними. Этот протокол не может быть произвольным. Он должен быть признан в данное время сообществом Интернета в качестве стандартного для внешних шлюзов. Такой протокол маршрутизации называется **внешним шлюзовым протоколом** (Exterior Gateway Protocol, EGP) и в настоящее время им является протокол BGP версии 4 (BGPv4). Все остальные протоколы (например, RIP, OSPF, IS-IS) являются **внутренними шлюзовыми протоколами** (Interior Gateway Protocols, IGP). Внутри автономной системы может использоваться любой внутренний протокол. Например, в одной OSPF, в другой RIP и т.д.

Внешний шлюзовой протокол отвечает за выбор *маршрута между автономными системами.* В качестве адреса следующего маршрутизатора указывается адрес точки входа в соседнюю автономную систему.

Внутренние шлюзовые протоколы отвечают за *маршрут внутри автономной системы* (через внутренние маршрутизаторы). В случае транзитной автономной системы эти протоколы указывают точную последовательность маршрутизаторов от точки входа в автономную систему до точки выхода из нее.

Автономные системы составляют магистраль Интернета. Концепция автономных систем скрывает от администраторов магистрали Интернета проблемы маршрутизации пакетов на более низком уровне — уровне сетей. Для администратора магистрали неважно, какие протоколы маршрутизации применяются внутри автономных систем и, как они изменяются, для него существует единственный протокол маршрутизации - **BGPv4.**

Кроме того, деление Internet на автономные системы способствует агрегированию (объединению) информации во внешних шлюзах. Внутренние шлюзы могут использовать для внутренней маршрутизации достаточно подробные графы связей между собой, чтобы выбрать наиболее рациональный маршрут. Однако, если такая детальная информация обо всех сетях автономных систем будет храниться во внешних маршрутизаторах, то их топологические базы данных так разрастутся, что потребуют наличия памяти гигантских размеров, а время принятия решений о маршрутизации станет неприемлемо большим. Поэтому детальная топологическая информация

остается внутри автономной системы, а автономную систему как единое целое для остальной части Internet представляют внешние шлюзы. Внешние шлюзы сообщают о внутреннем составе автономной системы минимально необходимые сведения — количество IP-сетей, их адреса и внутреннее расстояние до этих сетей от данного внешнего шлюза.

Техника бесклассовой маршрутизации CIDR может значительно сократить объёмы маршрутной информации, передаваемой между автономными системами. Так, если все сети внутри некоторой автономной системы начинаются с общего префикса, например, 194.27.0.0/16, то внешний шлюз этой автономной системы должен делать объявления только об этом адресе, и не сообщать отдельно о существовании внутри данной автономной системы, например, о сети 194.27.32.0/19 или 194.27.40.0/21, так как эти адреса агрегируются в адрес 194. 27. 0. 0/16.

7.5. Маршрутизаторы

7.5.1. Функции и технические характеристики маршрутизаторов

В разделе 7.2.7 были рассмотрены **основные функции** маршрутизаторов, которые состоят в составлении таблицы маршрутизации и организации передачи данных на основе этой таблицы через сложную составную сеть, состоящую из подсетей, построенных по разным локальным и глобальным технологиям.

Основными характеристиками маршрутизаторов являются: тип конструктива, общая производительность в пакетах в секунду, набор поддерживаемых сетевых протоколов и протоколов маршрутизации, количество портов и поддерживаемые на них интерфейсы глобальных и локальных сетей.

К числу **дополнительных функций** маршрутизаторов относятся одновременная поддержка сразу нескольких сетевых протоколов и нескольких протоколов маршрутизации, возможность приоритетной обработки трафика, разделение функций построения таблиц маршрутизации и продвижения пакетов между маршрутизаторами разного класса на основании готовых таблиц маршрутизации. Это примеры тех функции, которые расширяют возможности основных функций, связанных с маршрутизацией трафика. Однако, современные аппаратные IP– маршрутизаторы снабжаются целым рядом дополнительных функций, которые превращают его в многофункциональное устройство по обработке трафика. Это автоматическая настройка стека TCP/IP на компьютерах сети по протоколу DHCP, средства защиты сети от внешних атак – межсетевые экраны и анализаторы вторжений, технологии трансляции сетевых адресов NAT, поддержка защищенных внешних соединений VPN, организация группового вещания по протоколу IGMP и многое другое.

С технической точки зрения типичный аппаратный маршрутизатор представляет собой сложный специализированный компьютер, работающий под управлением специализированной операционной системы, оптимизированной для выполнения операций построения таблиц маршрутизации и перемещения пакетов на основе этих таблиц. Многие такие системы в свое время разрабатывались на основе UNIX.

Маршрутизатор часто строится по многопроцессорной схеме, причем используется симметричная многопроцессорность. Наиболее рутинные операции обработки пакетов выполняются программно и аппаратно специализированными процессорами или чисто

аппаратно большими интегральными схемами (БИС/ASIC). Более высокоуровневые действия выполняют программно универсальные процессоры.

По конструктивному исполнению наиболее часто встречаются маршрутизаторы с фиксированным количеством портов и модульные.

По областям применения маршрутизаторы делятся на: магистральные маршрутизаторы, маршрутизаторы региональных подразделений, маршрутизаторы удаленных офисов и маршрутизаторы локальных сетей / коммутаторы третьего уровня.

Магистральные маршрутизаторы – это наиболее мощные устройства, способные обрабатывать сотни тысяч или миллионы пакетов в секунду, оснащенные большим количеством интерфейсов локальных и глобальных сетей. Чаще всего магистральный маршрутизатор конструктивно выполняется по модульной схеме на основе шасси с большим количеством слотов – до 12-14. Большое внимание в магистральных маршрутизаторах уделяется надежности и отказоустойчивости, которая достигается за счет системы терморегуляции, избыточных источников питания, модулей «горячей замены» (hot-swap) и симметричной многопроцессорности.

Маршрутизаторы региональных отделений – это обычно несколько упрощенные версии магистральных маршрутизаторов. Количество слотов в его шасси – обычно до 4-5. Возможны и решения с фиксированным количеством портов. Поддерживаемые интерфейсы локальных и глобальных сетей – менее скоростные.

Маршрутизаторы удаленных офисов соединяют, как правило, единственную локальную сеть удаленного офиса с центральной сетью или региональным отделением по глобальной связи, поэтому имеют небольшое фиксированное количество портов. Маршрутизатор удаленного офиса в качестве резервной связи для выделенного канала может поддерживать работу по телефонной линии. Существует очень много типов маршрутизаторов удаленных офисов. Их производительность обычно составляет от 5 до 20-30 тысяч пакетов в секунду.

Маршрутизаторы локальных сетей предназначены для разделения крупных локальных сетей на подсети с целью улучшения управляемости, разграничения прав доступа и сокращения широковещательного трафика, который в крупных коммутируемых сетях может заметно снизить полезную пропускную способность сети. Основное требование, предъявляемое к этим устройствам – высокая скорость маршрутизации, так как в такой сети все порты – скоростные, обычно 100 Мб/с. Однако, сегодня основным решением перечисленных задач внутри локальной сети является использование не маршрутизатора, а *коммутатора третьего уровня*.

7.5.2. Коммутаторы третьего уровня

Объем внешнего трафика в ЛВС постоянно растет. В недалеком прошлом наметился разрыв между производительностью типичного коммутатора в ЛВС и маршрутизатора, объединяющего подсети ЛВС.

Решение данной проблемы шло по двум направлениям:

1. увеличение производительности маршрутизаторов;
2. отказ от маршрутизации там, где это возможно.

В коммутаторах третьего уровня получили отражение оба направления. Это комбинированные устройства, совмещающие в себе функции коммутаторов и маршрутизаторов.

Характерная особенность устройств данного типа – использование специализированных заказных БИС, многопроцессорность, распараллеливание с помощью специальных процессоров портов, как у коммутаторов. Максимальная скорость достигается, когда вместо универсальных или специализированных процессоров используются специализированные БИС, то есть используется не программная, а аппаратная реализация основных протоколов (например, IP, Ethernet).

Функции коммутации и маршрутизации совмещаются следующим образом. Коммутаторы третьего уровня поддерживают технику виртуальных локальных сетей (VLAN). Каждому VLAN обычно присваивается номер IP– подсети. Маршрутизация на основе IP– адресов выполняется по каждому пакету, требующему передачи из одной подсети в другую, а коммутация на основе MAC– адресов выполняется для пакетов, принадлежащих одной подсети. Выбор режима передачи пакета определяется конфигурированием IP– адресов портов коммутатора и подключенных к портам компьютеров.

Нескольким портам коммутатора 3-го уровня и компьютерам, подключенным к этим портам, присваиваются IP– адреса, принадлежащие одной подсети. Они образуют один VLAN. Аналогично, другие порты коммутатора вместе с подключенными к ним компьютерами образуют VLAN другой IP– подсети. Для всех компьютеров, которые подключены к одному порту коммутатора (возможно через обычные коммутаторы или концентраторы), в качестве адреса маршрутизатора по умолчанию указывается IP– адрес этого порта. Когда компьютер посылает пакет адресату из своей IP– подсети, то в качестве MAC-адреса получателя будет указан адрес компьютера адресата, а если адресат находится в другой IP– подсети, то в качестве MAC-адреса получателя будет указан адрес маршрутизатора по умолчанию (т.е. порта коммутатора 3-го уровня, к которому подключен компьютер– отправитель).

Действия коммутатора 3-го уровня: если кадр данных имеет MAC-адрес получателя, отличный от MAC-адреса порта коммутатора, то кадр коммутируется, а если кадр направлен непосредственно порту коммутатора, то – маршрутизируется.

В процессе коммутации кадр по таблице коммутации данного VLAN сразу отправляется на нужный порт. В процессе маршрутизации сначала отправляется ARP– запрос на все порты другого VLAN, где находится получатель или следующий маршрутизатор, с целью определения его MAC-адреса, а затем исходный IP– пакет упаковывается в новый кадр канального уровня и отправляется на уровень коммутации этого VLAN. Вместо номера выходного порта в таблице маршрутизации указывается номер соответствующего VLAN, т.к. порты виртуального маршрутизатора объединяют VLAN-ы между собой (см. рис.6.14).

При необходимости коммутатор 3-го уровня может быть сконфигурирован как обычный коммутатор или обычный маршрутизатор.

7.5.3. Сети предприятий

Сети предприятий обычно создаются на основе маршрутизаторов и связей с глобальной сетью. Ее основной частью, как правило, является оборудование,

предназначенное для объединения большого числа пользователей в центральной точке. Это могут быть большие коммутаторы 3-го уровня или маршрутизаторы на шасси.

Существуют также корпоративные многофункциональные концентраторы, представляющие собой устройства, в которых на общей внутренней шине объединяются модули разного типа — концентраторы, мосты, коммутаторы и маршрутизаторы. Такое объединение дает возможность программного конфигурирования сети с определением состава подсетей и сегментов вне зависимости от физического подключения к тому или иному порту устройства.

На уровне сети предприятия (рис. 7.11.) особое значение приобретает маршрутизация по следующим причинам:

1. Защита крупной сети от широковещательных штормов (>20% общего трафика) и ошибочных кадров.

2. Развитые возможности защиты от несанкционированного доступа.

3. Связь отдельных сегментов и подсетей через глобальные связи.

4. Связь с сетью Internet.

5. Неразделенная маршрутизаторами сеть имеет ограничение на число компьютеров. Например, IP сеть класса C (самый доступный) допускает 255 узлов.

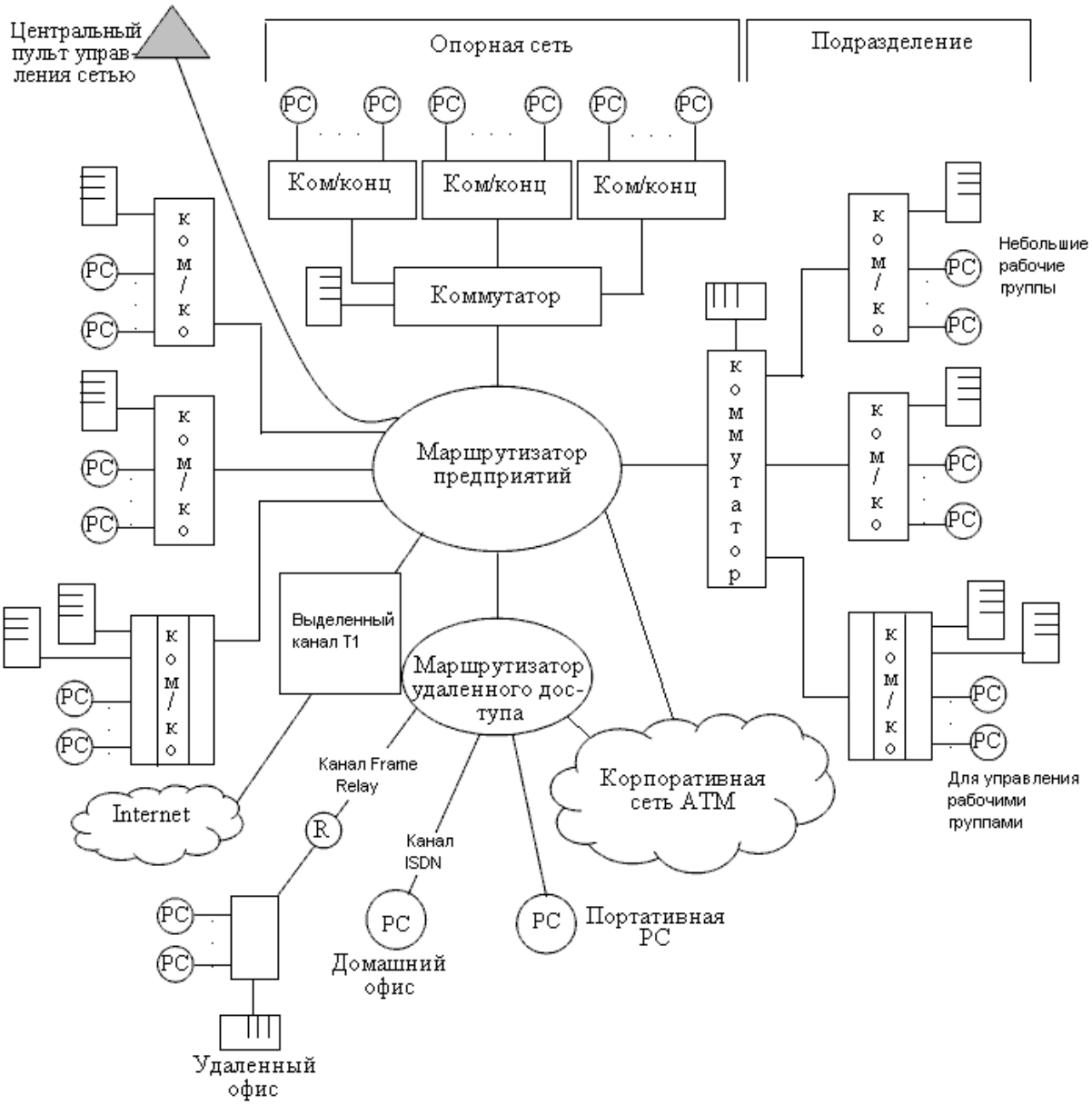


Рис. 7.11. Пример сети предприятия

Краткая информация по главе 7

- Составная сеть (internetwork или internet) — это совокупность нескольких сетей, называемых также подсетями (subnet), которые соединяются между собой маршрутизаторами. Организация совместной транспортной службы в составной сети называется межсетевым взаимодействием (internetworking).
- В функции сетевого уровня входит: передача пакетов между конечными узлами в составных сетях, выбор маршрута, согласование локальных технологий отдельных подсетей.
- Маршрут — это последовательность маршрутизаторов, которые должен пройти пакет от отправителя до пункта назначения. Задачу выбора маршрута из нескольких возможных решают маршрутизаторы и конечные узлы на основе таблиц маршрутизации.

- Существует несколько источников, поставляющих записи в таблицу маршрутизации. Во-первых, при инициализации программное обеспечение стека TCP/ IP заносит в таблицу записи о непосредственно подключенных сетях и маршрутизаторах по умолчанию, а также записи об особых адресах типа 127.0.0.0. Во-вторых, администратор вручную заносит статические записи о специфичных маршрутах или о маршрутизаторе по умолчанию. В-третьих, протоколы маршрутизации автоматически заносят в таблицу динамические записи о имеющихся маршрутах.

- Протоколы маршрутизации (например, RIP или OSPF) следует отличать от собственно сетевых протоколов (например, IP или IPX). В то время как первые собирают и передают по сети чисто служебную информацию о возможных маршрутах, вторые предназначены для передачи пользовательских данных.

- Сетевые протоколы и протоколы маршрутизации реализуются в виде программных модулей на конечных узлах-компьютерах и на промежуточных узлах-маршрутизаторах.
- Маршрутизатор представляет собой сложное многофункциональное устройство, в задачи которого входит: построение таблицы маршрутизации, определение на ее основе маршрута, буферизация, фрагментация и фильтрация поступающих пакетов, поддержка сетевых интерфейсов. Функции маршрутизаторов могут выполнять как специализированные устройства, так и универсальные компьютеры.

- Для алгоритмов маршрутизации характерны одношаговый и многошаговый подходы. Одношаговые алгоритмы делятся на алгоритмы фиксированной, простой и адаптивной маршрутизации. Адаптивные протоколы маршрутизации являются наиболее распространенными и в свою очередь могут быть основаны на дистанционно-векторных алгоритмах и алгоритмах состояния связей.

- Стандартом де-факто для построения составных сетей в последнее время стал стек TCP/IP. Стек TCP/IP имеет 4 уровня: прикладной, основной, уровень межсетевого взаимодействия и уровень сетевых интерфейсов. Соответствие уровней стека TCP/IP уровням модели OSI достаточно условно.

- *Прикладной уровень* объединяет все службы, предоставляемые системой пользовательским приложениям: традиционные сетевые службы типа telnet, FTP, TFTP, DNS, SNMP, а также сравнительно новые, такие, например, как протокол передачи гипертекстовой информации HTTP.
- *На основном уровне* стека TCP/IP, называемом также транспортным, функционируют протоколы TCP и UDP. Протокол управления передачей TCP решает задачу обеспечения надежной информационной связи между двумя конечными узлами. Дейтаграммный протокол UDP используется как экономичное средство связи уровня межсетевого взаимодействия с прикладным уровнем.

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

- Протоколы *уровня сетевых интерфейсов* обеспечивают интеграцию в составную сеть других сетей. Этот уровень не регламентируется, но поддерживает все популярные стандарты физического и канального уровней: для локальных сетей — Ethernet, Token Ring, FDDI и т. д., для глобальных сетей — X. 25, frame relay, PPP, ISDN и т.д.

- Протокол IP решает задачу доставки сообщений между узлами составной сети по сетевым адресам. Протокол IP относится к протоколам без установления соединений, поэтому он не дает никаких гарантий надежной доставки сообщений. Все вопросы обеспечения надежности доставки данных в составной сети в стеке TCP/IP решает

протокол TCP, основанный на установлении логических соединений между взаимодействующими процессами.

- IP-пакет состоит из заголовка и поля данных. Максимальная длина пакета 65 535 байт. Заголовок обычно имеет длину 20 байт и содержит информацию о сетевых адресах отправителя и получателя, о времени жизни пакета, о контрольной сумме и некоторых других. В поле данных IP-пакета находятся сообщения более высокого уровня, например TCP или UDP.
- В заголовках пакетов транспортного уровня TCP и UDP содержатся номера портов, которые указывают (адресуют) точки входа в прикладные процессы, выполняющиеся на узлах сети. Таким образом, данные пользователя доставляются на узел в IP-пакетах по сетевому адресу, а затем извлекаются из пакета транспортного протокола и передаются прикладному протоколу или приложению по номеру порта.

Основная литература

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3-е изд.–СПб: Питер. 2006.- 958с. (Dragon2/ebooks/Networking)
2. Таненбаум Э. Компьютерные сети. 4-е изд.–СПб: Питер. 2005.- 992с. (Dragon2/ebooks/Networking)
3. Кулаков Ю.О., Луцький Г.М. Комп'ютерні мережі. Підручник/ за ред. Ю.С. Ковтанюка –К: Юніор, 2005.-400с.
4. Компьютерные сети. Сертификация Networks+ .Учебный курс/Пер.с англ.-М.: Издательско-торговый дом «Русская редакция». 2002.-703с.
5. Кульгин М. Энциклопедия. Технологии корпоративных сетей, –Санкт-Петербург: "Питер", 2000.

КНУ Шевч. - Інтелектуальних та інформаційних систем

http://fit.univ.kiev.ua/%D0%BA%D0%B0%D1%84%D0%B5%D0%B4%D1%80%D0%B8/%D1%96%D0%BD%D1%82%D0%B5%D0%BB%D0%B5%D0%BA%D1%82%D1%83%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D1%85-%D1%82%D0%B0-%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B8%D1%85-%D1%81