Федеральное агентство по образованию

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ
(ТУСУР)

Кафедра Электронных приборов (ЭП)

Е.Ю. Агеев

Локальные компьютерные сети

Конспект лекций по курсу «Локальные компьютерные сети»
для студентов специальности 200300
«Электронные приборы и устройства»

Томск 2007

Оглавление

1. Локальные компьютерные сети, базовые понятия

1.1. Компьютерные сети и эволюция компьютеров

Появление компьютерных сетей является логическим результатом развития компьютерной технологии. Связь одного компьютера с другими компьютерами, обмен информацией между ними, подключение к удаленным ресурсам и оборудованию, все это расширяет возможности отдельного компьютера, повышает эффективность его использования. Однако такая задача не решается просто физическим соединением компьютеров каналами связи. Она оказывается сложной, многоуровневой и должна быть решена на каждом из этих уровней.

Для того, чтобы компьютеры могли обмениваться информацией, они должны уметь обрабатывать запросы друг от друга. Обработка запроса другого компьютера – это особый режим работы, без которого связь невозможна. Любой компьютер работает под управлением операционной системы (ОС), в состав которой входят программы-драйверы, обеспечивающие взаимодействие с периферийными устройствами: клавиатурой, монитором, магнитными дисками и прочими. Программа-драйвер интегрируется в состав ОС однократно и впоследствии не изменяется, как не изменяется и само периферийное устройство, которое она обслуживает. Поскольку управление всеми устройствами компьютера осуществляет ОС, никаких проблем с их работой не возникает. Но процесс обмена информацией между несколькими компьютерами не может быть обеспечен каким-то «внешним» управлением, нет такой ОС, в состав которой входят все компьютеры сети, да и негде ее разместить. Более того, сами компьютеры в сети могут работать под управлением разных ОС. Это не должно мешать им «договариваться». Задача решается включением в состав ОС каждого компьютера специальных клиент-серверных модулей, такие модули – необходимая составная часть сетевой ОС.

Сетевая ОС *– операционная система, обеспечивающая работу компьютера в*

сети.

Серверные модули сетевой ОС постоянно находятся в режиме ожидания запросов, поступающих по сети от других компьютеров. Клиентские модули вырабатывают запросы на доступ к удаленным ресурсам и передают их по сети на нужный компьютер. Пара модулей «клиент-сервер» обеспечивает совместный доступ пользователей к определенному типу ресурсов, например к файлам. В этом случае говорят, что пользователь имеет дело с файловой службой (service). Обычно сетевая ОС поддерживает несколько видов сетевых служб: файловую службу, службу печати, службу электронной почты, службу удаленного доступа и т. п. Сетевые службы всегда представляют собой распределенные программы.

Распределенная программа *– это программа, которая состоит из нескольких взаимодействующих частей, выполняющихся на разных компьютерах.*

Термины «клиент» и «сервер» используются не только для обозначения программных модулей, но и компьютеров, подключенных к сети. Если компьютер предоставляет свои ресурсы другим компьютерам сети, то он называется сервером, а если он их потребляет – клиентом. Зачастую один и тот же компьютер может одновременно играть роли и сервера, и клиента.

1.1.1. Оборудование компьютерных сетей

Любая компьютерная сеть состоит из следующих элементов:

- компьютеров с установленными сетевыми операционными системами;
- линий связи;
- коммуникационного оборудования.

Каждый компьютер для подключения к сети оснащается сетевым адаптером или сетевой картой (англ.: NIC – Net Interface Card). Хотя компьютеры и являются центральными элементами обработки данных в сетях, не менее важную роль играют линии связи и коммуникационные устройства. Скорость обмена

информацией определяется не только, а часто и не столько возможностями локального компьютера, сколько характеристиками линии связи и коммуникационного оборудования. Сегодня коммуникационное устройство может представлять собой сложный специализированный мультипроцессор, который нужно конфигурировать, оптимизировать и администрировать. Рассмотрим основные типы сетевых коммуникационных устройств.

Повторитель (англ.: repeater) - простейшее из коммуникационных устройств, имеет два порта. Повторитель, получив сигнал на одном из своих портов, восстанавливает мощность, амплитуду и форму сигнала и повторяет его на другом порту, соединяя участки сети, в которых сигнал распространяется без заметного ослабления. Такие участки называют **сегментами** сети. Это позволяет преодолеть ограничения на длину линий связи, вызванные затуханием и искажением при распространении сигнала, однако прохождение сигнала через повторитель вносит дополнительную задержку распространения.

Концентратор (англ.: hub) - многопортовый повторитель, имеет от 4 до 24 портов. Сигнал, полученный на одном из портов, повторяется на всех остальных портах. Существует несколько типов концентраторов:

- **Пассивный** (Passive hub) – не выполняет усиления и восстановления формы сигнала, служит только для создания общей кабельной системы, объединяющей все компьютеры сети.
- **Активный** (Active hub) – работает подобно повторителю с той разницей, что имеет больше портов.
- **Умный** (Intelligent hub) – кроме усиления и восстановления формы сигнала способен анализировать состояние портов и отключать порт, к которому подключен неисправный компьютер, непрерывно передающий сигналы, блокируя работу всей сети.

Мост (англ.: bridge) имеет два порта. Делит общую среду передачи сети на две части (часто называемые логическими сегментами), передавая информацию из одного сегмента в другой только в том случае, если такая передача дей-

ствительно необходима, то есть если адрес компьютера назначения принадлежит другой подсети. (Мост использует адреса, которыми маркируют сетевые карты производители, каждая сетевая карта имеет уникальный адрес). Тем самым мост изолирует **трафик** (суммарный объем передаваемой и принимаемой информации) одной подсети от трафика другой, повышая общую производительность передачи данных в сети. Локализация трафика не только экономит пропускную способность, но и уменьшает возможность несанкционированного доступа к данным, так как **кадры** (блоки информации, которыми происходит передача по кабельной системе) не выходят за пределы своего сегмента и их сложнее перехватить злоумышленнику.

Коммутатор (англ.: switch, switching hub) – многопортовый мост. Одно из самых сложных и «интеллектуальных» коммуникационных устройств. Основное отличие коммутатора от моста состоит в том, что каждый его порт оснащен специализированным процессором, который обрабатывает кадры по алгоритму моста независимо от процессоров других портов. За счет этого общая производительность коммутатора обычно намного выше производительности традиционного моста, имеющего один процессорный блок. Можно сказать, что коммутаторы - это мосты нового поколения, которые обрабатывают кадры в параллельном режиме.

Маршрутизатор (англ.: router) Маршрутизатор представляет собой специализированный компьютер. Маршрутизаторы также образуют логические сегменты в сети используя систему адресации. Но маршрутизаторы используют не аппаратные адреса сетевых карт, а **сетевые адреса**, присваиваемые каждому компьютеру сети. В этих адресах имеется поле номера сети, так что все компьютеры, у которых значение этого поля одинаково, принадлежат к одному сегменту, называемому в данном случае подсетью (subnet). Маршрутизаторы не передают **широковещательные** запросы (запросы специального типа, подобные объявлению: «Всем! Всем! Всем!») из одной подсети в другую. Маршрутизаторы не имеют портов, их входы аналогичны сетевым картам компьютеров.

Любой маршрутизатор имеет не менее двух таких входов.

1.1.2. Топология и способ построения компьютерной сети

Структура построения компьютерной сети описывается топологией. Можно определить физическую и логическую топологии компьютерной сети. Под физической топологией понимается конфигурация физических каналов связи, соединяющих компьютеры и коммуникационное оборудование в сети, а под логической – конфигурация информационных потоков между компьютерами. Во многих случаях физическая и логическая топологии сети совпадают, но так бывает не всегда.

Три основных сетевых топологии получили название:

- **Общая шина** (англ.: bus). Физическая топология общая шина характеризуется тем, что все компьютеры сети подключены к одной общей линии связи. Логическая топология общая шина означает, что информация от каждого компьютера может одновременно передаваться всем остальным компьютерам;
- **Звезда** (англ.: star). Физическая топология звезда предполагает наличие выделенного, центрального элемента в сети: компьютера или коммуникационного устройства. К центральному элементу линиями связи присоединяются остальные компьютеры. В случае логической топологии звезда, центральный компьютер управляет сетью, он определяет когда и какой компьютер сети может передать сообщение, принимает его и определяя адресата, отправляет по назначению;
- **Кольцо** (англ.: ring). Физическая топология кольцо означает последовательное соединение всех компьютеров сети в замкнутую цепочку. Логическая топология кольцо строго задает направление передачи информации. Каждый компьютер передает информацию всегда только одному компьютеру, следующему за ним в цепочке, а получает информацию только от предыдущего в цепочке компьютера.

Существуют и другие топологии, например **полносвязная** (англ.: mesh) топология, в которой каждый компьютер сети соединен со всеми остальными компьютерами отдельными каналами связи. Полносвязная топология используется в тех случаях, когда существует риск повреждения и выхода из строя линий связи и, в то же время, нельзя допустить прекращения обмена информацией. Достаточно распространена топология **дерево** (англ.: tree) или (другое название этой топологии) **иерархическая звезда**. На практике иногда используют и комбинации различных топологий.

Кроме топологии или способа соединения компьютеров в локальной сети, различают два способа построения таких сетей: одноранговые сети (они еще называются сетями peer-to-peer, сокращенно p2p) и сети с выделенным сервером.

Одноранговые сети – это сети равноправных компьютеров, т.е. каждый компьютер одновременно выполняет функции и клиента (отправляет запросы по сети) и сервера (обрабатывает поступающие запросы). Процесс создания одноранговой сети в Windows 9x/2000/XP решается достаточно просто: каждый компьютер должен получить уникальное сетевое имя и входить в одну и ту же рабочую группу с другими компьютерами локальной сети. Управление сетевыми ресурсами компьютеров также не вызывает трудностей, можно разрешить совместный доступ к дискам, файлам или устройствам, подключенным к конкретному компьютеру, создать сетевую папку, диск или принтер на своем компьютере, разрешив к ней доступ из сети. Если это сделают и другие пользователи в сети, то вы сможете работать с дисками друг друга. Преимущества одноранговой сети очевидны: это простое и экономичное решение. Однако у одноранговых сетей есть и серьезные недостатки:

- Низкая скорость доступа к данным. Данные, которыми будут пользоваться все клиенты сети, скорее всего будут размещены на одном или нескольких компьютерах. Однако, обычные компьютеры плохо приспособлены для обработки большого количества сетевых запросов. В то же время, в

организации невозможно на каждом рабочем месте поставить высокопроизводительный компьютер.

- Низкая надежность работы сети. Для повышения надежности может быть принят целый ряд мер: дублирование дисков, регулярное резервное копирования, обеспечение компьютера источником бесперебойного питания и т.д. Но если использовать все эти меры на каждом компьютере одноранговой сети, теряются ее преимущества – простота и экономичность.

В локальной сети с выделенным сервером, компьютеры пользователей (обычно они носят название рабочих станций) работают, как правило, только как клиенты, отправляя серверу свои запросы. Компьютер, выполняющий роль сервера может специализироваться на работе с файлами (файловый сервер), выполнять задачи архивного хранения данных (сервер резервного копирования), управления печатью на сетевом принтере (сервер печати), получения и обработки электронной почты (почтовый сервер) или организации доступа в Интернет (вебсервер). Все эти задачи могут выполняться отдельно специализированными компьютерами, а могут быть совмещены в рамках одного компьютера, в зависимости от объема и интенсивности сетевых запросов. Обычные пользователи за сервером не работают, он обслуживается и настраивается администратором сети. Компьютер, выполняющий функции сервера, может быть сконфигурирован на основе обычной рабочей станции с высокоскоростным процессором, увеличенным объемом оперативной памяти и применением высоконадежной дисковой системы, а может быть построен на основе специализированной серверной компьютерной системы, целиком разрабатываемой для обеспечения высокопроизводительной обработки большого количества сетевых запросов и предоставления ресурсов клиентам. При этом сервер может не иметь монитора, для его обслуживания используются специализированные программы, запускаемые на других компьютерах сети или даже извне, по каналам связи, и подключающиеся к серверу так же, как другие клиенты. Сети с выделенным сервером имеют высокую надежность и производительность, однако это решение более доро-

гое. Если же в локальной компьютерной сети необходимо обеспечить безопасность и конфиденциальность доступа к информации, единственным решением будет сеть с выделенным сервером. На сервер устанавливается специальная сетевая операционная система с четкой моделью разграничения прав доступа и протоколированием процесса входа в сеть каждого пользователя. Используются надежные алгоритмы аутентификации (подтверждения личности пользователя) и шифрования персональных пользовательских данных. Сам компьютер-сервер устанавливается в хорошо защищенном и охраняемом помещении, а в качестве компьютеров пользователей могут использоваться бездисковые рабочие станции, т.е. компьютеры, у которых отсутствует винчестер и дисковод, так что после выключения в них не сохраняется никакой информации (все файлы хранятся на сервере). Это предотвращает несанкционированное копирование секретной информации.

1.1.3. Стандартизация подходов, модели взаимодействия, модель OSI

Сложная задача организации взаимодействия компьютеров в сети, как и многие другие сложные задачи, решается путем ее разбиения на взаимосвязанную последовательность из нескольких более простых задач. При этом решение каждой составной части общей проблемы можно рассматривать самостоятельно, согласовав интерфейс взаимодействия с предыдущими и последующими частями общей задачи. Иерархическое представление сложного процесса в виде последовательности связанных уровней, на каждом из которых выполняются вполне определенные действия, позволяет упростить решение сложной задачи, облегчает анализ ошибок, допущенных в ходе поиска решения, облегчает понимание логики решения проблемы. В случае взаимодействия компьютеров в сети особенно важно установить единый, стандартный подход ко всем этапам такого взаимодействия, чтобы реализация этого подхода не влияла на нормальную работу компьютера в сети независимо от его производителя, установленной операционной системы или аппаратной конфигурации.

В начале 80-х годов ряд международных организаций по стандартизации разработали модель, которая сыграла значительную роль в развитии компьютерных сетей. Эта модель называется **моделью взаимодействия открытых систем** (Open System Interconnection, OSI) или моделью OSI. Модель OSI определяет различные уровни взаимодействия систем, дает им стандартные имена и указывает, какие функции должен выполнять каждый уровень. Модель OSI была разработана на основании большого опыта, полученного при создании компьютерных сетей. В модели OSI (рис. 1) средства взаимодействия делятся на семь уровней: прикладной, представительный, сеансовый, транспортный, сетевой, канальный и физический. Каждый уровень имеет дело с одним определенным аспектом взаимодействия сетевых устройств. При этом процедура взаимодействия на каждом уровне может быть описана в виде набора формализованных правил, определяющих последовательность и формат сообщений, которыми обмениваются сетевые компоненты, лежащие на одном уровне в разных узлах. Такой набор правил для каждого уровня называют **протоколом** взаимодействия. Для одного и того же уровня может существовать целый ряд различных протоколов, но в конкретном случае взаимодействия, в определенный момент времени всегда используется какой-то один определенный протокол.

Функции всех уровней модели OSI могут быть отнесены к одной из двух групп: либо к функциям, зависящим от конкретной технической реализации сети, либо к функциям не зависящим от такой реализации. Три нижних уровня: физический, канальный и сетевой, являются сетезависимыми, то есть протоколы этих уровней тесно связаны с технической реализацией сети и используемым коммуникационным оборудованием.

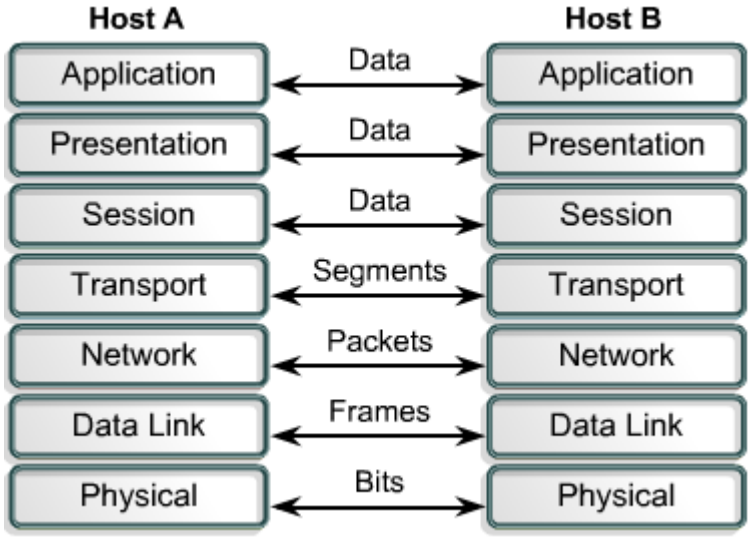

Рис. 1. Модель сетевого взаимодействия OSI

Три верхних уровня - прикладной, представительный и сеансовый – ориентированы на программные приложения и мало зависят от технических особенностей построения сети. На протоколы этих уровней не влияют изменения в топологии сети, замена оборудования или переход на другую сетевую технологию. Транспортный уровень является промежуточным, он скрывает все детали функционирования нижних уровней от верхних. Это позволяет разрабатывать приложения, не зависящие от технических средств непосредственной транспортировки сообщений.

Все протоколы верхних уровней, начиная с транспортного уровня и выше, реализуются программными средствами конечных узлов сети – компонентами их сетевых операционных систем. Протоколы нижних четырех уровней обобщенно называют сетевым транспортом или транспортной подсистемой, так как они полностью решают задачу транспортировки сообщений с заданным уровнем качества в составных сетях с произвольной топологией и различными технологиями. Верхние уровни решают задачи предоставления прикладных сервисов на основании имеющейся транспортной подсистемы.

Рассмотрим более подробно функции, выполняемые каждым уровнем в модели OSI.

- **Прикладной уровень** (Application layer). Большое число типов разделяемых ресурсов определяет соответственно широкий спектр протоколов, с помощью которых пользователи сети, запуская то или иное приложение, получают доступ к этим ресурсам. Это могут быть, например, файлы, принтеры, гипертекстовые страницы или сообщения электронной почты. Единица данных, которой оперирует прикладной уровень, обычно называется сообщением (message).
- **Представительный уровень** (Presentation layer) С помощью средств данного уровня протоколы прикладных уровней могут преодолеть синтаксические различия в представлении данных или же различия в кодировке символов. Задача, выполняемая уровнем представления информация, состоит в том, чтобы информация, передаваемая прикладным уровнем одной системы, была всегда понятна прикладному уровню другой системы. На этом уровне может выполняться шифрование и дешифрование данных, благодаря которому секретность обмена данными обеспечивается сразу для всех прикладных служб.
- **Сеансовый уровень** (Session layer) На сеансовом уровне осуществляется координация и управление работой компьютеров в сеансе связи. Выполняется синхронизация работы компьютеров, устанавливается, какая из сторон является активной в настоящий момент.
- **Транспортный уровень** (Transport layer) Задача, выполняемая транспортным уровнем – обеспечить передачу данных с той степенью надежности, которая требуется программным приложениям или верхним уровням – прикладному и сеансовому. На транспортном уровне сообщение разбивается на отдельные сегменты (segments) для проверки правильности передачи которых предусмотрены специальные процедуры.
- **Сетевой уровень** (Network layer). Сетевой уровень обеспечивает доставку данных между сетями, на этом уровне происходит выбор маршрута передачи. Под сетью здесь понимается совокупность компьютеров, соеди-

ненных между собой в соответствии с одной из стандартных типовых топологий и использующих для передачи данных один из протоколов нижнего, канального уровня, определенный для этой топологии. Сети соединяются между собой маршрутизаторами. На сетевом уровне сегменты, составляющие сообщение, дробятся на пакеты (packets).

- **Канальный уровень** (Data Link layer). На этом уровне выполняется проверка доступности физической среды для передачи данных, некоторые протоколы канального уровня позволяют выполнять проверку корректности передачи информации, выполнять обнаружение и коррекцию ошибок, однако функция исправления ошибок не является обязательной для канального уровня. На канальном уровне пакеты данных делятся на кадры (frames).
- **Физический уровень** (Physical layer). На данном уровне происходит передача битов по физическому каналу связи, задаются характеристики электрических сигналов, передающих дискретную информацию, например, крутизна фронтов импульсов, уровни напряжения или тока передаваемого сигнала, тип кодирования, скорость передачи сигналов. Кроме этого, здесь стандартизуются типы разъемов и назначение каждого контакта. Функции физического уровня реализуются во всех устройствах, подключенных к сети. Со стороны компьютера функции физического уровня выполняются сетевым адаптером.

1.1.4. Локальные сети в общей классификации компьютерных сетей

С самого момента появления первых компьютерных сетей существовало разделение их на локальные (LAN) и глобальные (WAN) компьютерные сети. Такое разделение обычно связывается с размером сети, в то же время, очевидно, что этот размер достаточно условен. Более глубокая причина необходимости такой классификации компьютерных сетей связана с тем, что сетевые технологии, используемые в локальных компьютерных сетях, не могут применяться в гло-

бальных сетях.

Сетевая технология *– это согласованный набор стандартных протоколов и реализующих их программно-аппаратных средств (сетевых адаптеров, драйверов, кабелей, разъемов и т.п.), достаточный для построения вычислительной сети*

В пределах небольшой компьютерной сети легко реализовать однотипный канал связи, одну сетевую технологию и получить высокую скорость передачи данных. Огромная стоимость глобальной сети, которая могла бы быть построена на основе подобного подхода, определяет нереальность ее создания. Поэтому сетевые технологии глобальных компьютерных сетей изначально существенно отличаются от технологий локальных сетей. Однако, ситуация в этой области не остается такой же, как и 20 лет назад. Развитие глобальных компьютерных сетей привело к появлению единой глобальной сети – Интернет. Если создание локальной сети в эпоху «до Интернет» преследовало цели обмена информацией внутри локальной сети и совместного использования оборудования (например, принтеров), то сейчас всякая локальная сеть имеет связь с Интернет и, иногда, возможность выхода в Интернет из локальной сети рассматривается как основная функция этой сети. Создание в последние годы в крупных городах сетей высокоскоростных оптоволоконных каналов связи, привело к появлению в «размерной» классификации сетей промежуточного звена – городских компьютерных сетей (MAN). Эффективность некоторых технологий глобальных компьютерных сетей оказалась настолько высокой, что они стали использоваться и в локальных сетях. Происходит развитие сетевых технологий в целом и в этом процессе локальные и глобальные компьютерные сети оказываются тесно связанными. Возможно, в отдаленном будущем это и приведет к созданию единой глобальной сверхсети, построенной с использование какой-то одной, возможно, еще не известной, сетевой технологии.

Вопросы для самостоятельной проработки:

1. Поясните значения терминов «клиент», «сервер».
2. Что такое топология сети, какие виды топологий вам известны.
3. Какое оборудование используется в компьютерных сетях, опишите функции, выполняемые этим оборудованием.
4. Чем сетевая операционная система отличается он несетевой.
5. Что такое распределенная программа.
6. Какие уровни модели OSI являются сетезависимыми, какие сетенезависимыми.
7. Что такое сетевая технология.
8. Перечислите уровни, существующие в модели OSI и функции ими выполняемые.
9. Что такое сетевой протокол.
10. Чем локальные компьютерные сети отличаются от глобальных.
11. Что такое сетевая служба.
12. На каком уровне модели OSI передаваемые данные группируются в пакеты, в кадры, в сегменты.
13. Что называется сетевым транспортом или транспортной подсистемой
14. Протоколы каких уровней OSI реализуются программными средствами конечных узлов сети.
15. Что такое сетевой трафик.

2. Классические технологии локальных сетей

Для упрощения и, соответственно, удешевления аппаратных и программных решений разработчики первых локальных сетей остановились на совместном использовании кабелей всеми компьютерами сети в режиме разделения времени. Использование разделяемых сред (shared media) позволяет упростить логику работы сети и удешевить ее. Протоколы, на основе которых строится

сеть определенной технологии, специально разрабатывались для совместной работы, поэтому не требуется дополнительных усилий по организации их взаимодействия. Иногда технологии локальных сетей называют **базовыми технологиями**, имея в виду то, что на их основе строится базис любой сети. Для получения работоспособной сети достаточно приобрести программные и аппаратные средства, относящиеся к одной базовой технологии – сетевые адаптеры с драйверами, концентраторы, коммутаторы, кабельную систему и т. п., – и соединить их в соответствии с требованиями стандарта на данную технологию.

Несмотря на появление новых технологий, классические протоколы локальных сетей продолжают использоваться, кроме того, современные высокопроизводительные технологии в значительной степени сохраняют преемственность со своими предшественниками. Поэтому знание базовых технологий локальных сетей необходимо для успешного применения современной коммуникационной аппаратуры.

2.1. Структура стандартов IEEE 802.X

В 1980 году в институте IEEE был организован комитет 802 по стандартизации локальных сетей, в результате работы которого было принято семейство стандартов IEEE 802.x, которые содержат рекомендации по проектированию нижних уровней локальных сетей. Стандарты семейства IEEE 802.x охватывают только два нижних уровня модели OSI – физический и канальный. Это связано с тем, что именно эти уровни в наибольшей степени отражают специфику работы локальных сетей. Старшие же уровни, начиная с сетевого, в значительной степени имеют общие черты, как для локальных, так и для глобальных сетей.

Специфика локальных сетей нашла свое отражение в разделении канального уровня на два подуровня:

- логической передачи данных (Logical Link Control, LLC);
- управления доступом к среде (Media Access Control, MAC).

Уровень MAC появился из-за существования в локальных сетях разделяемой

среды передачи данных. Именно этот уровень обеспечивает корректное совместное использование общей среды, предоставляя ее в соответствии с определенным алгоритмом в распоряжение той или иной станции сети. Независимо от используемой технологии, все сетевые адаптеры снабжены уникальным адресом длиной 6 байт, получившим наименование **MAC-адреса**. Уровень LLC организует передачу логических единиц данных, кадров информации, с заданным качеством транспортных услуг. Протоколы уровней MAC и LLC взаимно независимы.

Сегодня комитет 802 включает ряд подкомитетов, в который входят как уже упомянутые, так и некоторые другие:

- 802.1 – Internetworking – объединение сетей;
- 802.2 – Logical Link Control, LLC – управление логической передачей данных;
- 802.3 – Ethernet с методом доступа CSMA/CD;
- 802.4 – Token Bus LAN – локальные сети с методом доступа Token Bus;
- 802.5 – Token Ring LAN – локальные сети с методом доступа Token Ring;
- 802.6 – Metropolitan Area Network, MAN – сети мегаполисов;
- 802.7 – Broadband Technical Advisory Group – техническая консультационная группа по широкополосной передаче;
- 802.8 – Fiber Optic Technical Advisory Group – техническая консультационная группа по волоконно–оптическим сетям;
- 802.9 – Integrated Voice and data Networks – интегрированные сети передачи голоса и данных;
- 802.10 – Network Security – сетевая безопасность;
- 802.11 – Wireless Networks – беспроводные сети;
- 802.12 – Demand Priority Access LAN, 100VG-AnyLAN – локальные сети с методом доступа по требованию с приоритетами;
- 802.14 – Cable-TV Based Broadband Communication Network – широкополосные сети на основе телевизионных кабельных сетей;

- 802.16 – Worldwide Interoperability for Microwave Access – новый стандарт беспроводных сетей.

2.2. Технология Ethernet (стандарт IEEE 802.3)

Ether в переводе с английского – эфир. Ethernet – «эфирная сеть», сеть основанная на принципе использования общей разделяемой среды доступа – «эфира». Впервые метод доступа, используемый в сетях Ethernet, был опробован во второй половине 60-х годов в радиосети Гавайского университета. В 1980 году фирмы DEC, Intel и Xerox на основании фирменного стандарта компании Xerox разработали и опубликовали стандарт Ethernet для сети, построенной на основе коаксиального кабеля. Стандарт Ethernet DIX с небольшими доработками был «узаконен» институтом инженеров по электротехнике и электронике (IEEE), как стандарт IEEE 802.3. Основной принцип, положенный в основу Ethernet, – случайный метод доступа к разделяемой физической среде передачи данных. Для обозначения метода доступа в сетях Ethernet используется аббревиатура **CSMA/CD**, расшифровывается как: Carrier Sense Multiple Access with Collision Detection – множественный доступ с контролем несущей и обнаружением столкновений. Этот метод применяется исключительно в сетях с логической общей шиной (к которым относятся и радиосети, породившие этот метод). Все компьютеры такой сети имеют непосредственный доступ к общей шине, поэтому она может быть использована для передачи данных между любыми двумя узлами сети. Простота схемы подключения – это один из факторов, определивших успех стандарта Ethernet. Говорят, что кабель, к которому подключены все станции, работает в режиме коллективного доступа (Multiply Access, MA). При передаче двоичных сигналов используется манчестерское кодирование. В качестве физической среды может использоваться толстый или тонкий коаксиальный кабель, витая пара, оптическое волокно или радиоволны.

В зависимости от типа физической среды стандарт IEEE 802.3 имеет различные модификации, перечисленные в таблице 1.

Табл. 1

Наименование модификации Ethernet	Используемая физическая среда
10Base5	Толстый (внешний диаметр около 10 мм) коаксиальный кабель
10Base2	Тонкий (внешний диаметр около 5 мм) коаксиальный кабель
10Base T	Витая пара (медный кабель, свитый из двух проводников)
10Base FL	Многомодовое или одномодовое оптоволокно
10Base FB	Многомодовое или одномодовое оптоволокно

Число рабочих станций в сети Ethernet не должно превышать 1024, однако модификации, использующие коаксиальный кабель, устанавливают более жесткие ограничения. Слово Base, присутствующее в названиях всех модификаций технологии Ethernet, происходит от Baseband network и означает сеть с немодулированной передачей (в отличие от Broadband сетей), в которой сообщения пересылаются в цифровой форме по единственному каналу, без частотного разделения. Цифра слева от Base показывает частоту передачи данных в МГц, а цифры или буквы справа – тип физической среды.

2.2.1. Формат кадра и этапы доступа к среде

Все данные, передаваемые по сети, помещаются в кадры следующей структуры:

- **Поле преамбулы** (Preamble) состоит из 7 байт 10101010, предназначенных для синхронизации передающей и приемной станций.
- **Начальный ограничитель кадра** (Start–of–frame–delimiter, SFD) состоит из одного байта 10101011, показывает, что следующие 6 байт содержат адрес назначения.
- **Адрес назначения** (Destination Address, DA) размер которого составляет 6 байт.

- **Адрес источника** (Source Address, SA) – это также 6–байтовое поле, содержащее адрес узла – отправителя кадра.
- **Длина** (Length, L) – 2–байтовое поле, которое определяет длину поля данных в кадре.
- **Поле данных** (Data) может содержать от 0 до 1500 байт. Но если длина поля меньше 46 байт, то используется следующее поле – поле заполнения, – чтобы дополнить кадр до минимально допустимого значения в 46 байт.
- **Поле заполнения** (Padding) состоит из такого количества байт заполнителей, которое обеспечивает минимальную длину поля данных в 46 байт. Если длина поля данных достаточна, то поле заполнения в кадре отсутствует.
- **Поле контрольной суммы** (Frame Check Sequence, FCS) состоит из 4 байт, содержащих контрольную сумму. После получения кадра рабочая станция выполняет собственное вычисление контрольной суммы для этого кадра, сравнивает полученное значение со значением поля контрольной суммы, определяя, не был ли искажен полученный кадр.

Таким образом, минимальный размер кадра составляет 72 байта, а максимальный 1526 байт.

Чтобы получить возможность передавать кадр, станция должна убедиться, что разделяемая среда свободна. Это достигается прослушиванием основной гармоники сигнала, которая также называется несущей частотой (carrier–sense, CS). Признаком незанятости среды является отсутствие на ней несущей частоты, которая при манчестерском способе кодирования равна 5-10 МГц, в зависимости от последовательности единиц и нулей, передаваемых в данный момент. Если среда свободна, то узел имеет право начать передачу кадра.

Все станции, подключенные к кабелю, могут распознать факт передачи кадра, и та станция, которая узнает собственный адрес в заголовках кадра, записывает его содержимое в свой внутренний буфер, обрабатывает полученные данные, передает их вверх по своему стеку, а затем посылает по кабелю кадр-

ответ. Так как адрес станции источника содержится в исходном кадре, станция-получатель знает, кому нужно послать ответ.

После окончания передачи кадра все узлы сети обязаны выдержать технологическую паузу (Inter Packet Gap) в 9,6 мкс. Эта пауза, называемая также межкадровым интервалом, нужна для приведения сетевых адаптеров в исходное состояние, а также для предотвращения монопольного захвата среды одной станцией. После окончания технологической паузы узлы имеют право начать передачу своего кадра, так как среда свободна. Из-за задержек распространения сигнала по кабелю не все узлы строго одновременно фиксируют факт окончания передачи кадра.

2.2.2. Обработка коллизий и производительность сети

Механизм прослушивания среды и пауза между кадрами не гарантируют от возникновения такой ситуации, когда две или более станции одновременно решают, что среда свободна, и начинают передавать свои кадры. Говорят, что при этом происходит **коллизия** (collision), так как содержимое обоих кадров сталкивается на общем кабеле и происходит искажение информации – методы кодирования, используемые в Ethernet, не позволяют в этом случае выделять сигналы каждой станции из общего сигнала.

Коллизия – это нормальная ситуация в работе сетей Ethernet, она является следствием распределенного характера сети. Коллизия возникает из–за того, что один узел начинает передачу раньше другого, но до второго узла сигналы первого просто не успевают дойти к тому времени, когда второй узел решает начать передачу своего кадра.

Чтобы корректно обработать коллизию, все станции одновременно наблюдают за возникающими на кабеле сигналами. Если передаваемые и наблюдаемые сигналы отличаются, то фиксируется **обнаружение коллизии** (collision detection, CD). Для того, чтобы все рабочие станции быстрее «заметили» коллизию, станция, которая обнаружила коллизию первой, прерывает передачу своего

кадра (в произвольном месте, возможно, и не на границе байта) и усиливает ситуацию коллизии посылкой в сеть специальной последовательности из 32 бит, называемой **jam–последовательностью**.

После этого обнаружившая коллизию передающая станция обязана прекратить передачу и сделать паузу в течение короткого случайного интервала времени. Затем она может снова предпринять попытку захвата среды и передачи кадра. Случайная пауза выбирается по формуле:

$$\text{Пауза} = L * (\text{интервал отсрочки}), \quad (1)$$

где интервал отсрочки равен 512 битовым интервалам (в технологии Ethernet принято все интервалы измерять в битовых интервалах; битовый интервал обозначается как **bt** и соответствует времени между появлением двух последовательных бит данных на кабеле; для скорости 10 Мбит/с величина битового интервала равна 0,1 мкс или 100 нс);

L представляет собой целое число, выбранное с равной вероятностью из диапазона $[0, 2^N]$, где N – номер повторной попытки передачи данного кадра: 1,2,..., 10. После 10-й попытки интервал, из которого выбирается пауза, не увеличивается. Таким образом, случайная пауза может принимать значения от 0 до 52,4 мс. Если 16 последовательных попыток передачи кадра вызывают коллизию, то передатчик должен прекратить попытки и отбросить этот кадр.

Все компьютеры в сети Ethernet, использующие одну разделяемую среду доступа, образуют так называемый **домен коллизий** (collision domain). Узлы, образующие один домен коллизий, работают как единая распределенная электронная схема. Сеть Ethernet, построенная на повторителях или концентраторах, всегда образует один домен коллизий. Мосты, коммутаторы и маршрутизаторы делят сеть Ethernet на несколько доменов коллизий.

Четкое распознавание коллизий всеми станциями сети является необходимым условием корректной работы сети Ethernet. Для надежного распознавания коллизий должно выполняться следующее соотношение:

$$T_{min} >= PDV, \quad (2)$$

где T_{min} – время передачи кадра минимальной длины, а PDV – время, за которое сигнал коллизии успевает распространиться до самого дальнего узла сети. Так как в худшем случае сигнал должен пройти дважды между наиболее удаленными друг от друга станциями сети (в одну сторону проходит неискаженный сигнал, а на обратном пути распространяется уже искаженный коллизией сигнал), то это время называется **временем двойного оборота** (Path Delay Value, PDV). Кроме того, дополнительные задержки распространения сигнала, обозначаемые как PVV (Path Variability Value), вносит коммуникационное оборудование, это сказывается на сокращении межкадрового интервала IPG. Для упрощения расчетов конкретных сегментов сети обычно используются справочные данные, содержащие значения задержек распространения сигналов в повторителях, приемопередатчиках и различных физических средах.

В любом случае передающая станция должна успевать обнаружить коллизию, которую вызвал переданный ее кадр, еще до того, как она закончит передачу этого кадра. Выполнение этого условия зависит, с одной стороны, от длины минимального кадра, пропускной способности сети и наличия коммуникационного оборудования, а с другой стороны, от длины кабельной системы сети и скорости распространения сигнала в кабеле (для разных типов кабеля эта скорость несколько отличается).

Все параметры протокола Ethernet подобраны таким образом, чтобы при нормальной работе узлов сети коллизии всегда четко распознавались. В стандарте Ethernet принято, что минимальная длина поля данных кадра составляет 46 байт (что вместе со служебными полями дает минимальную длину кадра – 72 байт или 576 бит). Отсюда может быть определено ограничение на расстояние между наиболее удаленными станциями. Это расстояние называют также максимальным **диаметром сети**.

При разработке стандарта Ethernet в конце 70–х годов скорость передачи

данных в 10 Мбит/с была высока по сравнению со скоростью работы интерфейсной шины ISA, использовавшейся тогда в компьютерах, поэтому загрузка сети всегда была небольшой и сеть работала эффективно. При увеличении нагрузки растет число коллизий, и полезная пропускная способность сети Ethernet резко падает, так как сеть почти постоянно занята повторными попытками передачи кадров. Оптимальной считается 30% загрузка.

2.2.3. Производительность сети Ethernet

В качестве характеристики производительности коммуникационного оборудования используются единицы кадр/с и бит/с. Чаще используется единица кадр/с, так как для коммуникационного оборудования наиболее тяжелым режимом является обработка кадров минимальной длины. Количество таких кадров, поступающих на устройство в единицу времени, максимально, а на обработку каждого кадра мост, коммутатор или маршрутизатор тратит примерно одно и то же время. Другая характеристика производительности коммуникационного оборудования – бит/с – используется реже, так как она не учитывает размер обрабатываемого кадра, а на кадрах максимального размера достичь высокой производительности в бит/с гораздо легче.

Рассчитаем максимальную производительность сети Ethernet в кадр/с, для кадров минимальной и максимальной длины. Размер кадра минимальной длины составляет 72 байт или 576 бит, поэтому на его передачу затрачивается 57,6 мкс. Прибавив межкадровый интервал в 9,6 мкс, получаем, что период следования кадров минимальной длины составляет 67,2 мкс. Это дает 14 880 кадр/с.

Размер кадров максимальной длины составляет 1526 байт или 12 208 бит, а период следования кадров с учетом межкадрового интервала 1230,4 мкс. В этом случае максимальная пропускная способность составляет 813 кадр/с.

В проведенном расчете не учитывалось количество полезной информации, переданной по сети. Под **полезной пропускной способностью** понимается

скорость передачи пользовательских данных, которые переносятся полем данных кадра. Эта пропускная способность всегда меньше номинальной битовой скорости протокола Ethernet за счет наличия в кадре служебной информации, межкадровых интервалов и ожидания доступа к среде. Полезная пропускная способность измеряется в бит/с. Для кадров минимальной длины полезная пропускная способность равна:

$$C_П = 14880 * 46 * 8 = 5{,}48 \text{ Мбит/с}. \quad (3)$$

Это намного меньше 10 Мбит/с, но следует учесть, что кадры минимальной длины, вообще говоря, не используются для передачи данных, а выполняют служебные функции. Для кадров максимальной длины полезная пропускная способность равна:

$$C_П = 813 * 1500 * 8 = 9{,}76 \text{ Мбит/с}, \quad (4)$$

что весьма близко к номинальной скорости работы сети. Наличие в сети нескольких узлов кратно снижает эту величину за счет ожидания доступа к среде, а также за счет коллизий, приводящих к необходимости повторной передачи кадров.

2.2.4. Реализации технологии Ethernet 10 МГц

Стандарт 10Base–5

Использует толстый коаксиальный кабель марок RG8, RG11 с волновым сопротивлением 50 Ом максимальной длиной 500 м. При использовании повторителей, можно соединить несколько сегментов, но не более 5. В случае соединения 5 сегментов используется 4 повторителя. Два из 5 сегментов должны быть ненагружены, т.е. к ним нельзя подключать рабочие станции, они служат только для увеличения размера сети. Между нагруженными сегментами должны быть ненагруженные сегменты, так что максимальная конфигурация сети представляет собой два нагруженных крайних сегмента, которые соединяются ненагруженными сегментами еще с одним центральным нагруженным сегмен-

том. Правило применения повторителей в сети Ethernet 10 Base-5 носит название «**правило 5–4–3**». На концах кабеля в каждом сегменте должны быть установлены согласующие **терминаторы** («заглушки»), поглощающие распространяющиеся по кабелю сигналы и препятствующие возникновению отраженных сигналов. При отсутствии терминаторов работа сети становится невозможной. Станция подключается к кабелю при помощи приемопередатчика – **трансивера** (transmitter+receiver = transceiver). Трансивер может подсоединяться к кабелю как методом прокалывания, обеспечивающим непосредственный физический контакт, так и бесконтактным (индукционным) методом. Трансивер соединяется с сетевым адаптером интерфейсным кабелем **AUI** (Attachment Unit Interface) длиной до 50 м, состоящим из 4 витых пар (адаптер должен иметь разъем AUI). Наличие стандартного интерфейса между трансивером и остальной частью сетевого адаптера очень полезно при переходе с одного типа кабеля на другой. Для этого достаточно только заменить трансивер, а остальная часть сетевого адаптера остается неизменной. Для присоединения к интерфейсу AUI используется разъем DB-15.

Допускается подключение к одному сегменту не более 100 трансиверов, причем расстояние между подключениями трансиверов не должно быть меньше 2,5 м. На кабеле имеется разметка через каждые 2,5 м, которая обозначает точки подключения трансиверов. На самом деле точек подключения, отстоящих на 2,5 м, на 500 метровом кабеле не 100, а 99, причем для крайнего сегмента одна из них будет использована повторителем, а для среднего сегмента повторители включаются с двух сторон и забирают 2 точки подключения. Таким образом, максимальный диаметр сети 10 Base-5 составит 2500 метров, а максимальное количество подключаемых компьютеров – 293.

Стандарт 10 Base-2

Использует тонкий коаксиальный кабель марки RG-58 с волновым сопротивлением 50 Ом. Максимальная длина сегмента без повторителей составляет

185 м, как и в случае 10 Base-5, сегмент должен иметь на концах терминаторы. Стандарт 10 Base-2 также разрешает использование повторителей, применение которых должно соответствовать «правилу 5–4–3». Станции подключаются к кабелю с помощью высокочастотного BNC Т–коннектора, который представляет собой тройник, один отвод которого соединяется с сетевым адаптером, а два других – с двумя концами разрыва кабеля. Максимальное количество станций, подключаемых к одному сегменту – 30. Минимальное расстояние между станциями – 1 м. Кабель «тонкого» коаксиала имеет разметку для подключения узлов с шагом в 1 м.

Тонкий коаксиальный кабель дешевле толстого, кроме того, трансиверы в стандарте 10 Base-2 объединены с сетевыми адаптерами, поэтому реализация этого стандарта на практике приводит к наиболее дешевому решению, из–за чего сети 10 Base-2 иногда называют сетями Cheapernet (от cheaper – более дешевый). Но за дешевизну кабеля приходится расплачиваться качеством – «тонкий» коаксиал обладает худшей помехозащищенностью, худшей механической прочностью и более узкой полосой пропускания, к тому же большое количество механических соединений приводит к частым и трудноустранимым проблемам, – сеть не работает, но чтобы найти место повреждения нужно проверить все коннекторы.

Максимальный диаметр сети Ethernet 10Base-2 равен 5x185 = 925 м, максимальное число узлов в сети 86.

Стандарт 10 Base-T

Сети 10 Base-T используют в качестве среды две неэкранированные витые пары категории 3 (Unshielded Twisted Pair, UTP-3). В сети 10 Base-T должно присутствовать дополнительное устройство – концентратор. При этом одна витая пара используется для передачи данных к концентратору, а другая – для передачи данных от концентратора к станции. Конечные узлы соединяются с концентратором по топологии «звезда». Концентратор повторяет сигналы, по-

ступившие от одного из конечных узлов, на всех своих портах, кроме того, с которого они получены. Так образуется единая среда передачи данных – логическая общая шина. Максимальная длина витой пары, соединяющей концентратор и рабочую станцию 100 м. Концентраторы 10Base-T можно соединять друг с другом с помощью тех же портов, которые предназначены для подключения конечных узлов. Для обеспечения надежного распознавания коллизий устанавливается максимально число концентраторов между любыми двумя станциями сети – не более 4. Это правило носит название «**правила 4–х хабов**» и оно заменяет «правило 5–4–3», применяемое к коаксиальным сетям. При создании сети 10Base-T с большим числом рабочих станций концентраторы можно соединять друг с другом иерархическим способом, таким образом можно создать сеть, содержащую 1024 рабочих станции. Максимальный диаметр сети 10 Base-T составляет 5*100 = 500 м.

Сети, построенные на основе стандарта 10 Base-T, оказываются более удобными в эксплуатации по сравнению с коаксиальными вариантами Ethernet. Физическое разделение общей кабельной среды доступа на отдельные отрезки позволяет контролировать их состояние и отключать в случае обрыва, короткого замыкания или неисправности сетевого адаптера на индивидуальной основе. Это обстоятельство существенно облегчает эксплуатацию больших сетей Ethernet, так как концентратор может автоматически выполнять такие функции, уведомляя администратора сети о возникшей проблеме.

Оптоволоконный Ethernet

Функционально сеть Ethernet на оптическом кабеле состоит из тех же элементов, что и сеть стандарта 10Base–T – сетевых адаптеров, многопортового повторителя и отрезков кабеля, соединяющих адаптер с портом повторителя. Как и в случае витой пары, для соединения адаптера с повторителем используются два оптоволокна – приемное и передающее.

Стандарт FOIRL (Fiber Optic Inter–Repeater Link) первый стандарт коми-

тета 802.3 для использования оптоволокна в сетях Ethernet. Он устанавливает длину оптоволокна между повторителями до 1 км при общей длине сети не более 2500 м. Максимальное число повторителей между любыми узлами сети – 4.

Стандарт 10Base–FL представляет собой незначительное улучшение стандарта FOIRL. Увеличена мощность передатчиков, поэтому максимальное расстояние между узлом и концентратором увеличилось до 2000 м. При этом сохранилось требование выполнения «правила 4–х хабов» и не изменился максимальный диаметр сети в 2500 м.

Стандарт 10Base–FB предназначен только для соединения повторителей. Конечные узлы не могут использовать этот стандарт для присоединения к портам концентратора. Между узлами сети можно установить до 5 повторителей 10Base–FB при максимальной длине одного сегмента 2000 м и максимальной длине всей сети 2740 м.

Максимальное число конечных станций в случае Ethernet 10 Base-F также может достигать 1024.

2.3. Технология Token Ring (стандарт IEEE 802.5)

Технология Token Ring был разработана компанией IBM в 1984 году, а затем передана в качестве проекта стандарта в комитет IEEE 802, который на ее основе принял в 1985 году стандарт 802.5. Компания IBM использует технологию Token Ring в качестве своей основной сетевой технологии для построения локальных сетей на основе компьютеров различных классов.

Сети Token Ring работают с двумя битовыми скоростями – 4 и 16 Мбит/с. Смешение станций, работающих на различных скоростях, в одном кольце не допускается. Для контроля сети одна из станций выступает в роли **активного монитора**. Активный монитор выбирается во время инициализации кольца как станция с максимальным значением MAC–адреса, Если активный монитор выходит из строя, процедура инициализации кольца повторяется и выбирается новый активный монитор. Чтобы сеть могла обнаружить отказ активного монито-

ра, последний в работоспособном состоянии каждые 3 секунды генерирует специальный кадр своего присутствия. Если этот кадр не появляется в сети более 7 секунд, то остальные станции сети начинают процедуру выборов нового активного монитора.

2.3.1. Маркерный метод доступа к разделяемой среде

В сети Token Ring кольцо образуется отрезками кабеля, соединяющими соседние станции. Каждая станция связана с предшествующей и последующей и может непосредственно обмениваться данными только с ними. Данные любая станция всегда получает только от станции, которая находится перед ней в кольце. Такая станция называется **ближайшим активным соседом, расположенным выше по течению** (данных) – Nearest Active Upstream Neighbor, NAUN. Передачу же данных станция всегда осуществляет своему ближайшему соседу вниз по течению.

В сетях Token Ring со скоростью работы 4 Мбит/с применяется следующий алгоритм доступа станций к физической среде. По кольцу циркулирует специальный кадр – маркер (token). Получив маркер, станция анализирует его и при отсутствии у нее данных для передачи передает следующей станции. Станция, которая имеет данные для передачи, при получении маркера изымает его из кольца и выдает в кольцо кадр данных. Кадр снабжен адресом назначения и адресом источника. Переданные данные движутся по кольцу в одном направлении. Все станции кольца ретранслируют кадр. Когда кадр достигает станции назначения, она, распознав свой адрес, копирует кадр в свой внутренний буфер и, вставляя в кадр признак подтверждения приема, ретранслирует его дальше. Кадр, двигаясь дальше по кольцу, достигает станции–отправителя, которая, принимая этот кадр и обнаружив признак подтверждения приема, вновь передает в сеть маркер для обеспечения возможности другим станциям сети передавать данные.

В сетях Token Ring 16 Мбит/с используется несколько другой алгоритм

доступа к кольцу, называемый алгоритмом **раннего освобождения маркера** (Early Token Release). В соответствии с ним станция передает маркер доступа следующей станции сразу же после окончания передачи кадра, не дожидаясь его возвращения с признаком подтверждения приема. В этом случае пропускная способность кольца используется более эффективно, так как по кольцу одновременно продвигаются кадры нескольких станций.

Время владения разделяемой средой в сети Token Ring ограничивается **временем удержания маркера** (token holding time), по истечении которого станция обязана прекратить передачу данных (текущий кадр разрешается завершить) и передать маркер далее по кольцу. Станция может успеть передать за время удержания маркера один или несколько кадров в зависимости от размера кадров и величины времени удержания маркера. Обычно время удержания маркера по умолчанию равно 10 мс, а максимальный размер кадра в стандарте 802.5 не определен. Для сетей 4 Мбит/с он обычно равен 4 Кбайт, а для сетей 16 Мбит/с – 16 Кбайт. Это связано с тем, что за время удержания маркера станция должна успеть передать хотя бы один кадр. При скорости 4 Мбит/с за время 10 мс можно передать 5000 байт, а при скорости 16 Мбит/с – соответственно 20 000 байт. Максимальные размеры кадра выбраны немного меньше этих предельных значений, с некоторым запасом.

Для различных видов сообщений, передаваемым кадрам, могут назначаться различные **приоритеты**: от 0 (низший) до 7 (высший). Решение о приоритете конкретного кадра принимает передающая станция. Маркер также всегда имеет некоторый уровень текущего приоритета. Станция имеет право захватить переданный ей маркер только в том случае, если приоритет кадра, который она хочет передать, выше (или равен) приоритета маркера. В противном случае станция обязана передать маркер следующей по кольцу станции. За наличие в сети маркера, причем единственной его копии, отвечает активный монитор. Если активный монитор не получает маркер в течение длительного времени (например, 2,6 с), то он порождает новый маркер.

2.3.2 Форматы кадров Token Ring

В Token Ring существуют три формата кадров:

- маркер;
- кадр данных;
- прерывающая последовательность.

Кадр маркера

Кадр маркера состоит из трех полей, каждое длиной в один байт.

- **Начальный ограничитель** (Start Delimiter, SD) присутствует в начале маркера, а также в начале любого кадра, проходящего по сети.
- **Управление доступом** (Access Control) состоит из четырех подполей:

PPP	T	M	RRR

PPP – биты приоритета, T – бит маркера, M – бит монитора, RRR – резервные биты приоритета. Бит T, установленный в 1, указывает на то, что данный кадр является маркером доступа. Бит монитора устанавливается в 1 активным монитором и в 0 любой другой станцией, передающей маркер или кадр. Если активный монитор видит маркер или кадр, содержащий бит монитора со значением 1, то активный монитор знает, что этот кадр или маркер уже однажды обошел кольцо и не был обработан станциями. Если это кадр, то он удаляется из кольца. Если это маркер, то активный монитор передает его дальше по кольцу.

- **Конечный ограничитель** (End Delimeter, ED) – последнее поле маркера. Это поле содержит два однобитовых признака: I и E. Признак I (Intermediate) показывает, является ли кадр последним в серии кадров, в этом случае бит I равен 0 или промежуточным. Признак E (Error) – это признак ошибки. Он устанавливается в 0 станцией–отправителем, и любая станция кольца, через которую проходит кадр, должна установить этот признак в 1, если она обнаружит ошибку по контрольной сумме или другую некорректность кадра.

Кадр данных

Кадр данных состоит из следующих полей:

- начальный ограничитель (Start Delimiter, SD);
- управление кадром (Frame Control, PC);
- адрес назначения (Destination Address, DA);
- адрес источника (Source Address, SA);
- данные (INFO);
- контрольная сумма (Frame Check Sequence, PCS);
- конечный ограничитель (End Delimeter, ED);
- статус кадра (Frame Status, FS).

Кадр данных может переносить либо служебные данные для управления кольцом (данные MAC-уровня), либо пользовательские данные (LLC-уровня). Стандарт Token Ring определяет 6 типов управляющих кадров MAC-уровня. Поле FS определяет тип кадра (MAC или LLC), и если он определен как MAC, то поле также указывает, какой из шести типов кадров представлен данным кадром.

Прерывающая последовательность

Состоит из двух байтов, содержащих начальный и конечный ограничители. Прерывающая последовательность может появиться в любом месте потока битов и сигнализирует о том, что текущая передача кадра или маркера отменяется.

2.3.3. Реализация технологии Token Ring

Стандарт Token Ring фирмы IBM изначально предусматривал построение связей в сети с помощью концентраторов, называемых MSAU (Multi-Station Access Unit). Сеть Token Ring может включать до 260 узлов. Концентратор Token Ring может быть активным или пассивным.

Пассивный концентратор просто соединяет порты внутренними связями

так, чтобы станции, подключаемые к этим портам, образовали кольцо. Ни усиление сигналов, ни их ресинхронизацию пассивный MSAU не выполняет. Такое устройство можно считать простым кроссовым блоком за одним исключением – MSAU обеспечивает обход какого-либо порта, когда присоединенный к этому порту компьютер выключают. Такая функция необходима для обеспечения связности кольца вне зависимости от состояния подключенных компьютеров. Роль усилителя сигналов берет на себя каждый сетевой адаптер, а роль ресинхронизирующего блока выполняет сетевой адаптер активного монитора кольца.

Активный концентратор выполняет функции регенерации сигналов и поэтому иногда называется повторителем, как в стандарте Ethernet.

Все станции в кольце должны работать на одной скорости – либо 4 Мбит/с, либо 16 Мбит/с. Кабели, соединяющие станцию с концентратором, называются ответвительными (lobe cable), а кабели, соединяющие концентраторы, – магистральными (trunk cable). Технология Token Ring позволяет использовать для соединения конечных станций и концентраторов различные типы кабеля: STP Type 1, UTP Type 3, UTP Type 6, а также волоконно–оптический кабель. В таблице 2 приведены предельные характеристики сети Token Ring для двух наиболее распространенных типов кабеля.

Табл. 2

Тип кабеля	**Максимальное количество станций в кольце**	**Длина кабеля между рабочей станцией и MSAU (м)**	**Расстояние между пассивными MSAU (м)**	**Расстояние между активными MSAU (м)**
STP Type 1	260	100	100	730
UTP Type 3	72	45	45	365

Максимальная длина кольца Token Ring составляет 4000 м. Ограничения на максимальную длину кольца и количество станций в кольце в технологии Token Ring не являются жесткими, как в технологии Ethernet. Здесь эти ограничения во многом связаны со временем оборота маркера по кольцу. Если кольцо состоит из 260 станций, то при времени удержания маркера в 10 мс маркер вернется в активный монитор в худшем случае через 2,6 с, а это время как раз составляет

тайм-аут контроля оборота маркера. В принципе, все значения тайм-аутов в сетевых адаптерах узлов сети Token Ring можно настраивать, поэтому можно построить сеть Token Ring с большим количеством станций и с большей длиной кольца.

2.4. Технология FDDI

Технология FDDI (Fiber Distributed Data Interface) – оптоволоконный интерфейс распределенных данных – это первая технология локальных сетей, в которой средой передачи данных является волоконно-оптический кабель. Работы по созданию технологий и устройств для использования волоконно–оптических каналов в локальных сетях начались в 80-е годы, вскоре после начала промышленной эксплуатации подобных каналов в глобальных сетях.

Технология FDDI во многом основывается на технологии Token Ring, развивая и совершенствуя ее основные идеи. Сеть FDDI строится на основе двух оптоволоконных колец, которые образуют основной и резервный пути передачи данных между узлами сети. Наличие двух колец – это основной способ повышения отказоустойчивости в сети FDDI, и узлы, которые хотят воспользоваться этим повышенным потенциалом надежности, должны быть подключены к обоим кольцам. В нормальном режиме работы сети данные проходят через все узлы и все участки кабеля только первичного (Primary) кольца, этот режим называется режимом **Thru** – «сквозным» или «транзитным». Вторичное кольцо (Secondary) в этом режиме не используется. В случае какого–либо отказа, когда часть первичного кольца не может передавать данные (например, обрыв кабеля или отказ узла), первичное кольцо, объединяется со вторичным (рис. 2), вновь образуя единое кольцо.

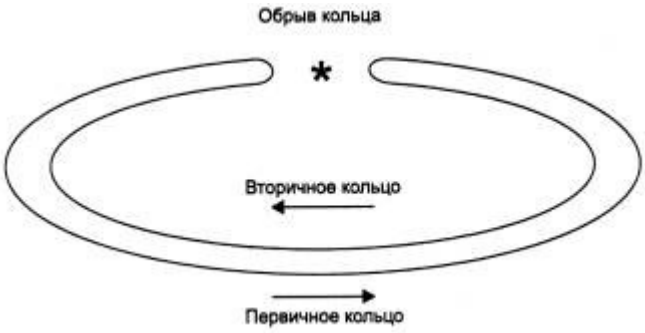

Рис. 2. Реконфигурация колец FDDI при отказе.

Этот режим работы сети называется **Wrap**, то есть «свертывание» или «сворачивание» колец. Операция свертывания производится средствами концентраторов и/или сетевых адаптеров FDDI. Для упрощения этой процедуры данные по первичному и вторичному кольцу всегда передаются в разных направлениях. Поэтому при образовании общего кольца из двух колец передатчики станций по-прежнему остаются подключенными к приемникам соседних станций, что позволяет правильно передавать и принимать информацию соседними станциями.

Кольца в сетях FDDI рассматриваются как общая среда передачи данных, и для нее задается метод доступа. Этот метод очень близок к методу доступа в сетях Token Ring и также называется методом маркерного кольца – token ring. Отличия метода доступа заключаются в том, что время удержания маркера в сети FDDI не является постоянной величиной, как в сети Token Ring. Это время зависит от загрузки кольца – при небольшой загрузке оно увеличивается, а при больших перегрузках может уменьшаться до нуля. Эти изменения в методе доступа касаются только асинхронного трафика, который не критичен к небольшим задержкам передачи кадров. Для синхронного трафика время удержания маркера по–прежнему остается фиксированной величиной. Механизм приоритетов кадров в технологии FDDI отсутствует. Разработчики технологии решили, что деление трафика на 8 уровней приоритетов избыточно и достаточно разделить трафик на два класса – асинхронный и синхронный, последний из которых обслуживается всегда, даже при перегрузках кольца. В остальном пересыл-

ка кадров между станциями кольца на уровне MAC полностью соответствует технологии Token Ring. Станции FDDI применяют алгоритм раннего освобождения маркера, как 16 Мегабитные сети Token Ring.

Формат кадра FDDI близок к формату кадра Token Ring, основные отличия заключаются в отсутствии полей приоритетов. Признаки распознавания адреса, копирования кадра и ошибки позволяют сохранить имеющиеся в сетях Token Ring процедуры обработки кадров станцией-отправителем, промежуточными станциями и станцией-получателем.

В технологии FDDI используется логическое кодирование 4B/5B в сочетании с физическим кодированием NRZI. Эта схема приводит к передаче по линии связи сигналов с тактовой частотой 125 МГц. Носителем информации является световой пучок с длиной волны 1300 нм. В качестве физической среды может использоваться многомодовый или одномодовый волоконно–оптический кабель. Для стандартного многомодового кабеля предельное расстояние между узлами составляет 2 км, а для одномодового кабеля расстояние увеличивается до 10–40 км в зависимости от качества кабеля. Максимальная общая длина кольца FDDI составляет 100 километров, максимальное число станций с двойным подключением в кольце – 500.

Вопросы для самостоятельной проработки.

1. Какие уровни модели OSI охватывают стандарты локальных компьютерных сетей.
2. Каковы функции уровней MAC и LLC.
3. Каков основной принцип технологии Ethernet.
4. Какие физические среды могут использоваться в классических вариантах технологии Ethernet для передачи данных.
5. Какое ограничение накладывает стандарт IEEE 802.3 на максимальное количество рабочих станций, объединенное локальной сетью.
6. Каков минимальный и максимальный размер кадра в сети Ethernet 10Base-

T

7. Какова минимальная единица информации, передаваемая рабочей станцией в сети Ethernet 10Base-5.
8. Что такое диаметр сети.
9. Какое правило существует в сетях Ethernet, использующих коаксиальный кабель.
10. Что такое сегмент сети.
11. На каком принципе основана работа сетей Token Ring.
12. На каких частотах работают сети Token Ring.
13. В чем различие между технологиями FDDI и FOIRL.
14. Какие физические среды используются для передачи данных в технологии Token Ring.

3. Современные технологии локальных сетей

3.1. Технология Fast Ethernet

В начале 90-х годов начала ощущаться недостаточная пропускная способность в сетях Ethernet. Скорость обработки данных в компьютерах возросла настолько, что сети Ethernet с пропускной способностью 10 Мбит/с стало явно недостаточно. Назрела необходимость в разработке «нового» Ethernet, то есть технологии, которая была бы такой же эффективной по соотношению цена/качество при производительности 100 Мбит/с. Осенью 1995 года комитет IEEE 802.3 принял спецификацию **Fast Ethernet** в качестве стандарта **802.3u**, который не является самостоятельным стандартом, а представляет собой дополнение к существующему стандарту IEEE 802.3.

3.1.1. Отличия от классического Ethernet

Все отличия технологии Fast Ethernet от Ethernet сосредоточены на физическом уровне. Канальный уровень с подуровнями MAC и LLC в Fast Ethernet не изменился. В технологии Fast Ethernet используются три варианта кабельных систем: волоконно-оптический кабель, витая пара 5 категории, витая пара 3 категории. Сети Fast Ethernet всегда имеют иерархическую древовидную структуру, построенную на концентраторах. Основным отличием конфигураций сетей Fast Ethernet от обычного Ethernet является сокращение диаметра сети примерно до 200 м, что объясняется уменьшением времени передачи кадра минимальной длины в 10 раз за счет увеличения скорости передачи. Это обстоятельство не препятствует построению крупных сетей с использованием технологии Fast Ethernet, если в этих сетях вместо концентраторов используются коммутаторы. При использовании коммутаторов протокол Fast Ethernet может работать в **полнодуплексном** режиме, в котором нет ограничений на общую длину сети, а

остаются только ограничения на длину физических сегментов, соединяющих соседние устройства (адаптер – коммутатор или коммутатор – коммутатор).

Стандарт 802.3u установил три спецификации для физического уровня Fast Ethernet:

- **100Base-TX** для двухпарного кабеля на неэкранированной витой паре UTP категории 5 или экранированной витой паре STP Type 1;
- **100Base-T4** для четырехпарного кабеля на неэкранированной витой паре UTP категории 3, 4 или 5;
- **100Base-FX** для многомодового оптоволоконного кабеля, используются два волокна.

Форматы кадров в технологии Fast Ethernet не изменились. Межкадровый интервал (IPG) равен 0,96 мкс, а битовый интервал равен 10 нс. Все временные параметры алгоритма доступа (интервал отсрочки, время передачи кадра минимальной длины и т. п.), измеренные в битовых интервалах, остались прежними, поэтому изменения в разделы стандарта, касающиеся уровня MAC, не вносились. Признаком свободного состояния среды является передача по ней специального сигнала Idle, а не отсутствие сигналов. Физический уровень включает три элемента:

- уровень согласования (reconciliation sublayer);
- независимый от среды интерфейс (Media Independent Interface, MII);
- устройство физического уровня (Physical layer device, PHY).

Уровень согласования нужен для того, чтобы уровень MAC, рассчитанный на интерфейс AUI, смог работать с физическим уровнем через интерфейс МП.

Устройство физического уровня (PHY) состоит, в свою очередь, из нескольких подуровней:

- подуровня логического кодирования данных, преобразующего поступающие от уровня MAC байты в символы кода 4B/5B или 8B/6T;
- подуровней физического присоединения и подуровня зависимости от физической среды (PMD), которые обеспечивают формирование сигналов в

соответствии с методом физического кодирования, например NRZI или MLT-3;

- подуровня автопереговоров, который позволяет двум взаимодействующим портам автоматически выбрать наиболее эффективный режим работы, например, полудуплексный или полнодуплексный.

Разъем MII в отличие от разъема AUI имеет 40 контактов, максимальная длина кабеля MII составляет один метр.

3.1.1.1 Fast Ethernet 100Base-FX

Эта спецификация определяет работу протокола Fast Ethernet по многомодовому оптоволокну в полудуплексном и полнодуплексном режимах на основе хорошо проверенной схемы кодирования FDDI. Каждый узел соединяется с сетью двумя оптическими волокнами, идущими от приемника (R_x) и от передатчика (T_x).

В стандарте Fast Ethernet определен метод кодирования – 4B/5B. Этот метод уже показал свою эффективность в стандарте FDDI и без изменений перенесен в спецификацию 100Base-FX/TX. При этом методе каждые 4 бита данных подуровня MAC (называемых символами) представляются 5 битами. Избыточный бит позволяет применить потенциальные коды при представлении каждого из пяти бит в виде электрических или оптических импульсов. Существование запрещенных комбинаций символов позволяет отбраковывать ошибочные символы, что повышает устойчивость работы сетей с 100Base-FX/TX.

Для отделения кадра Ethernet от символов Idle используется комбинация символов Start Delimiter (пара символов J (11000) и K (10001) кода 4B/5B, а после завершения кадра перед первым символом Idle вставляется символ T (рис. 3).

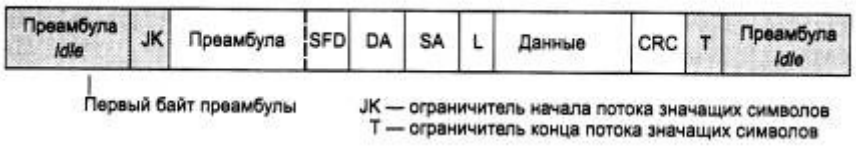

Рис. 3. Кадр данных и служебные сигналы спецификаций 100Base-FX/TX

После преобразования 4-битовых порций кодов MAC в 5-битовые порции физического уровня их необходимо представить в виде оптических или электрических сигналов в кабеле, соединяющем узлы сети. Для этого используется метод физического кодирования NRZI.

3.1.1.2. Fast Ethernet 100Base-TX и 100Base-T4

В качестве среды передачи данных спецификация 100Base-TX использует кабель UTP категории 5 или кабель STP Type 1. Максимальная длина кабеля в обоих случаях − 100 м. В отличие от спецификации 100Base-FX в Fast Ethernet 100Base-TX – используется метод MLT-3 для передачи сигналов 5-битовых порций кода 4B/5B по витой паре.

Спецификация 100Base-T4 была разработана для того, чтобы можно было использовать для высокоскоростного Ethernet существующую телефонную проводку на витой паре категории 3. Эта спецификация позволяет повысить общую пропускную способность за счет одновременной передачи потоков бит по 4 парам кабеля. Вместо кодирования 4B/5B в этом методе используется кодирование 8B/6T, которое обладает более узким спектром сигнала и при скорости 33 Мбит/с укладывается в полосу 16 МГц витой пары категории 3. Каждые 8 бит информации уровня MAC кодируются 6-ю троичными цифрами (ternary symbols), то есть цифрами, имеющими три состояния. Каждая троичная цифра имеет длительность 40 нс. Группа из 6-ти троичных цифр затем передается на одну из трех передающих витых пар, независимо и последовательно. Четвертая пара всегда используется для прослушивания несущей частоты в целях обнаружения коллизии. Скорость передачи данных по каждой из трех передающих пар равна 33,3 Мбит/с, поэтому общая скорость протокола 100Base-T4 составляет 100 Мбит/с. В то же время из-за принятого способа кодирования скорость изменения сигнала на каждой паре равна всего 25 Мбод, что и позволяет использо-

вать витую пару категории 3.

3.1.1.3. Функция Auto-negotiation

Схема автопереговоров позволяет двум соединенным физически устройствам, которые поддерживают несколько стандартов физического уровня, отличающихся битовой скоростью и количеством витых пар, выбрать наиболее выгодный режим работы. Обычно процедура автопереговоров происходит при подсоединении сетевого адаптера, который может работать на скоростях 10 и 100 Мбит/с, к концентратору или коммутатору. Всего определено 5 различных режимов работы, которые могут поддерживать устройства 100Base-TX или 100Base-T4 на витых парах:

1. 10Base-T - 2 пары категории 3;
2. 10Base-T full-duplex - 2 пары категории 3;
3. 100Base-TX - 2 пары категории 5 (или Type 1A STP);
4. 100Base-T4 - 4 пары категории 3;
5. 100Base-TX full-duplex - 2 пары категории 5 (или Type 1A STP).

Режим 10Base-T имеет самый низкий приоритет при переговорном процессе, а полнодуплексный режим 100Base-TX - самый высокий. Переговорный процесс происходит при включении питания устройства, а также может быть инициирован в любой момент модулем управления устройства. Устройство, начавшее процесс Auto-negotiation, посылает своему партнеру пачку специальных импульсов Fast Link Pulse burst (FLP), в которой содержится 8-битовое слово, кодирующее предлагаемый режим взаимодействия, начиная с самого приоритетного, поддерживаемого данным узлом. Если узел-партнер поддерживает функцию Auto-negotiation и также может поддерживать предложенный режим, он отвечает пачкой импульсов FLP, в которой подтверждает данный режим, и на этом переговоры заканчиваются. Если же узел-партнер может поддерживать менее приоритетный режим, то он указывает его в ответе, и этот режим выбирается в качестве рабочего. Таким образом, всегда выбирается наиболее приоритетный

общий режим узлов.

Узел, который поддерживает только технологию 10Base-T, каждые 16 мс посылает манчестерские импульсы для проверки целостности линии, связывающей его с соседним узлом. Такой узел не понимает запрос FLP, который делает ему узел с функцией Auto-negotiation, и продолжает посылать свои импульсы. Узел, получивший в ответ на запрос FLP только импульсы проверки целостности линии, понимает, что его партнер может работать только по стандарту 10Base-T, и устанавливает этот режим работы и для себя.

3.1.2. Правила построения сегментов Fast Ethernet при использовании повторителей

Технология Fast Ethernet рассчитана на использование концентраторов-повторителей для образования связей в сети. Правила корректного построения сегментов сетей Fast Ethernet включают ограничения на максимальные длины сегментов, соединяющих Data Terminal Equipment (DTE) с другим DTE (в качестве DTE может выступать любой источник кадров данных для сети): ограничения на максимальные длины сегментов, соединяющих DTE с портом повторителя; ограничения на максимальный диаметр сети; ограничения на максимальное число повторителей и максимальную длину сегмента, соединяющего повторители. Спецификация IEEE 802.3u определяет следующие максимальные длины сегментов DTE-DTE, приведенные в табл. 3.

Табл. 3.

Стандарт	Тип кабеля	Максимальная длина сегмента
100Base-TX	UTP-5	100 м
100Base-FX	Многомодовое оптоволокно	412 м полудуплекс, 2 км полный дуплекс
100Base-T4	UTP-5, 4 или 3	100 м

Повторители Fast Ethernet делятся на два класса. Повторители класса I поддерживают все типы логического кодирования данных: как 4B/5B, так и 8B/6T. По-

вторители класса II поддерживают только какой-либо один тип логического кодирования - либо 4B/5B, либо 8B/6T. То есть повторители класса I позволяют выполнять трансляцию логических кодов с битовой скоростью 100 Мбит/с, а повторителям класса II эта операция недоступна. Поэтому повторители класса I могут иметь порты всех трех типов физического уровня: 100Base-TX, 100Base-FX и 100Base-T4. Повторители класса II имеют либо все порты 100Base-T4, либо порты 100Base-TX и 100Base-FX, так как последние используют один логический код 4B/5B. В одном домене коллизий допускается наличие только одного повторителя класса I. Это связано с тем, что такой повторитель вносит задержку 70 bt при распространении сигналов из-за необходимости трансляции различных систем кодирования.

Повторители класса II вносят меньшую задержку при передаче сигналов: 46 bt для портов TX/FX и 33,5 bt для портов T4. Поэтому максимальное число повторителей класса II в домене коллизий - 2, причем они должны быть соединены между собой кабелем не длиннее 5 метров.

Небольшое количество повторителей Fast Ethernet не является препятствием при построении больших сетей, так как применение коммутаторов и маршрутизаторов делит сеть на несколько доменов коллизий, каждый из которых будет строиться на одном или двух повторителях. Общая длина сети не будет иметь в этом случае ограничений. В табл. 4. приведены правила построения сети на основе повторителей класса I.

Таким образом, правило 4-х хабов превратилось для технологии Fast Ethernet в правило одного или двух хабов, в зависимости от класса хаба. При определении корректности конфигурации сети можно не руководствоваться правилами одного или двух хабов, а выполнять расчет времени двойного оборота сигнала в сети. Время двойного оборота нужно сравнивать с величиной 512 битовых интервала (bt), то есть со временем передачи кадра минимальной длины без преамбулы.

Таблица 4.

Тип кабелей	Макимальный диаметр сети (метров)	Максимальная длина сегмента (метров)
Только витая пара (TX)	200	100
Только оптоволокно (FX)	272	136
Несколько сегментов на витой паре и один на оптоволокне	260	100 (TX) 160 (FX)
Несколько сегментов на витой паре и несколько сегментов на оптово-локне	272	100 (TX) 136(FX)

3.1.3. Работа коммутаторов в полудуплексном режиме

При работе в полудуплексном режиме коммутатор не может изменять протокол и пользоваться для управления потоком новыми командами, такими как «Приостановить передачу» и «Возобновить передачу». В этом случае управление осуществляется с помощью механизмов алгоритма доступа к среде, который конечный узел обязан отрабатывать. Эти приемы основаны на том, что конечные узлы строго соблюдают все параметры алгоритма доступа к среде, а порты коммутатора - нет. Обычно применяются два основных способа управления потоком кадров - обратное давление на конечный узел и агрессивный захват среды. **Метод обратного давления (backpressure)** состоит в создании искусственных коллизий в сегменте, который чересчур интенсивно посылает кадры в коммутатор. Для этого коммутатор использует jam-последовательность, отправляемую на выход порта, к которому подключен сегмент (или узел), чтобы приостановить его активность. Кроме того, метод обратного давления может применяться в тех случаях, когда процессор порта не рассчитан на поддержку максимально возможного для данного протокола трафика.

Второй метод «торможения» конечного узла в условиях перегрузки внутренних буферов коммутатора основан на так называемом **агрессивном поведении порта коммутатора**. В этом случае коммутатор начинает передачу нового

кадра не дожидаясь окончания технологической паузы в 9,6 мкс или паузы после коллизии в 51,2 мкс, как это положено по стандарту. Коммутатор может пользоваться этим механизмом избирательно, увеличивая степень своей агрессивности по мере необходимости. Практически во всех моделях коммутаторов, реализуют тот или иной алгоритм управления потоком кадров при полудуплексном режиме работы портов.

3.1.4. Работа коммутаторов в полнодуплексном режиме

Технология коммутации сама по себе не имеет непосредственного отношения к методу доступа к среде, который используется портами коммутатора. При подключении сегментов, представляющих собой разделяемую среду, порт коммутатора должен поддерживать полудуплексный режим, так как является одним из узлов этого сегмента. Однако, когда к каждому порту коммутатора подключен не сегмент, а только один компьютер, порт может работать как в обычном полудуплексном режиме, так и в полнодуплексном. Подключение к портам коммутатора не сегментов, а отдельных компьютеров называется **микросегментацией**. В полудуплексном режиме порт коммутатора по-прежнему распознает коллизии, Доменом коллизий в этом случае будет участок сети, включающий передатчик коммутатора, приемник коммутатора, передатчик сетевого адаптера компьютера, приемник сетевого адаптера компьютера и две витые пары, соединяющие передатчики с приемниками (рис. 4).

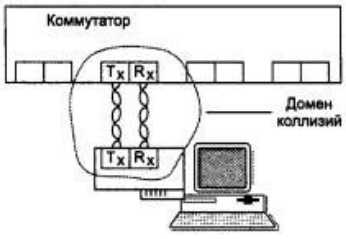

Рис. 4. Домен коллизий, образуемый компьютером и портом коммутатора

Коллизия возникает, когда передатчики порта коммутатора и сетевого адаптера одновременно начинают передачу своих кадров, считая, что изображенный на

рисунке сегмент свободен. Конечно, вероятность коллизии в таком сегменте гораздо меньше, чем в сегменте, состоящем из 20-30 узлов, но она не нулевая. При этом максимальная производительность сегмента Ethernet в 14 880 кадров в секунду при минимальной длине кадра делится между передатчиком порта коммутатора и передатчиком сетевого адаптера. Если считать, что она делится пополам, то каждому предоставляется возможность передавать примерно по 7440 кадров в секунду.

В полнодуплексном режиме одновременная передача данных передатчиком порта коммутатора и сетевого адаптера коллизией не считается. Это нормальный режим работы. Естественно, необходимо, чтобы MAC - узлы взаимодействующих устройств поддерживали этот специальный режим. Управление потоком данных в этом случае осуществляется специальными командами: «Приостановить передачу» и «Возобновить передачу». Команды управления передачей реализуются на уровне символов кодов физического уровня, таких как 4B/5B, а не на уровне команд, оформленных в специальные управляющие кадры. Сетевой адаптер или порт коммутатора, поддерживающий стандарт 802.3x и получивший команду «Приостановить передачу», должен прекратить передавать кадры впредь до получения команды «Возобновить передачу».

3.2. Технология Gigabit Ethernet и 10Gigabit Ethernet

3.2.1. Gigabit Ethernet

Достаточно быстро после появления на рынке продуктов Fast Ethernet сетевые интеграторы и администраторы почувствовали недостаточность скорости, предоставляемой технологией Fast Ethernet при построении магистральных линий корпоративных сетей. За основу первого варианта Gigabit Ethernet на оптоволоконном кабеле (стандарт **IEEE 802.3z**) был принята технология Fiber Channel, с ее кодом 8B/10B.

Первая версия стандарта была рассмотрена в январе 1997 года, а оконча-

тельно он был принят в 1998 году. Стандарт Gigabit Ethernet на витой паре (**IEEE 802.3ab**) был принят в 1999 году. Разработчики стандарта Gigabit Ethernet постарались максимально сохранить принципы классической технологии Ethernet при достижении битовой скорости в 1000 Мбит/с:

1. Сохранены форматы кадров Ethernet.
2. По-прежнему существует полудуплексная версия протокола, поддерживающая метод доступа CSMA/CD, и полнодуплексная версия, работающая с коммутаторами.
3. Поддерживаются волоконно-оптический кабель и витая пара категории 5.

Однако, на этот раз изменения пришлось внести не только в физический уровень, но и в уровень MAC.

Для расширения максимального диаметра сети Gigabit Ethernet в полудуплексном режиме до 200 м разработчики технологии предприняли достаточно естественные меры, основывающиеся на известном соотношения времени передачи кадра минимальной длины и временем двойного оборота. Минимальный размер кадра был увеличен (без учета преамбулы) с 64 до 512 байт или до 4096 bt. Для увеличения длины кадра до требуемой величины сетевой адаптер дополняет поле данных до длины 448 байт так называемым **расширением** (extention), представляющим собой поле, заполненное запрещенными символами кода 8B/10B, которые невозможно принять за коды данных. Для сокращения накладных расходов при использовании слишком длинных кадров для передачи коротких квитанций разработчики стандарта разрешили конечным узлам передавать несколько кадров подряд, без передачи среды другим станциям. Такой режим получил название **Burst Mode** – монопольный пакетный режим. Станция может передать подряд несколько кадров с общей длиной не более 65 536 бит или 8192 байт. Если станции нужно передать несколько небольших кадров, то она может не дополнять их до размера в 512 байт, а передавать подряд до исчерпания предела в 8192 байт (в этот предел входят все байты кадра, в том числе преамбула, заголовок, данные и контрольная сумма). Предел 8192 байт называ-

ется **BurstLength**. Если станция начала передавать кадр и предел BurstLength был достигнут в середине кадра, то кадр разрешается передать до конца.

В стандарте Gigabit Ethernet определены три типа физической среды:

- одномодовый волоконно-оптический кабель;
- многомодовый волоконно-оптический кабель;
- витая пара категории 5.

3.2.1.1. Спецификации Gigabit Ethernet 1000Base-SX и 1000Base-LX

Для передачи данных по многомодовому волоконно-оптическому кабелю стандарт определяет применение излучателей, работающих на двух длинах волн: 1300 и 850 нм. В соответствии с этим в стандарте 802.3z определены спецификации 1000Base-SX и 1000Base-LX. В первом случае используется длина волны 850 нм (S означает Short Wavelength, короткая волна) и могут применяться как лазерные источники излучения, так и светодиодные. Во втором длина волны составляет 1300 нм (L - от Long Wavelength, длинная волна), используются только лазерные излучатели. Для спецификации 1000Base-SX предельная длина оптоволоконного сегмента для кабеля 62,5/125 оставляет 220 м, а для кабеля 50/125 – 500 м. Очевидно, что эти максимальные значения могут достигаться только для полнодуплексной передачи данных, так как время двойного оборота сигнала на двух отрезках 220 м равно 4400 bt, что превосходит предел 4095 bt даже без учета повторителя и сетевых адаптеров. Для полудуплексной передачи максимальные значения сегментов оптоволоконного кабеля всегда должны быть меньше 100 м.

Основная область применения стандарта 1000Base-LX - это одномодовое оптоволокно. Максимальная длина кабеля для одномодового волокна равна 5000 м. Спецификация 1000Base-LX может работать и на многомодовом кабеле. В этом случае предельное расстояние получается небольшим — 550 м. Это связано с особенностями распространения когерентного света в широком канале многомодового кабеля. Для присоединения лазерного трансивера к многомодо-

вому кабелю необходимо использовать специальный адаптер.

3.2.1.2. Спецификация Gigabit Ethernet 1000Base-T

Витая пара 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 4 парам кабеля. Для кодирования данных был применен код PAM5, использующий 5 уровней потенциала: -2, -1, 0, +1, +2. Поэтому за один такт по одной паре передается 2,322 бит информации. При этом тактовая частота снижается с 250 МГц до 125 МГц. Если использовать не все коды, а передавать 8 бит за такт (по 4 парам), то выдерживается требуемая скорость передачи в 1000 Мбит/с и еще остается запас неиспользуемых кодов, так как код PAM5 содержит $5^4 = 625$ комбинаций, а если передавать за один такт по всем четырем парам 8 бит данных, то для этого требуется всего $2^8 = 256$ комбинаций. Оставшиеся комбинации приемник может использовать для контроля принимаемой информации и выделения правильных комбинаций на фоне шума. Код PAM5 на тактовой частоте 125 МГц укладывается в полосу 100 МГц кабеля категории 5.

Для распознавания коллизий и организации полнодуплексного режима применяется техника, используемая 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 передатчиков по диапазону частот оба передатчика работают навстречу друг другу по каждой из 4-х пар в одном и том же диапазоне частот, так как используют один и тот же потенциальный код PAM5 (рис. 5). Схема гибридной развязки **H** позволяет приемнику и передатчику одного и того же узла использовать одновременно витую пару и для приема и для передачи.

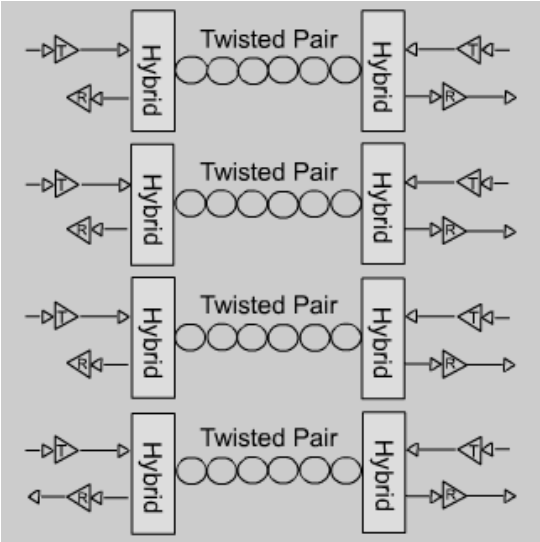

Рис. 5. Двунаправленная передача по четырем парам UTP категории 5

Для отделения принимаемого сигнала от своего собственного 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). При полудуплексном режиме работы получение встречного потока данных считается коллизией, а для полнодуплексного режима работы – нормальной ситуацией.

3.2.2. 10Gigabit Ethernet

В 2002г. был принят стандарт **IEEE 802.3ae**, в котором установлена новая ступень скорости передачи данных. В качестве физической среды передачи данных предусмотрено использование только оптоволокна (многомодового и одномодового). Полудуплексный режим передачи данных не используется, применяется только полнодуплексный режим. Новый стандарт предназначен для работы на высокоскоростных магистральных каналах.

3.3. 100VG – AnyLAN

Технология 100VG-AnyLAN была предложена как альтернатива Ethernet компаниями Hewlett-Packard и AT&T, которые решили воспользоваться удобным случаем для устранения некоторых известных недостатков технологии Eth-

ernet. Разработчиками этой технологии был предложен совершенно новый метод доступа, названный **Demand Priority** – приоритетный доступ. Он существенно менял картину поведения узлов в сети, поэтому не смог вписаться в технологию Ethernet и для его стандартизации был организован новый комитет **IEEE 802.12**. Комитет 802.12 принял соответствующий стандарт. Технология 100VG-AnyLAN использует кадры двух форматов - Ethernet и Token Ring. Главные отличия 100VG-AnyLAN от Ethernet:

- Используется метод доступа Demand Priority, который обеспечивает более справедливое распределение пропускной способности сети по сравнению с методом CSMA/CD, кроме того, этот метод поддерживает приоритетный доступ для синхронных приложений.
- Кадры передаются не всем станциям сети, а только станции назначения.
- В сети есть выделенный арбитр доступа - концентратор, и это заметно отличает данную технологию от других, в которых применяется распределенный между станциями сети алгоритм доступа.
- Поддерживаются кадры двух технологий - Ethernet и Token Ring (именно это обстоятельство дало добавку AnyLAN в названии технологии).
- Данные передаются одновременно по 4 парам кабеля UTP категории 3. По каждой паре данные передаются со скоростью 25 Мбит/с, что в сумме дает 100 Мбит/с. Поскольку в сетях 100VG-AnyLAN нет коллизий, удалось использовать для передачи стандартный кабель категории 3. Для кодирования данных применяется код 5B/6B, который обеспечивает спектр сигнала в диапазоне до 16 МГц (полоса пропускания UTP категории 3) при скорости передачи данных 25 Мбит/с. Сеть 100VG-AnyLAN состоит из центрального концентратора, называемого также корневым, и соединенных с ним конечных узлов и других концентраторов (рис. 6).

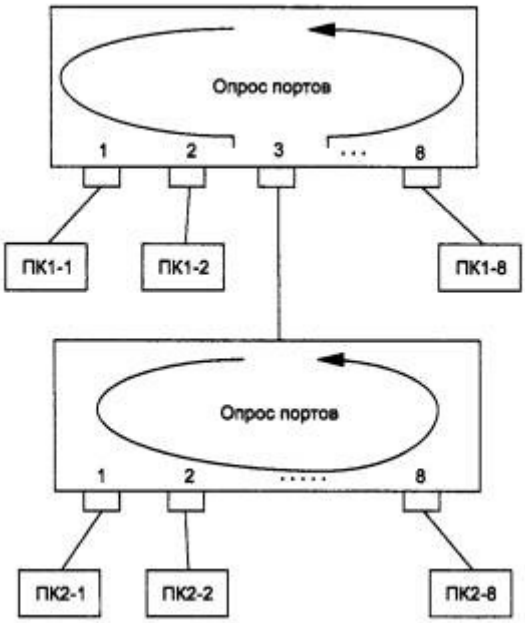

Рис. 6. Сеть 100VG-AnyLAN

Допускаются три уровня иерархии. Каждый концентратор и сетевой адаптер 100VG-AnyLAN настраивается либо на работу с кадрами Ethernet, либо с кадрами Token Ring, одновременная циркуляция обоих типов кадров не допускается.

Концентратор циклически выполняет опрос портов. Станция, желающая передать пакет, посылает специальный низкочастотный сигнал концентратору, запрашивая передачу кадра и указывая его приоритет. В сети 100VG-AnyLAN используются два уровня приоритетов – низкий и высокий. Низкий уровень приоритета соответствует обычным данным, а высокий приоритет соответствует данным, чувствительным к временным задержкам (например, мультимедиа). Приоритеты запросов имеют статическую и динамическую составляющие, то есть станция с низким уровнем приоритета, долго не имеющая доступа к сети, получает высокий приоритет.

Если сеть свободна, то концентратор разрешает передачу пакета. После анализа адреса получателя в принятом пакете концентратор автоматически отправляет пакет станции назначения. Если сеть занята, концентратор ставит полученный запрос в очередь, которая обрабатывается в соответствии с порядком поступления запросов и с учетом приоритетов. Если к порту подключен другой

концентратор, то опрос приостанавливается до завершения опроса концентратором нижнего уровня. Станции, подключенные к концентраторам различного уровня иерархии, не имеют преимуществ по доступу к разделяемой среде, так как решение о предоставлении доступа принимается после проведения опроса всеми концентраторами всех своих портов.

Для определения порта, на который необходимо отправить кадр для определенной станции назначения, концентратор в момент физического присоединения станции к сети определяет ее MAC-адрес и запоминает его в таблице MAC-адресов, аналогичной таблице моста/коммутатора. В отличие от моста/коммутатора у концентратора 100VG-AnyLAN нет внутреннего буфера для хранения кадров. Поэтому он принимает от станций сети только один кадр, отправляет его на порт назначения и, пока этот кадр не будет принят станцией назначения, новые кадры концентратор не принимает. Так что эффект разделяемой среды сохраняется. Улучшается только безопасность сети - кадры не попадают на чужие порты, и их труднее перехватить.

Технология 100VG-AnyLAN поддерживает несколько спецификаций физического уровня. Первоначальный вариант был рассчитан на четыре неэкранированные витые пары категорий 3, 4, 5. Позже появились варианты физического уровня, рассчитанные на две неэкранированные витые пары категории 5, две экранированные витые пары типа 1 или же два оптических многомодовых оптоволокна.

Несмотря на большое число удачных технических решений, технология 100VG-AnyLAN значительно уступает по популярности технологии Fast Ethernet.

3.4. Технология ATM

Технология **асинхронного режима передачи** (Asynchronous Transfer Mode, ATM) была разработана крупными телефонными компаниями как единый универсальный транспорт для нового поколения телефонных сетей с инте-

грацией услуг в 1993 году. Такие телефонные сети называются широкополосными сетями ISDN (Broadband-ISDN, B-ISDN). С помощью техники виртуальных каналов в технологии ATM удается добиться эффективной передачи в одной сети разных типов трафика.

3.4.1. Принципы технологии ATM

Коммутаторы ATM пользуются 20-байтными адресами конечных узлов для маршрутизации трафика на основе техники виртуальных каналов. Для частных сетей ATM определен протокол маршрутизации PNNI (Private NNI), с помощью которого коммутаторы могут строить таблицы маршрутизации автоматически. В публичных сетях ATM таблицы маршрутизации могут строиться администраторами вручную или могут поддерживаться протоколом PNNI.

Коммутация пакетов происходит на основе идентификатора виртуального канала (Virtual Channel Identifier, VCI), который назначается соединению при его установлении и уничтожается при разрыве соединения. Адрес конечного узла ATM, на основе которого прокладывается виртуальный канал, имеет иерархическую структуру, подобную номеру в телефонной сети, и использует префиксы, соответствующие кодам стран, городов, сетям поставщиков услуг и т. п., что упрощает маршрутизацию запросов установления соединения. Виртуальные соединения могут быть постоянными (Permanent Virtual Circuit, PVC) и коммутируемыми (Switched Virtual Circuit, SVC). Для ускорения коммутации в больших сетях используется понятие виртуального пути – Virtual Path, который объединяет виртуальные каналы, имеющие в сети ATM общий маршрут между исходным и конечным узлами или общую часть маршрута между некоторыми двумя коммутаторами сети. Идентификатор виртуального пути (Virtual Path Identifier, VPI) является старшей частью локального адреса и представляет собой общий префикс для некоторого количества различных виртуальных каналов. Таким образом, идея агрегирования адресов в технологии ATM применена

на двух уровнях – на уровне адресов конечных узлов (работает на стадии установления виртуального канала) и на уровне номеров виртуальных каналов (работает при передаче данных по имеющемуся виртуальному каналу).

Соединения конечной станции ATM с коммутатором нижнего уровня определяются стандартом UNI (User Network Interface). Спецификация UNI определяет структуру пакета, адресацию станций, обмен управляющей информацией, уровни протокола ATM, способы установления виртуального канала и способы управления трафиком.

В технологии ATM используются две скорости передачи данных: OC-3 (155 Мбит/с) и OC-12 (622 Мбит/с). На скорости 155 Мбит/с можно использовать не только волоконно-оптический кабель, но и неэкранированную витую пару категории 5. На скорости 622 Мбит/с допустим только волоконно-оптический кабель (одномодовый или многомодовый).

Подход, реализованный в технологии ATM, состоит в передаче любого вида трафика - компьютерного, телефонного или видео - пакетами фиксированной и очень маленькой длины в 53 байта. Пакеты ATM называют ячейками - **cell**. Поле данных ячейки занимает 48 байт, а заголовок - 5 байт. Чтобы пакеты содержали адрес узла назначения и в то же время процент служебной информации не превышал размер поля данных пакета, в технологии ATM применен стандартный для глобальных вычислительных сетей прием - передача ячеек в соответствии с техникой виртуальных каналов с длиной номера виртуального канала в 24 бит, что вполне достаточно для обслуживания большого количества виртуальных соединений каждым портом коммутатора глобальной (может быть всемирной) сети ATM. Чем меньше пакет, тем легче имитировать услуги каналов с постоянной битовой скоростью, которая характерна для телефонных сетей.

В технологии ATM определено пять классов трафика, отличающихся: наличием или отсутствием пульсации, требованием к синхронизации данных, типом протокола (с установлением или без установления соединения).

Основные характеристики классов трафика ATM приведены в табл. 5.

Таблица 5. Классы трафика ATM

Класс трафика	Характеристика
A	Постоянная битовая скорость (Constant Bit Rate, CBR). Требуется сохранение временных соотношений между передаваемыми и принимаемими данными. С установлением соединения. Например, видеоизображение, передача голоса
B	Переменная битовая скорость (Variable Bit Rate, VBR). Требуется сохранение временных соотношений между передаваемыми и принимаемими данными. С установлением соединения. Например, сжатое видеоизображение.
C	Переменная битовая скорость (Variable Bit Rate, VBR). Не требуется сохранение временных соотношений между передаваемыми и принимаемими данными. С установлением соединения. Например, компьютерный трафик, когда конечные узлы работают в режиме установления соединения
D	Переменная битовая скорость (Variable Bit Rate, VBR). Не требуется сохранение временных соотношений между передаваемыми и принимаемими данными. Без установления соединения. Например, компьютерный трафик, когда конечные узлы работают в режиме без установления соединения.
X	Тип трафика и его параметры задаются пользователем

Для каждого класса трафика определен набор параметров, которые приложение должно задать. Например, для трафика класса A необходимо указать постоянную скорость, с которой приложение будет посылать данные в сеть, а для трафика класса B – максимально возможную скорость, среднюю скорость и максимально возможную пульсацию. Для голосового трафика можно не только указать на важность синхронизации между передатчиком и приемником, но и количественно задать верхние границы задержки и вариации задержки ячеек.

Поддерживается следующий набор основных количественных параметров:

- Peak Cell Rate (PCR) – максимальная скорость передачи данных;
- Sustained Cell Rate (SCR) – средняя скорость передачи данных;
- Minimum Cell Rate (MCR) – минимальная скорость передачи данных;
- Maximum Burst Size (MBS) – максимальный размер пульсации;
- Cell Loss Ratio (CLR) – доля потерянных ячеек;
- Cell Transfer Delay (CTD) – задержка передачи ячеек;
- Cell Delay Variation (CDV) – вариация задержки ячеек.

Параметры скорости измеряются в ячейках в секунду, максимальный размер пульсации – в ячейках, а временные параметры – в секундах. Максимальный размер пульсации задает количество ячеек, которое приложение может передать с максимальной скоростью PCR, если задана средняя скорость. Доля потерянных ячеек является отношением потерянных ячеек к общему количеству отправленных ячеек по данному виртуальному соединению. Так как виртуальные соединения являются дуплексными, то для каждого направления соединения могут быть заданы разные значения параметров.

3.4.1.1. Уровень адаптации AAL

Уровень адаптации (ATM Adaptation Layer, AAL) представляет собой набор протоколов AAL1-AAL5, которые преобразуют сообщения протоколов верхних уровней сети ATM в ячейки ATM нужного формата. Функции этих уровней достаточно условно соответствуют функциям транспортного уровня модели OSI, например функциям протоколов TCP или UDP. Протоколы AAL при передаче пользовательского трафика работают только в конечных узлах сети. Каждый протокол уровня AAL обрабатывает пользовательский трафик определенного класса.

Уровень адаптации состоит из нескольких подуровней.

Нижний подуровень AAL называется **подуровнем сегментации и реассемблирования** (Segmentation And Reassembly, SAR). Эта часть не зависит от

типа протокола AAL (и, соответственно, от класса передаваемого трафика) и занимается разбиением (сегментацией) сообщения, принимаемого AAL or протокола верхнего уровня, на ячейки ATM, снабжением их соответствующим заголовком и передачей уровню ATM для отправки в сеть.

Верхний подуровень AAL называется **подуровнем конвергенции** - Convergence Sublayer, CS. Этот подуровень зависит от класса передаваемого трафика. Протокол подуровня конвергенции решает такие задачи, как, например, обеспечение временной синхронизации между передающим и принимающим узлами (для трафика, требующего такой синхронизации), контролем и возможным восстановлением битовых ошибок в пользовательской информации, контролем целостности передаваемого пакета.

Протоколы AAL для выполнения своей работы используют служебную информацию, размещаемую в заголовках уровня AAL. После приема ячеек, пришедших по виртуальному каналу, подуровень SAR протокола AAL собирает посланное по сети исходное сообщение (которое в общем случае было разбито на несколько ячеек ATM) с помощью заголовков AAL. После сборки исходного сообщения протокол AAL проверяет служебные поля заголовка и концевика кадра AAL и на их основании принимает решение о корректности полученной информации. Протоколы AAL не занимаются восстановлением потерянных или искаженных данных. Восстановление потерянных данных (или игнорирование этого события) отводится протоколам верхних уровней, не входящим в стек протоколов технологии ATM.

Протокол AAL1 обычно обслуживает трафик класса A с постоянной битовой скоростью (Constant Bit Rate, CBR), который характерен, например, для цифрового видео и цифровой речи и чувствителен к временным задержкам.

Протокол AAL3/4 обрабатывает пульсирующий трафик (класс B) - обычно характерный для локальных сетей - с переменной битовой скоростью (Variable Bit Rate, VBR). Этот протокол выполняет процедуру контроля ошибок при передаче ячеек, нумеруя каждую составляющую часть исходного сообщения и

снабжая каждую ячейку контрольной суммой. При искажениях или потерях ячеек все сообщение отбрасывается и запрашивается его повторная передача.
Протокол AAL5 вычисляет контрольную сумму не для каждой ячейки сообщения, а для всего исходного сообщения в целом. Этот протокол может поддерживать различные параметры качества обслуживания, кроме тех, которые связаны с синхронизацией передающей и принимающей сторон. Поэтому он обычно используется для поддержки всех классов трафика, относящегося к передаче компьютерных данных, то есть классов C и D.

Приложение на локальном компьютере, используя уровень AAL, заказывает необходимые параметры передачи трафика. Технология ATM допускает два варианта определения параметров QoS:

- непосредственное задание их каждым приложением;
- назначение их по умолчанию в зависимости от типа трафика.

Самостоятельно обеспечить требуемые параметры трафика и QoS протоколы AAL не могут. Для выполнения соглашений трафик - контракта требуется согласованная работа коммутаторов сети вдоль всего виртуального соединения. Эта работа выполняется протоколом ATM, обеспечивающим передачу ячеек различных виртуальных соединений с заданным уровнем качества обслуживания.

3.4.2. Технология ATM и традиционные технологии локальных сетей

Технология ATM разрабатывалась обособленно и для ее использования необходим полный отказ от использования существующего сетевого оборудования, замена его на новое. В глобальных сетях, где стоимость высокоскоростных оптоволоконных каналов, проложенных на большие расстояния, намного превышает стоимость сетевого оборудования, переход на новую технологию, дающую большую гибкость управления трафиком, во многих случаях оказывается экономически оправданным. Для локальных сетей, в которых замена коммутаторов и сетевых адаптеров равнозначна созданию новой сети, переход на техно-

логию ATM зачастую был совершенно неприемлем, несмотря на ее преимущества. Для обеспечения совместимости традиционных протоколов и оборудования локальных сетей с технологией ATM была разработана спецификация LAN emulation, **LANE** (то есть эмуляция локальных сетей). Спецификация LANE определяет способ преобразования кадров и адресов MAC - уровня традиционных технологий локальных сетей в ячейки и коммутируемые виртуальные соединения SVC технологии ATM, а также способ обратного преобразования. Всю работу по преобразованию протоколов выполняют специальные компоненты, встраиваемые в обычные коммутаторы локальных сетей, поэтому ни коммутаторы ATM, ни рабочие станции локальных сетей не замечают того, что они работают с чуждыми им технологиями.

Спецификация LANE определяет только канальный уровень взаимодействия, поэтому с помощью коммутаторов ATM и компонентов LANE можно образовать только виртуальные сети, называемые здесь эмулируемыми сетями, а для их соединения нужно использовать обычные маршрутизаторы.

Рассмотрим основные идеи спецификации на примере сети, изображенной на рис. 7. Основными элементами LANE являются программные компоненты LEC (LAN Emulation Client) и LES (LAN Emulation Server). Клиент LEC выполняет роль пограничного элемента, работающего между сетью ATM и станциями локальной сети. На каждую присоединенную к сети ATM локальную сеть приходится один клиент LEC. Сервер LES ведет общую таблицу соответствия MAC-адресов станций локальных сетей и ATM-адресов пограничных устройств с установленными на них компонентами LEC, к которым присоединены локальные сети, содержащие эти станции.

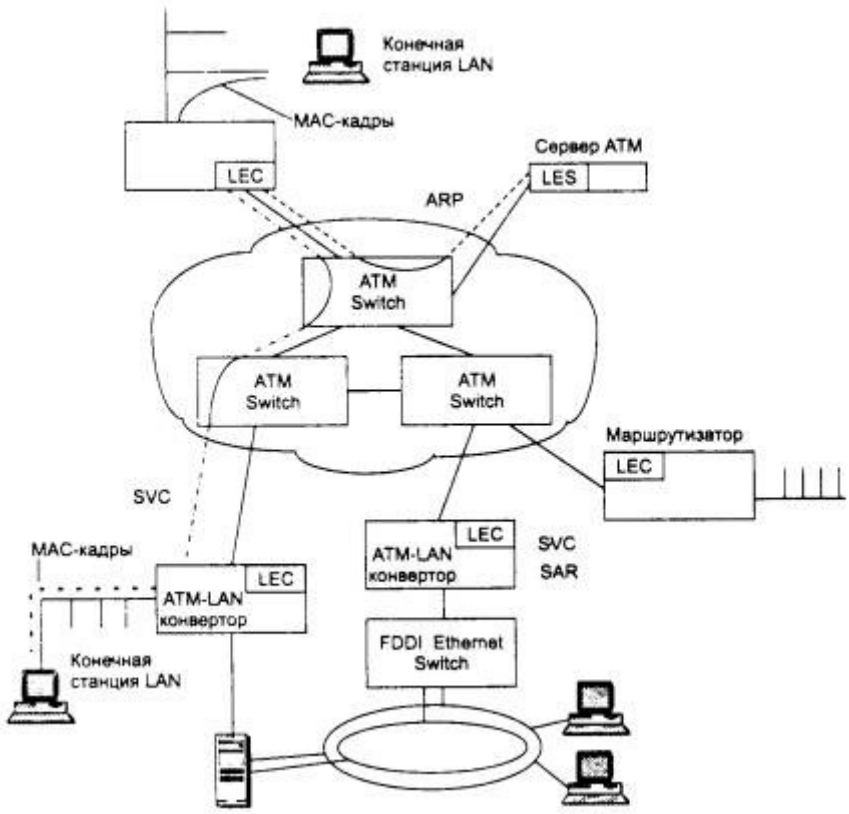

Рис. 7. Принципы работы технологии LANE

Таким образом, для каждой присоединенной локальной сети сервер LES хранит один ATM-адрес пограничного устройства LEC и несколько MAC-адресов станций, входящих в эту сеть. Клиентские части LEC динамически регистрируют в сервере LES MAC-адреса каждой станции, заново подключаемой к присоединенной локальной сети.

Программные компоненты LEC и LES могут быть реализованы в любых устройствах – коммутаторах, маршрутизаторах или рабочих станциях ATM. Когда элемент LEC хочет послать пакет через сеть ATM станции другой локальной сети, также присоединенной к сети ATM, он посылает запрос на установление соответствия между MAC-адресом и ATM-адресом серверу LES. Сервер LES отвечает на запрос, указывая ATM-адрес пограничного устройства LEC, к которому присоединена сеть, содержащая станцию назначения. Зная ATM-адрес, устройство LEC исходной сети самостоятельно устанавливает виртуальное соединение SVC через сеть ATM обычным способом, описанным в спецификации UNI. После установления связи кадры MAC локальной сети преобразуются

в ячейки ATM каждым элементом LEC с помощью стандартных функций сборки-разборки пакетов (функции SAR) стека ATM. В спецификации LANE также определен сервер для эмуляции в сети ATM широковещательных пакетов локальных сетей, а также пакетов с неизвестными адресами, так называемый сервер BUS (Broadcast and Unknown Server). Этот сервер распространяет такие пакеты во все пограничные коммутаторы, присоединившие свои сети к эмулируемой сети. Если необходимо образовать несколько эмулируемых сетей, не взаимодействующих прямо между собой, то для каждой такой сети необходимо активизировать собственные серверы LES и BUS, а в пограничных коммутаторах активизировать по одному элементу LEC для каждой эмулируемой сети. Для хранения информации о количестве активизированных эмулируемых сетей, а также ATM-адресах соответствующих серверов LES и BUS вводится еще один сервер – сервер конфигурации LECS (LAN Emulation Configuration Server).

Основной соперник технологии ATM в локальных сетях – технология Gigabit Ethernet. Она превосходит ATM в скорости передачи данных – 1000 Мбит/с по сравнению с 622 Мбит/с, а также в затратах на единицу скорости. Поэтому технология ATM используется только в том случае, когда важно качество обслуживания (видеоконференции, трансляция телевизионных передач и т. п.).

Вопросы для самостоятельной проработки

1. В чем преимущества технологии ATM перед технологиями Fast и Gigabit Ehternet.
2. Что такое микросегментация.
3. Каков максимальный диаметр сети при использовании технологии Fast Ethernet на медном кабеле.
4. Какой стандарт определяет технологию Fast Ethernet.
5. Какова максимальная скорость передачи данных в сетях с технологией Ethernet, как называется этот вариант технологии, назовите номер стан-

дарта и физические среды, используемые для передачи данных.

6. Какую задачу решает спецификация LANE в технологии ATM.
7. Какой способ кодирования используется в технологии Gigabit Ethernet, реализованной на медном кабеле. Разрешен ли в этой технологии полудуплексный режим работы узлов сети.
8. В чем суть метода приоритетного доступа, в какой технологии он реализован, назовите номер стандарта, описывающего эту технологию.

4. Проектирование локальных сетей

Сложность задачи разработки проекта вновь создаваемой или реконструкции существующей локальной сети зависит в первую очередь от размера и количества конечных станций в этой сети. Если небольшие локальные сети могут быть полностью спроектированы одним человеком, то для крупных сетей, объединяющих сотни пользователей, задача проектирования обычно разделяется между несколькими разработчиками, каждый из которых отвечает за определенную часть работы.

Основой локальных сетей являются кабельные линии связи. Поэтому правильное проектирование кабельной системы компьютерной сети во многом определяет эффективность ее работы в целом. Построение кабельной системы имеет общие принципы, но выбор конкретного типа кабеля тесно связан с выбором сетевой технологии, которая будет использоваться в локальной сети. В том случае, когда выполняется реконструкция локальной сети, выбор сетевой технологии часто зависит не только от задач, которые будет решать сеть, но и от ранее используемых технологии и оборудования.

Кабельная система является фундаментом построения локальной сети, но не меньшее влияние на качество работы сетевых приложений и скорость обработки запросов оказывает грамотная логическая структуризация сети. Логическое проектирование определяет места расположения ресурсов, приложений и способы группировки этих ресурсов в логические сегменты.

Выбор сетевого оборудования и программного обеспечения, которые в совокупности и обеспечат выполнение сетью возложенных на нее задач, обычно выполняется на завершающем этапе, хотя и неразрывно связан с этапом логического проектирования сети.

4.1. Проектирование кабельной системы

Локальная компьютерная сеть должна строится на основе структуриро-

ванной кабельной системы (Structured Cabling System, SCS). Такой подход позволяет создавать в сети регулярные, легко расширяемые структуры связей. При построении структурированной кабельной системы подразумевается ее избыточность, например, каждое рабочее место оснащается розетками для подключения телефона и компьютера, даже если в данный момент этого не требуется. В будущем это может сэкономить средства, так как изменения в подключении новых устройств можно производить за счет перекоммутации уже проложенных кабелей.

Структурированная кабельная система планируется и строится иерархически, с главной магистралью и ответвлениями от нее. Типичная иерархическая структура структурированной кабельной системы включает:

- горизонтальные подсистемы (в пределах этажа);
- вертикальные подсистемы (внутри здания);
- главная магистраль(backbone) (соединяет здания).

Большинство проектировщиков начинает разработку структурированной кабельной системы с горизонтальных подсистем, так как именно к ним подключаются конечные пользователи. При этом они могут выбирать между экранированной витой парой, неэкранированной витой парой, коаксиальным кабелем и волоконно-оптическим кабелем. Возможно использование и беспроводных линий связи. Горизонтальная подсистема характеризуется большим количеством ответвлений кабеля, так как его нужно провести к каждой пользовательской розетке. Поэтому к кабелю, используемому в горизонтальной проводке, предъявляются повышенные требования к удобству выполнения ответвлений, а также удобству его прокладки в помещениях. На этаже обычно устанавливается кроссовая панель, которая позволяет с помощью коротких отрезков кабеля, оснащенного разъемами, провести перекоммутацию соединений между пользовательским оборудованием и концентраторами/коммутаторами.

Медный провод, в частности неэкранированная витая пара, является предпочтительной средой для горизонтальной кабельной подсистемы, хотя,

если пользователям нужна очень высокая пропускная способность или кабельная система прокладывается в агрессивной среде, лучшим выбором для нее будет волоконно-оптический кабель. Коаксиальный кабель – это устаревшая технология, которой следует избегать.

Кабель вертикальной (или магистральной) подсистемы, которая соединяет этажи здания, должен передавать данные на большие расстояния и с большей скоростью по сравнению с кабелем горизонтальной подсистемы. В прошлом основным видом кабеля для вертикальных подсистем был толстый коаксиальный кабель. Теперь для этой цели чаще всего используется оптоволоконный кабель.

Применение оптоволоконного кабеля в вертикальной подсистеме имеет ряд преимуществ. Он передает данные на значительно большие расстояния без необходимости регенерации сигнала, имеет сердечник меньшего диаметра, поэтому может быть проложен в более узких местах. Так как передаваемые по нему сигналы являются световыми, а не электрическими, оптоволоконный кабель не чувствителен к электромагнитным и радиочастотным помехам. Это делает оптоволоконный кабель идеальной средой передачи данных для промышленных сетей. Оптоволоконному кабелю не страшна молния, поэтому он хорош и для внешней прокладки. Он обеспечивает более высокую степень защиты от несанкционированного доступа, так как ответвление гораздо легче обнаружить, чем в случае медного кабеля (при ответвлении резко уменьшается интенсивность света). Недостатками оптоволоконного кабеля являются его высокая цена, большая стоимость прокладки и меньшая прочность. Инструменты, применяемые при прокладке и тестировании оптоволоконного кабеля, также имеют высокую стоимость, для работы с ними необходим высококвалифицированный персонал.

4.2. Проектирование логической структуры сети

При построении небольших сетей, состоящих из 10-30 узлов, использова-

ние стандартных технологий на разделяемых средах передачи данных приводит к экономичным и эффективным решениям. Однако крупные сети, насчитывающие сотни и тысячи узлов, плохо работают на одной разделяемой среде. Основные недостатки сети на одной разделяемой среде начинают проявляться при превышении некоторого порога количества узлов, подключенных к разделяемой среде. Технология Ethernet наиболее чувствительна к перегрузкам разделяемого сегмента, но и другие технологии также весьма страдают от этого эффекта.

Ограничения, возникающие из-за использования общей разделяемой среды, можно преодолеть, подвергнув сеть **логической структуризации -** разделив ее на несколько сегментов, соединенных мостами, коммутаторами или маршрутизаторами. Эти коммуникационные устройства передают кадры с одного своего порта на другой, анализируя адрес назначения. (В отличие от концентраторов, которые просто повторяют кадры на всех своих портах). Мосты и коммутаторы выполняют операцию передачи кадров на основе MAC-адресов, а маршрутизаторы – на основе номера сети. При этом единая разделяемая среда, созданная концентраторами, делится на несколько частей, каждая из которых присоединена к порту моста, коммутатора или маршрутизатора. Это снижает нагрузку на каждый из вновь образованных сегментов, снижается время ожидания доступа, а в сетях Ethernet – и интенсивность коллизий. Положительные результаты структуризации локальной сети будут наиболее заметны при таком разделении на сегменты, которое обеспечит максимальный внутрисегментный трафик и минимальный межсегментный. На практике на предприятии всегда можно выделить группу компьютеров, которые принадлежат сотрудникам, выполняющим общую задачу и нуждающимся главным образом в локальных ресурсах. Кроме того, каждая подсеть может быть адаптирована к специфическим потребностям рабочей группы или отдела, например, использованием необходимых в работе данного отдела сетевых приложений, баз данных или операционной системы.

Деление сети на подсети повышает безопасность данных. При подключе-

нии пользователей к различным физическим сегментам сети можно запретить доступ определенных пользователей к ресурсам других сегментов. Устанавливая различные логические фильтры на мостах, коммутаторах и маршрутизаторах, можно контролировать доступ к ресурсам, чего не позволяют сделать повторители.

Побочным эффектом уменьшения трафика и повышения безопасности данных является упрощение управления сетью. Проблемы, как правило, возникают внутри сегмента. При этом проблемы, возникшие в одной подсети, не оказывают влияния на нормальную работу других подсетей. Подсети образуют логические домены управления сетью.

4.2.1. Виртуальные локальные сети как способ стуктуризации сети

Появившаяся относительно недавно в коммутаторах технология виртуальных локальных сетей (Virtual LAN, VLAN), позволяет преодолеть ограничение, заставляющее коммутаторы транслировать широковещательный трафик во все сегменты сети.

> ***Виртуальной сетью*** *называется группа узлов сети, трафик которой, в том числе и широковещательный, на канальном уровне полностью изолирован от других узлов сети.*

Передача кадров между разными виртуальными сетями на основании адреса канального уровня (MAC-адреса) невозможна, независимо от типа адреса – уникального, группового или широковещательного. В то же время внутри виртуальной сети кадры передаются на тот порт, который связан с адресом назначения кадра. Виртуальные сети могут пересекаться, если один или несколько компьютеров входят в состав более чем одной виртуальной сети. Говорят, что виртуальная сеть образует **домен широковещательного трафика** (broadcast domain), по аналогии с доменом коллизий, который образуется повторителями сетей Ethernet.

Технология виртуальных сетей создает гибкую основу для построения крупной сети, соединенной маршрутизаторами, так как коммутаторы позволяют создавать полностью изолированные сегменты программным путем, не прибегая к физической коммутации. При использовании технологии виртуальных сетей в коммутаторах одновременно решаются две задачи:

- повышение производительности в каждой из виртуальных сетей, так как коммутатор передает кадры в такой сети только узлу назначения;
- изоляция сетей друг от друга для управления правами доступа пользователей и создания защитных барьеров на пути широковещательных штормов.

Для связи 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 называемым **коммутатором 3-го уровня**.

Технология образования и работы виртуальных сетей с помощью коммутаторов долгое время не стандартизировалась, хотя и была реализована в большом числе коммутаторов разных производителей. Такое положение изменилось после принятия в 1998 году стандарта **IEEE 802.1Q**, который определяет базовые правила построения виртуальных локальных сетей, не зависящие от протокола канального уровня, который поддерживает коммутатор.

В виду долгого отсутствия стандарта на VLAN каждый крупный производитель коммутаторов разработал свою технологию виртуальных сетей, которая, как правило, была несовместима с технологиями других производителей. Поэтому, несмотря на появление стандарта, можно встретиться с ситуацией, когда виртуальные сети, созданные на коммутаторах одного производителя, не распознаются и не поддерживаются коммутаторами другого производителя.

Существует несколько способов создания виртуальных локальных сетей на коммутаторах, два из них основаны на добавлении дополнительной инфор-

мации к адресным таблицам моста.

Первый способ заключается в закреплении определенных портов коммутатора за одной из виртуальных локальных сетей. Такой метод чаще всего используется при создании виртуальных сетей на основе одного коммутатора. Порт можно приписать нескольким виртуальным сетям, хотя на практике так делают редко – пропадает эффект полной изоляции сетей. Группировка портов для одного коммутатора – наиболее логичный способ образования VLAN. Виртуальных сетей, построенных на основе одного коммутатора, не может быть больше количества портов этого коммутатора. Создание виртуальных сетей методом группирования портов не требует от администратора большого объема ручной работы – достаточно каждый порт приписать к одной из нескольких заранее поименованных виртуальных сетей. Обычно такая операция выполняется с помощью специальной программы, прилагаемой к коммутатору.

Второй способ образования виртуальных сетей основан на приписывании к той или иной виртуальной сети определенных MAC-адресов. При существовании в сети множества узлов этот способ требует выполнения большого количества ручных операций от администратора. Однако он оказывается более гибким при построении виртуальных сетей на основе нескольких коммутаторов, чем способ группирования портов.

Совершенно иной подход состоит в использовании имеющихся или дополнительных полей кадра для сохранения информации о принадлежности кадра к определенной виртуальной сети, при его перемещениях между коммутаторами сети. При этом нет необходимости запоминать в каждом коммутаторе принадлежность всех MAC-адресов виртуальным сетям. Указанное дополнительное поле с пометкой о номере виртуальной сети используется только тогда, когда кадр передается от коммутатора к коммутатору, а при передаче кадра конечному узлу оно удаляется. При этом модифицируется протокол взаимодействия «коммутатор - коммутатор», а программное и аппаратное обеспечение конечных узлов остается неизменным.

Существуют и другие способы построения виртуальных сетей, которые используют уже имеющиеся поля для маркировки принадлежности кадра виртуальной сети, однако эти поля принадлежат не кадрам канальных протоколов, а пакетам сетевого уровня. В этом случае виртуальные сети образуются на основе сетевых адресов, например адресов IP, то есть той же информации, которая используется при построении объединения сетей традиционным способом. Этот эффективный способ работает тогда, когда коммутаторы поддерживают не только протоколы канального уровня, но и протоколы сетевого уровня, то есть являются комбинированными коммутаторами - маршрутизаторами.

4.3. Выбор сетевого оборудования

4.3.1. Сетевые адаптеры

Сетевой адаптер совместно с драйвером выполняют две операции: передачу и прием кадра. Распределение обязанностей между сетевым адаптером и его драйвером стандартами не определяется, поэтому каждый производитель решает этот вопрос самостоятельно. Обычно сетевые адаптеры делятся на адаптеры для клиентских компьютеров и адаптеры для серверов.

В адаптерах для клиентских компьютеров значительная часть работы перекладывается на драйвер, тем самым адаптер оказывается проще и дешевле. Недостатком такого подхода является высокая степень загрузки центрального процессора компьютера рутинными работами по передаче кадров из оперативной памяти компьютера в сеть.

Адаптеры, предназначенные для серверов, обычно снабжаются собственными процессорами, позволяющими им самостоятельно выполнять большую часть работы по передаче кадров из оперативной памяти в сеть и в обратном направлении.

В зависимости от типа протокола, адаптеры делятся на Ethernet-адаптеры, Token Ring-адаптеры, FDDI-адаптеры и т. д. Протокол Fast Ethernet позволяет

автоматически выбрать скорость работы сетевого адаптера в зависимости от возможностей концентратора, поэтому многие адаптеры Ethernet сегодня поддерживают две скорости работы и имеют в своем названии приставку 10/100. Это свойство некоторые производители называют **авточувствительностью**.

Сетевой адаптер перед установкой в компьютер необходимо конфигурировать. При конфигурировании адаптера задаются используемый адаптером номер прерывания IRQ, номер канала прямого доступа к памяти DMA (если адаптер поддерживает режим DMA) и базовый адрес портов ввода/вывода. Если сетевой адаптер, аппаратура компьютера и операционная система поддерживают стандарт Plug-and-Play, то конфигурирование адаптера и его драйвера осуществляется автоматически. В противном случае нужно сначала сконфигурировать сетевой адаптер, а затем повторить параметры его конфигурации для драйвера.

4.3.2. Концентраторы

Концентратор обычно имеет несколько портов, к которым с помощью отдельных физических сегментов кабеля подключаются конечные узлы сети – компьютеры. Концентратор объединяет отдельные физические сегменты сети в единую разделяемую среду, доступ к которой осуществляется в соответствии с одной из технологий локальных сетей – Ethernet, Token Ring и т. п. Так как логика доступа к разделяемой среде существенно зависит от технологии, то для каждого типа технологии выпускаются свои концентраторы. Для конкретной технологии иногда используется свое, узкоспециализированное название этого устройства, более точно отражающее его функции или же использующееся в силу традиций, например, для концентраторов Token Ring характерно название MSAU.

Каждый концентратор выполняет основную функцию, определенную в соответствующей технологии, которую он поддерживает. Хотя эта функция достаточно детально определена в стандарте технологии, при ее реализации кон-

центраторы разных производителей могут отличаться такими деталями, как количество портов, поддержка нескольких типов кабелей и т. п. Кроме основной функции концентратор может выполнять некоторое количество дополнительных функций, которые либо в стандарте вообще не определены, либо являются факультативными. Например, концентратор Token Ring может выполнять функцию отключения некорректно работающих портов и перехода на резервное кольцо, хотя в стандарте такие его возможности не описаны. Концентратор оказался удобным устройством для выполнения дополнительных функций, облегчающих контроль и эксплуатацию сети.

Многосегментные концентраторы с десятками и сотнями портов имеют несколько несвязанных внутренних шин и возможность подключения или отключения портов от той или иной внутренней шины программно, изменением конфигурационной информации. Эта процедура называется конфигурационной коммутацией (configuration switching). Для крупных сетей многосегментный концентратор играет роль интеллектуального кроссового шкафа, который выполняет новое соединение не за счет механического перемещения вилки кабеля в новый порт, а за счет программного изменения внутренней конфигурации устройства.

Конструктивно концентраторы выполняются нескольких типов:

Концентратор с фиксированным количеством портов – это наиболее простое конструктивное исполнение, когда устройство представляет собой отдельный корпус со всеми необходимыми элементами (портами, органами индикации и управления, блоком питания), и эти элементы заменять нельзя.

Модульный концентратор выполняется в виде отдельных модулей с фиксированным количеством портов, устанавливаемых на общее шасси. Шасси имеет внутреннюю шину для объединения отдельных модулей в единый повторитель. Часто такие концентраторы являются многосегментными.

Стековый концентратор, как и концентратор с фиксированным числом портов, выполнен в виде отдельного корпуса без возможности замены отдель-

ных его модулей, но он имеет специальные порты, через которые, с помощью специального кабеля, можно объединить нескольких таких корпусов в единый повторитель.

4.3.3. Мосты

В локальных сетях используются мосты двух типов: так называемые, **прозрачные мосты** и **мосты с маршрутизацией от источника**.

Прозрачные мосты незаметны для сетевых адаптеров конечных узлов, так как они самостоятельно строят специальную адресную таблицу, на основании пассивного наблюдения за трафиком, циркулирующим в подключенных к его портам сегментах. По адресу источника кадра мост делает вывод о принадлежности узла сегменту сети и определяет, нужно передавать пришедший кадр в другой сегмент или нет. Сетевые адаптеры при использовании прозрачных мостов работают точно так же, как и в случае их отсутствия. Алгоритм прозрачного моста не зависит от технологии локальной сети, в которой устанавливается мост.

Мосты с маршрутизацией от источника применяются для соединения колец Token Ring и FDDI, хотя для этих же целей могут использоваться и прозрачные мосты. Маршрутизация от источника (Source Routing, SR) основана на том, что станция-отправитель помещает в посылаемый в другое кольцо кадр всю адресную информацию о промежуточных мостах и кольцах, которые должен пройти кадр перед тем, как попасть в кольцо, к которому подключена станция-получатель. Хотя в название этого способа входит термин «маршрутизация», настоящей маршрутизации в строгом понимании этого термина здесь нет, так как мосты и станции используют для передачи кадров данных только информацию MAC-уровня.

Кадры с **широковещательными** MAC-адресами передаются мостом на все его порты, как и кадры с неизвестным адресом назначения. Такой режим распространения кадров называется затоплением сети (flood). Наличие мостов в

сети не препятствует распространению широковещательных кадров по всем сегментам сети, сохраняя ее прозрачность. Однако это является достоинством только в том случае, когда широковещательный адрес выработан корректно работающим узлом. Если в результате программных или аппаратных сбоев протокол верхнего уровня или сам сетевой адаптер начинают работать некорректно и с высокой интенсивностью генерируют кадры с широковещательным адресом, то мост передает эти кадры во все сегменты, затапливая сеть ошибочным трафиком. Такая ситуация называется **широковещательным штормом** (broadcast storm).

4.3.3.1. Ограничения топологии сети, построенной на мостах

Отсутствие защиты от широковещательного шторма – одно из главных ограничений моста. Другим серьезным ограничением их функциональных возможностей является невозможность поддержки петлеобразных конфигураций сети. При образовании петлевых связей между мостами происходит «размножение» передаваемого кадра, то есть появление нескольких его копий, бесконечная циркуляция копий кадра по петле в противоположных направлениях и засорение сети ненужным трафиком. Ограничение топологии структурированной сети древовидной структурой вытекает из самого принципа построения адресной таблицы мостом. В простых сетях сравнительно легко гарантировать существование одного и только одного пути между двумя сегментами. Но когда количество соединений возрастает и сеть становится сложной, то вероятность непреднамеренного образования петли оказывается высокой. Причиной появления петлевых соединений могут стать резервные связи, создаваемые между мостами для повышения надежности.

4.3.4. Коммутаторы

Широкому применению коммутаторов, способствовало то обстоятельство, что внедрение технологии коммутации не требует замены установленного

в сетях оборудования – сетевых адаптеров, концентраторов, кабельной системы. Каждый из портов коммутатора обслуживается отдельным процессором. В случае сети Ethernet – EPP (Ethernet Packet Processor). Для 8 портов матрица может обеспечить 8 одновременных внутренних каналов при полудуплексном режиме работы портов и 16 при полнодуплексном, когда передатчик и приемник каждого порта работают независимо друг от друга. Этим объясняется основной прирост производительности при использовании коммутатора. Кроме того, коммутатор может дополнительно повысить скорость обработки данных за счет специальных режимов работы. Всего используются три режима:

1. **Cut-trough** (другое название этого режима on-the-fly), обработка кадров «на лету» – кадр транслируется на приемный порт коммутатора, как только прочитан адрес назначения (первые 14 байт). Максимально быстрая обработка кадров;
2. **Store-and-Forward** – выполняется буферизация кадра, проверяется контрольная сумма и кадр транслируется по назначению только если он не поврежден. Самый медленный режим работы;
3. **Fragment Free** – компромиссный режим работы, в котором буферизуется заголовок кадра (первые 64 байт), благодаря этому большинство ошибочных кадров могут быть отфильтрованы, после чего выполняется его направление по адресу назначения.

Кадры, поступающие на каждый порт, могут обрабатываться на скорости, максимальной для технологии, поддерживаемой коммутатором. Но наличие нескольких портов может привести к ситуации, когда на один из них будут поступать кадры от двух или более других портов, создавая более интенсивный поток данных, чем предусмотрено используемой технологией. Коммутаторы, способные обрабатывать поток данных на своих портах с той же скоростью, с какой они поступают, называются **неблокирующими** (non-blocking).

Коммутаторы первого поколения строились на центральном процессоре общего назначения, связанном с интерфейсными портами по внутренней ско-

ростной шине (рис. 8).

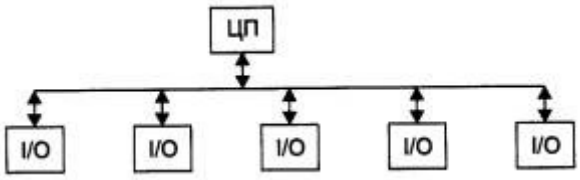

Рис. 8. Коммутатор на процессоре общего назначения

Такие устройства не обеспечивают необходимой скорости обработки данных и в настоящее время не используются. Современные коммутаторы используют в качестве базовой одну из трех схем, на которой строится такой узел обмена:

- коммутационная матрица;
- разделяемая многовходовая память;
- общая шина.

Наибольшее распространение получили коммутаторы на основе **коммутационной матрицы**, работающей по принципу коммутации каналов (рис. 9).

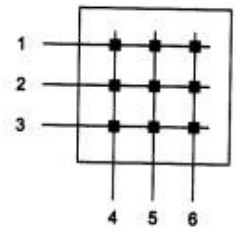

Рис. 9. Коммутационная матрица

Основные достоинства таких матриц – высокая скорость коммутации и регулярная структура, которую удобно реализовывать в интегральных микросхемах. Известным недостатком этой технологии является отсутствие буферизации данных внутри коммутационной матрицы.

В **коммутаторах с общей шиной** процессоры портов связывают высокоскоростной шиной, используемой в режиме разделения времени. Чтобы шина не блокировала работу коммутатора, ее производительность должна равняться по крайней мере сумме производительности всех портов коммутатора. Кадр передается по шине небольшими частями, по нескольку байт, чтобы передача кадров между несколькими портами происходила в псевдопараллельном режиме, не внося задержек в передачу кадра в целом. Шина, так же как и коммутаци-

онная матрица, не может осуществлять промежуточную буферизацию, но так как данные кадра разбиваются на небольшие ячейки, то задержек с начальным ожиданием доступности выходного порта в такой схеме нет.

В **коммутаторах с разделяемой памятью** входные порты (точнее процессоры, ими управляющие) соединяются с переключаемым входом разделяемой памяти, а выходные – с переключаемым выходом этой памяти. Переключением входа и выхода разделяемой памяти управляет менеджер очередей выходных портов. В разделяемой памяти менеджер организует несколько очередей данных, по одной для каждого выходного порта. Входные порты передают менеджеру портов запросы на запись данных в очередь того порта, который соответствует адресу назначения пакета. Менеджер по очереди подключает вход памяти к одному из входных блоков процессоров и тот переписывает часть данных кадра в очередь определенного выходного порта. По мере заполнения очередей менеджер производит также поочередное подключение выхода разделяемой памяти к выходным блокам процессоров портов, и данные из очереди переписываются в выходной буфер процессора.

Применение общей буферной памяти, гибко распределяемой менеджером между отдельными портами, снижает требования к размеру буферной памяти порта.

У каждой из описанных архитектур есть свои преимущества и недостатки, поэтому часто в сложных коммутаторах эти архитектуры применяются в комбинации друг с другом.

4.3.4.1. Поддержка алгоритма Spanning Tree

Алгоритм покрывающего дерева – Spanning Tree Algorithm (STA) позволяет коммутаторам автоматически определять древовидную конфигурацию связей в сети при произвольном соединения портов между собой. Т.к. для нормальной работы коммутатора требуется отсутствие замкнутых маршрутов в сети.

Поддерживающие алгоритм STA коммутаторы автоматически создают ак-

тивную древовидную конфигурацию связей (то есть связную конфигурацию без петель) на множестве всех связей сети. Такая конфигурация называется покрывающим деревом – Spanning Tree и ее название дало имя всему алгоритму. Алгоритм Spanning Tree описан в стандарте **IEEE 802.1D**, том же стандарте, который определяет принципы работы прозрачных мостов.

Коммутаторы строят покрывающее дерево с помощью обмена служебными пакетами. Реализация в коммутаторе алгоритма STA очень важна для работы в больших сетях. 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 дерево, если это возможно, и сеть автоматически восстанавливает работоспособность.

4.3.4.2. Структурные схемы локальной сети на коммутаторах

При построении локальной компьютерной сети на коммутаторах используют две базовые структуры – стянутую в точку магистраль и распределенную магистраль.

Стянутая в точку магистраль (collapsed backbone) – это структура, при которой объединение узлов, сегментов или сетей происходит на внутренней магистрали коммутатора. Преимуществом такой структуры является высокая производительность магистрали. Причем ее скорость не зависит от применяемых в сети протоколов. Подключение нового узла с новым протоколом часто требует не замены коммутатора, а просто добавления соответствующего интерфейсного модуля, поддерживающего этот протокол.

Распределенная магистраль – это разделяемый сегмент сети, поддерживающий определенный протокол, к которому присоединяются коммутаторы сетей рабочих групп и отделов (рис. 10).

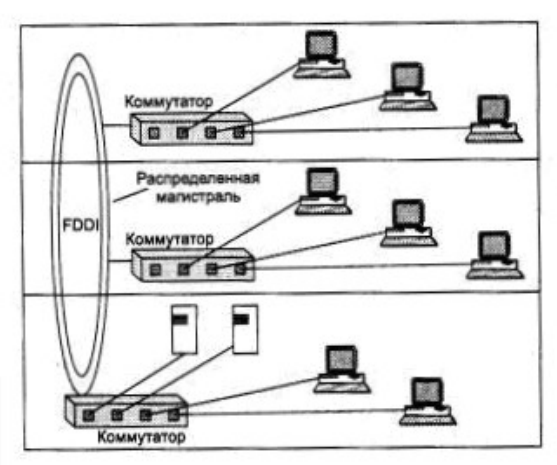

Рис. 10. Структура сети с распределенной магистралью

Иногда просто невозможно стянуть все кабели в одно помещение. В таких локальных сетях, покрывающих большие территории, используется вариант построения сети с распределенной магистралью.

4.3.5. Маршрутизаторы

Маршрутизатор – это устройство, стоящее на границе локальной сети и обеспечивающее выход из локальной сети в глобальную или соединение нескольких локальных сетей. Основная задача маршрутизатора – выбор наилучшего маршрута в сети – часто является достаточно сложной с математической точки зрения. Поэтому современный маршрутизатор является мощным вычислительным устройством с одним или несколькими специализированными процессорами, со сложным программным обеспечением. Если маршрутизатор может поддерживать несколько протоколов сетевого уровня, он называется **многопротокольным** маршрутизатором.

По областям применения маршрутизаторы делятся на несколько классов:

Магистральные маршрутизаторы (backbone routers) предназначены для построения центральной сети корпорации. Центральная сеть может состоять из большого количества локальных сетей, разбросанных по разным зданиям и использующих самые разнообразные сетевые технологии, типы компьютеров и операционных систем. Магистральные маршрутизаторы – это наиболее мощ-

ные устройства, способные обрабатывать несколько сотен тысяч или миллионов пакетов в секунду, имеющие большое количество интерфейсов локальных и глобальных сетей. Чаще всего магистральный маршрутизатор конструктивно выполнен по модульной схеме на основе шасси с большим количеством слотов. Большое внимание уделяется в магистральных моделях надежности и отказоустойчивости маршрутизатора, которая достигается за счет системы терморегуляции, резервных источников питания, заменяемых «на ходу» (hot swap) модулей, а также параллельного мультипроцессирования.

Маршрутизаторы региональных отделений соединяют соответствующие отделения между собой и с центральной сетью. Сеть регионального отделения, так же как и центральная сеть, может состоять из нескольких локальных сетей. Такой маршрутизатор обычно представляет собой несколько упрощенную версию магистрального маршрутизатора. Поддерживаемые интерфейсы локальных и глобальных сетей менее скоростные, их количество меньше.

Маршрутизаторы удаленных офисов соединяют, как правило, единственную локальную сеть удаленного офиса с центральной сетью или сетью регионального отделения. Как правило, интерфейс локальной сети – это Ethernet 10 Мбит/с, а интерфейс глобальной сети, в которую обеспечивает выход маршрутизатор, – выделенная линия со скоростью 64 Кбит/с, 1,544 или 2 Мбит/с. Маршрутизатор удаленного офиса может поддерживать и работу по коммутируемой телефонной линии в качестве резервной связи для выделенного канала. Существует большое количество типов маршрутизаторов удаленных офисов. Это объясняется как массовостью потенциальных потребителей, так и специализацией такого типа устройств, проявляющейся в поддержке одного конкретного типа глобальной связи.

Маршрутизаторы локальных сетей (коммутаторы 3-го уровня) предназначены для разделения крупных локальных сетей на подсети. Основное требование, предъявляемое к ним, – высокая скорость маршрутизации. Технологии локальных сетей высокоскоростные, поэтому в таких устройствах отсутствуют

низкоскоростные модемные порты.

4.3.5.1. Основные технические характеристики маршрутизатора

Основные технические характеристики маршрутизатора связаны с тем, как он решает свою главную задачу – маршрутизацию пакетов в составной сети. Именно эти характеристики прежде всего определяют возможности и сферу применения того или иного маршрутизатора.

Перечень поддерживаемых сетевых протоколов. Обычно включает протоколы IP, IPX, AppleTalk, DECnet, Banyan VINES, Xerox XNS.

Перечень протоколов маршрутизации. Это могут быть протоколы RIP, NLSP, OSPF, IS-IS, EIGRP, BGP и др.

Перечень поддерживаемых интерфейсов локальных и глобальных сетей. Для локальных сетей – это интерфейсы, реализующие физические и канальные протоколы сетей Ethernet, Token Ring, FDDI, Fast Ethernet, Gigabit Ethernet, 100VG-AnyLAN и ATM.

Общая производительность маршрутизатора. Высокая производительность маршрутизации важна для работы с высокоскоростными локальными сетями, а также для поддержки новых высокоскоростных глобальных технологий, таких как frame relay, Т3/Е3, SDH и ATM. Общая производительность маршрутизатора зависит от многих факторов, наиболее важными из которых являются: тип используемых процессоров, эффективность программной реализации протоколов, архитектурная организация вычислительных и интерфейсных модулей. Общая производительность маршрутизаторов колеблется от нескольких десятков тысяч пакетов в секунду до нескольких миллионов пакетов в секунду. Наиболее производительные маршрутизаторы имеют мультипроцессорную архитектуру, сочетающую симметричные и асимметричные свойства – несколько мощных центральных процессоров по симметричной схеме выполняют функции вычисления таблицы маршрутизации, а менее мощные процессоры в интерфейсных модулях занимаются передачей пакетов на подключенные к ним сети и

пересылкой пакетов на основании части таблицы маршрутизации, кэшированной в локальной памяти интерфейсного модуля.

4.3.5.2. Дополнительные возможности

К дополнительным возможностям относится, например, поддержка **политики маршрутных объявлений**. В большинстве протоколов обмена маршрутной информации (RIP, OSPF, NLSP) предполагается, что маршрутизатор объявляет в своих сообщениях обо всех сетях, которые ему известны. Аналогично предполагается, что маршрутизатор при построении своей таблицы учитывает все адреса сетей, которые поступают ему от других маршрутизаторов сети. Однако существуют ситуации, когда администратор хотел бы скрыть существование некоторых сетей в определенной части своей сети от других администраторов, например, по соображениям безопасности. Или же администратор хотел бы запретить некоторые маршруты, которые могли бы существовать в сети. При статическом построении таблиц маршрутизации решение таких проблем не составляет труда. Динамические же протоколы маршрутизации не позволяют стандартным способом реализовывать подобные ограничения. Существует только один широко используемый протокол динамической маршрутизации, в котором описана возможность существования правил (policy), ограничивающих распространение некоторых адресов в объявлениях, – это протокол BGP. Разработчики маршрутизаторов исправляют этот недостаток стандартов протоколов, вводя в маршрутизаторы поддержку правил передачи и использования маршрутной информации.

Поддержка немаршрутизируемых протоколов, также является весьма полезной дополнительной возможностью. Протоколы NetBIOS, NetBEUI или DEC LAT, не оперируют с таким понятием, как сеть, но в то же время, достаточно распространены. Маршрутизаторы могут обрабатывать пакеты таких протоколов двумя способами:

- они могут работать с пакетами этих протоколов как мосты, то есть пере-

давать их на основании изучения MAC-адресов. Маршрутизатор необходимо сконфигурировать особым способом, чтобы по отношению к некоторым немаршрутизируемым протоколам на некоторых портах он выполнял функции моста, а по отношению к маршрутизируемым протоколам – функции маршрутизатора. Такой мост/маршрутизатор иногда называют **brouter** (bridge плюс router).

- Другим способом передачи пакетов немаршрутизируемых протоколов является инкапсуляция этих пакетов в пакеты какого-либо сетевого протокола. Некоторые производители маршрутизаторов разработали собственные протоколы, специально предназначенные для инкапсуляции немаршрутизируемых пакетов. Кроме того, существуют стандарты для инкапсуляции некоторых протоколов в другие, в основном в IP. Примером такого стандарта является протокол DLSw, определяющий методы инкапсуляции пакетов SDLC и NetBIOS в IP-пакеты, а также протоколы PPTP и L2TP, инкапсулирующие кадры протокола PPP в IP-пакеты.

Вопросы для самостоятельной проработки:

1. Назовите этапы проектирования компьютерной сети.
2. От чего зависит выбор сетевой технологии.
3. Что такое логическая структуризация сети.
4. Какие ограничения имеет сеть, построенная на мостах.
5. Назовите и опишите разновидности локальных компьютерных сетей, построенных на коммутаторах.
6. В каких устройствах работает алгоритм покрывающего дерева (Spanning Tree), какие задачи выполняются с помощью этого алгоритма.
7. В каких режимах может работать коммутатор.
8. Какие принципы построения коммутаторов вы знаете.
9. Назовите основные технические характеристики маршрутизатора.

5. Системы управления и мониторинга компьютерных сетей

В основе любой системы управления сетью лежит элементарная схема взаимодействия агента с менеджером. На основе этой схемы могут быть построены системы практически любой сложности с большим количеством агентов и менеджеров разного типа. Агент является посредником между управляемым ресурсом и основной управляющей программой-менеджером. Чтобы один и тот же менеджер мог управлять различными реальными ресурсами, создается некоторая модель управляемого ресурса, которая отражает только те характеристики ресурса, которые нужны для его контроля и управления. Например, модель маршрутизатора обычно включает такие характеристики, как количество портов, их тип, таблицу маршрутизации, количество кадров и пакетов протоколов канального, сетевого и транспортного уровней, прошедших через эти порты. Менеджер получает от агента только те данные, которые описываются моделью ресурса. Агент поставляет менеджеру обработанную и представленную в нормализованном виде информацию. На основе этой информации менеджер принимает решения по управлению. Для получения требуемых данных от объекта, а также для выдачи на него управляющих воздействий агент взаимодействует с реальным ресурсом. Разработчик оборудования предусматривает точки и способы взаимодействия внутренних узлов устройства с агентом. При разработке агента для операционной системы разработчик пользуется теми интерфейсами, которые существуют в этой ОС, например интерфейсами ядра, драйверов и приложений.

Менеджер и агент должны использовать одну и ту же модель управляемого ресурса, иначе они не смогут понять друг друга. Однако работают они с этой моделью по разному. Агент наполняет модель управляемого ресурса текущими значениями характеристик, и в связи с этим модель агента называют **базой данных управляющей информации** – Management Information Base, MIB. Мене-

джер использует модель, чтобы знать о том, чем характеризуется ресурс, какие характеристики он может запросить у агента и какими параметрами можно управлять. Менеджер взаимодействует с агентом по стандартному протоколу. Этот протокол должен позволять менеджеру запрашивать значения параметров, хранящихся в базе MIB, а также передавать агенту управляющую информацию, на основе которой тот должен управлять устройством. Различают управление **inband**, то есть по тому же каналу, по которому передаются пользовательские данные, и управление **out-of-band**, то есть вне канала, по которому передаются пользовательские данные. Управление по тому же каналу, по которому работает сеть, более экономично, так как не требует создания отдельной инфраструктуры передачи управляющих данных. Однако способ out-of-band более надежен, так как предоставляет возможность управлять оборудованием сети и тогда, когда какие-то элементы сети вышли из строя и по основным каналам оборудование недоступно.

Обычно менеджер работает с несколькими агентами, обрабатывая получаемые от них данные и выдавая на них управляющие воздействия. Агенты могут встраиваться в управляемое оборудование, а могут и работать на отдельном компьютере, связанном с управляемым оборудованием по какому-либо интерфейсу. Менеджер обычно работает на отдельном компьютере, который выполняет также роль консоли управления для оператора или администратора системы.

5.1. Система управления сетью на основе протокола SNMP

В системах управления, построенных на основе протокола SNMP(Simple Network Management Protocol) – простой протокол управления сетью, стандартизуются следующие элементы:

- протокол взаимодействия агента и менеджера;
- язык описания моделей MIB и сообщений SNMP;
- несколько конкретных моделей MIB.

С помощью протокола SNMP от сетевых устройств можно получить информа-

цию об их статусе, производительности и других характеристиках. Простота SNMP во многом определяется простотой MIB SNMP. Она имеет древовидную структуру, содержащую обязательные (стандартные) ветви и позволяющую создавать пользовательские (private) поддеревья для управляния какими-либо специфическими функциями устройства на основе созданных объектов MIB.

Основные операции по управлению вынесены в менеджер, а агент SNMP выполняет чаще всего пассивную роль, передавая в менеджер по его запросу значения накопленных статистических переменных. При этом устройство работает с минимальными издержками на поддержание управляющего протокола. Оно использует почти всю свою вычислительную мощность для выполнения своих основных функций маршрутизатора, моста или концентратора, а агент занимается сбором статистики и значений переменных состояния устройства и передачей их менеджеру системы управления.

5.1.1. Структура SNMP MIB

Существует несколько стандартов на базы данных управляющей информации для протокола SNMP. Основными являются стандарты MIB-I и MIB-II, а также версия базы данных для удаленного управления RMON MIB. Кроме этого существуют стандарты для специальных устройств MIB конкретного типа (например, MIB для концентраторов или MIB для модемов), а также частные MIB конкретных фирм-производителей оборудования. Первоначальная спецификация MIB-I определяла только операции чтения значений переменных. Операции изменения или установки значений объекта являются частью спецификаций MIB-II.

На рис. 11 приведен пример древовидной структуры базы объектов MIB-II. На нем показаны две из 10 возможных групп объектов – System (имена объектов начинаются с префикса Sys) и Interfaces (префикс if). Объект SysUpTime содержит значение продолжительности времени работы системы с момен-

та последней перезагрузки, объект SysObjectID – идентификатор устройства (например, маршрутизатора). Объект ifNumber определяет количество сетевых интерфейсов устройства, а объект ifEntry является вершиной поддерева, описывающего один из конкретных интерфейсов устройства. Входящие в это поддерево объекты ifType и ifAdminStatus определяют соответственно тип и состояние одного из интерфейсов, в данном случае интерфейса Ethernet.

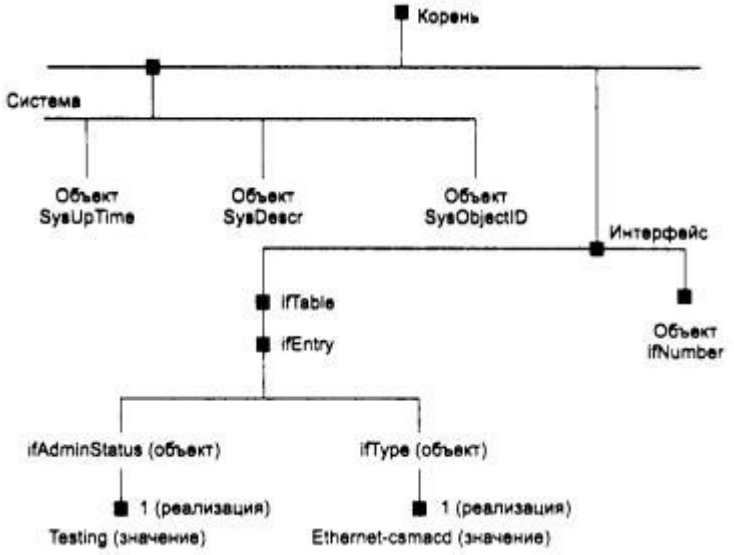

Рис. 11. Стандартное дерево MIB-II (фрагмент).

База данных MIB-II не дает детальной статистики по характерным ошибкам кадров Ethernet, кроме этого, она не отражает изменение характеристик во времени, что часто интересует сетевого администратора. Эти ограничения сняты в стандарте RMON MIB, который специально ориентирован на сбор детальной статистики по протоколу Ethernet, к тому же с поддержкой такой важной функции, как построение агентом зависимостей статистических характеристик от времени. С помощью агента RMON, встроенного в повторитель или другое коммуникационное устройство, можно провести очень детальный анализ работы сегмента Ethernet или Fast Ethernet. Сначала можно получить данные о встречающихся в сегменте типах ошибок в кадрах, а затем собрать с помощью группы History зависимости интенсивности этих ошибок от времени (в том числе и привязав их ко времени). После анализа временных зависимостей часто уже можно сделать некоторые предварительные выводы об источнике ошибоч-

ных кадров и на этом основании сформулировать более тонкие условия захвата кадров со специфическими признаками (задав соответствующие условия в группе Filter). После этого можно провести еще более детальный анализ за счет изучения захваченных кадров, извлекая их из объектов группы Packet Capture.

Новый стандарт RMON 2 распространяет идеи интеллектуальной RMON MIB на протоколы верхних уровней, выполняя часть работы анализаторов протоколов.

5.2. Мониторинг и анализ локальных сетей

Постоянный контроль за работой локальной сети, составляющей основу любой корпоративной сети, необходим для поддержания ее в работоспособном состоянии. Контроль – это необходимый первый этап, который должен выполняться при управлении сетью. Ввиду важности этой функции ее часто отделяют от других функций систем управления и реализуют специальными средствами. Такое разделение функций контроля и собственно управления полезно для небольших и средних сетей, для которых установка интегрированной системы управления экономически нецелесообразна. Использование автономных средств контроля помогает администратору сети выявить проблемные участки и устройства сети, а их отключение или реконфигурацию он может выполнять в этом случае вручную. Процесс контроля работы сети обычно делят на два этапа – **мониторинг** и **анализ**.

На этапе мониторинга выполняется более простая процедура – процедура сбора первичных данных о работе сети: статистики о количестве циркулирующих в сети кадров и пакетов различных протоколов, состоянии портов концентраторов, коммутаторов и маршрутизаторов и т. п.

Далее выполняется анализ, под которым понимается более сложный и интеллектуальный процесс осмысления собранной информации, сопоставления ее с данными, полученными ранее, и выработки предположений о возможных причинах замедленной или ненадежной работы сети.

Задачи мониторинга решаются программными и аппаратными измерителями, тестерами, сетевыми анализаторами, встроенными средствами мониторинга коммуникационных устройств, а также агентами систем управления. Задача анализа требует более активного участия человека и использования таких сложных средств, как экспертные системы, аккумулирующие практический опыт многих сетевых специалистов.

5.2.1. Классификация средств мониторинга и анализа

Все многообразие средств, применяемых для анализа и диагностики вычислительных сетей, можно разделить на несколько крупных классов:

1. Агенты систем управления, поддерживающие функции одной из стандартных MIB и поставляющие информацию по протоколу SNMP или CMIP. Для получения данных от агентов обычно требуется наличие системы управления, собирающей данные от агентов в автоматическом режиме.

2. Встроенные системы диагностики и управления (Embedded systems). Эти системы выполняются в виде программно-аппаратных модулей, устанавливаемых в коммуникационное оборудование, а также в виде программных модулей, встроенных в операционные системы. Они выполняют функции диагностики и управления одним устройством, и в этом их основное отличие от централизованных систем управления. Примером средств этого класса может служить модуль управления многосегментным повторителем Ethernet, реализующий функции автосегментации портов при обнаружении неисправностей, приписывания портов внутренним сегментам повторителя и некоторые другие. Как правило, встроенные модули управления «по совместительству» выполняют роль SNMP-агентов, поставляющих данные о состоянии устройства для систем управления.

3. Анализаторы протоколов (Protocol analyzers). Представляют собой программные или аппаратно-программные системы, которые ограничиваются в отличие от систем управления лишь функциями мониторинга и анализа трафика в сетях. Хороший анализатор протоколов может захватывать и декодировать паке-

ты большого количества протоколов, применяемых в сетях. Анализаторы протоколов позволяют установить некоторые логические условия для захвата отдельных пакетов и выполняют полное декодирование захваченных пакетов, то есть показывают в удобной для специалиста форме вложенность пакетов протоколов разных уровней друг в друга с расшифровкой содержания отдельных полей каждого пакета.

4. Экспертные системы. Этот вид систем аккумулирует знания технических специалистов о выявлении причин аномальной работы сетей и возможных способах приведения сети в работоспособное состояние. Экспертные системы часто реализуются в виде отдельных подсистем различных средств мониторинга и анализа сетей: систем управления сетями, анализаторов протоколов, сетевых анализаторов. Простейшим вариантом экспертной системы является контекстно-зависимая система помощи. Более сложные экспертные системы представляют собой, так называемые базы знаний, обладающие элементами искусственного интеллекта. Работа экспертных систем состоит в анализе большого числа событий для выдачи пользователю краткого диагноза о причине неисправности сети.

5. Оборудование для диагностики и сертификации кабельных систем. Условно это оборудование можно поделить на четыре основные группы: сетевые мониторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры.

- **Сетевые мониторы** (называемые также сетевыми анализаторами) предназначены для тестирование кабелей различных категорий. Сетевые мониторы собирают также данные о статистических показателях трафика – средней интенсивности общего трафика сети, средней интенсивности потока пакетов с определенным типом ошибки и т. п. Эти устройства являются наиболее интеллектуальными устройствами из всех четырех групп устройств данного класса, так как работают не только на физическом, но и на канальном, а иногда и на сетевом уровнях.

- **Устройства для сертификации кабельных систем** выполняют проверку кабельной системы на соответствие ее требованиям одного из стандартов на кабельные системы.
- **Кабельные сканеры** используются для диагностики медных кабельных систем.
- **Тестеры** предназначены для проверки кабелей на отсутствие физического разрыва.

6. Многофункциональные портативные устройства анализа и диагностики. В связи с развитием технологии больших интегральных схем появилась возможность производства портативных приборов, которые совмещали бы функции нескольких устройств: кабельных сканеров, сетевых мониторов и анализаторов протоколов.

5.2.1.1. Анализаторы протоколов

Анализатор протоколов представляет собой либо специализированное устройство, либо персональный компьютер, обычно переносной, класса Notebook, оснащенный специальной сетевой картой и соответствующим программным обеспечением. Применяемые сетевая карта и программное обеспечение должны соответствовать технологии сети (Ethernet, Token Ring, FDDI, Fast Ethernet). Анализатор подключается к сети точно так же, как и обычный узел. Отличие состоит в том, что анализатор может принимать все пакеты данных, передаваемые по сети, в то время как обычная станция – только адресованные ей. Для этого сетевой адаптер анализатора протоколов переводится в режим «беспорядочного» захвата – promiscuous mode. Программное обеспечение анализатора состоит из ядра, поддерживающего работу сетевого адаптера и программного обеспечения, декодирующего протокол канального уровня, с которым работает сетевой адаптер, а также наиболее распространенные протоколы верхних уровней, например IP, TCP, ftp, telnet, HTTP, IPX, NCP, NetBEUI, DECnet и т. п. В состав некоторых анализаторов может входить также экспертная система, ко-

торая позволяет выдавать пользователю рекомендации о том, какие эксперименты следует проводить в данной ситуации, что могут означать те или иные результаты измерений, как устранить некоторые виды неисправности сети.

Анализаторы протоколов имеют некоторые общие свойства:

- Возможность (кроме захвата пакетов) измерения среднестатистических показателей трафика в сегменте локальной сети, в котором установлен сетевой адаптер анализатора. Обычно измеряется коэффициент использования сегмента, матрицы перекрестного трафика узлов, количество хороших и плохих кадров, прошедших через сегмент.
- Возможность работы с несколькими агентами, поставляющими захваченные пакеты из разных сегментов локальной сети. Эти агенты чаще всего взаимодействуют с анализатором протоколов по собственному протоколу прикладного уровня, отличному от SNMP или CMIP.
- Наличие развитого графического интерфейса, позволяющего представить результаты декодирования пакетов с разной степенью детализации.
- Фильтрация захватываемых и отображаемых пакетов. Условия фильтрации задаются в зависимости от значения адресов назначения и источника, типа протокола или значения определенных полей пакета. Пакет либо игнорируется, либо записывается в буфер захвата. Использование фильтров значительно ускоряет и упрощает анализ, так как исключает захват или просмотр ненужных в данный момент пакетов.
- Использование триггеров. Триггеры – это задаваемые администратором некоторые условия начала и прекращения процесса захвата данных из сети. Такими условиями могут быть: время суток, продолжительность процесса захвата, появление определенных значений в кадрах данных. Триггеры могут использоваться совместно с фильтрами, позволяя более детально и тонко проводить анализ, а также продуктивнее расходовать ограниченный объем буфера захвата.
- Многоканальность. Некоторые анализаторы протоколов позволяют прово-

дить одновременную запись пакетов от нескольких сетевых адаптеров, что удобно для сопоставления процессов, происходящих в разных сегментах сети. Возможности анализа проблем сети на физическом уровне у анализаторов протоколов минимальные, поскольку всю информацию они получают от стандартных сетевых адаптеров. Поэтому они передают и обобщают информацию физического уровня, которую сообщает им сетевой адаптер, а она во многом зависит от типа сетевого адаптера. Некоторые сетевые адаптеры сообщают более детальные данные об ошибках кадров и интенсивности коллизий в сегменте, а некоторые вообще не передают такую информацию верхним уровням протоколов, на которых работает анализатор протоколов.

С распространением серверов Windows NT все более популярным становится анализатор **Network Monitor** фирмы Microsoft. Он является частью сервера управления системой SMS, а также входит в стандартную поставку Windows NT Server, начиная с версии 4.0 (версия с усеченными функциями). Network Monitor в версии SMS является многоканальным анализатором протоколов, поскольку может получать данные от нескольких агентов Network Monitor Agent, работающих в среде Windows NT Server, однако в каждый момент времени анализатор может работать только с одним агентом, так что сопоставить данные разных каналов с его помощью не удастся. Network Monitor поддерживает фильтры захвата (достаточно простые) и дисплейные фильтры, отображающие нужные кадры после захвата (более сложные). Экспертной системой Network Monitor не располагает.

5.2.1.2. Сетевые анализаторы

Сетевые анализаторы представляют собой эталонные измерительные приборы для диагностики и сертификации кабелей и кабельных систем. Они могут с высокой точностью измерить все электрические параметры кабельных систем, а также работают на более высоких уровнях стека протоколов. Сетевые анали-

заторы генерируют синусоидальные сигналы в широком диапазоне частот, что позволяет измерять на приемной паре амплитудно-частотную характеристику и перекрестные наводки, затухание и суммарное затухание. Сетевой анализатор представляет собой лабораторный прибор больших размеров, достаточно сложный в обращении.

Многие производители дополняют сетевые анализаторы функциями статистического анализа трафика – коэффициента использования сегмента, уровня широковещательного трафика, процента ошибочных кадров, а также функциями анализатора протоколов, которые обеспечивают захват пакетов разных протоколов в соответствии с условиями фильтров и декодирование пакетов.

5.2.1.3. Кабельные сканеры и тестеры

Основное назначение кабельных сканеров – измерение электрических и механических параметров кабелей: длины кабеля, параметра NEXT, затухания, импеданса, схемы разводки пар проводников, уровня электрических шумов в кабеле. Точность измерений, произведенных этими устройствами, ниже, чем у сетевых анализаторов, но вполне достаточна для оценки соответствия кабеля стандарту.

Для определения местоположения неисправности кабельной системы (обрыва, короткого замыкания, неправильно установленного разъема и т. д.) используется метод «отраженного импульса» (Time Domain Reflectometry, TDR). Суть этого метода состоит в том, что сканер излучает в кабель короткий электрический импульс и измеряет время задержки до прихода отраженного сигнала. По полярности отраженного импульса определяется характер повреждения кабеля (короткое замыкание или обрыв). В правильно установленном и подключенном кабеле отраженный импульс почти отсутствует.

Точность измерения расстояния зависит от того, насколько точно известна скорость распространения электромагнитных волн в кабеле. В различных кабелях она будет разной. Скорость распространения электромагнитных волн в ка-

беле (Nominal Velocity of Propagation, NVP) обычно задается в процентах от скорости света в вакууме. Современные сканеры содержат в себе электронную таблицу данных о NVP для всех основных типов кабелей, что дает возможность пользователю устанавливать эти параметры самостоятельно после предварительной калибровки.

Кабельные сканеры – это портативные приборы, которые обслуживающий персонал может постоянно носить с собой.

Кабельные тестеры – наиболее простые и дешевые приборы для диагностики кабеля. Они позволяют определить непрерывность кабеля, однако, в отличие от кабельных сканеров, не дают ответа на вопрос о том, в каком месте произошел сбой.

Вопросы для самостоятельной проработки:

1. На каком принципе построены системы управления компьютерной сетью.
2. Что такое MIB, какую функцию она выполняет в системах упраления сетью.
3. В чем различие между inband и out-of-band управлением.
4. Какие средства мониторинга компьютерных сетей вы знаете.
5. Чем отличаются сетевые анализаторы от анализаторов протоколов.
6. Может ли экспертная система помочь в поиске неисправности в локальной сети.

Список рекомендуемой литературы

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. СПб.: Питер. 2001. 864с.
2. Хелд Г. Технологии передачи данных. СПб.: Питер. 2003. 715.
3. Танненбаум Э. Компьютерные сети. СПб.: Питер. 2002. 992с
4. Спортак М. Компьютерные сети и сетевые технологии. Диасофт-ЮП. 2005. 720с.
5. Столлингс В. Современные компьютерные сети. СПб.: Питер. 2003. 784с.