ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САМАРСКИЙ ГОСУДАРСТВЕННЫЙ АЭРОКОСМИЧЕСКИЙ
УНИВЕРСИТЕТ имени академика С.П. КОРОЛЕВА
(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)»

КОМПЬЮТЕРНЫЕ СЕТИ

САМАРА 2010

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САМАРСКИЙ ГОСУДАРСТВЕННЫЙ АЭРОКОСМИЧЕСКИЙ
УНИВЕРСИТЕТ имени академика С.П. КОРОЛЕВА
(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)»

Д.В. Еленев

КОМПЬЮТЕРНЫЕ СЕТИ

Утверждено Редакционно-издательским советом университета
в качестве учебного пособия

САМАРА
Издательство СГАУ
2010

УДК СГАУ: 004(075)
ББК 32.97
Е504

Рецензенты:
проректор по информатизации СГАУ
доктор технических наук, профессор В. С. Кузьмичёв;
начальник информационно-вычислительного центра СамГТУ
кандидат технических наук, доцент Л. А. Льноградский

Еленев Д.В.

Е504 **Компьютерные сети**: учеб. пособие / *Д.В. Еленев*. Самара: Изд-во Самар. гос. аэрокосм. ун-та, 2010. – 80 с.: ил.

ISBN 978-5-7883-0799-2

Рассматриваются принципы построения компьютерных сетей, их топологии, среды передачи информации, методы доступа к среде передачи информации и методы контроля правильности передачи информации. Описываются архитектура TCP/IP, адресация, маршрутизация, протоколы IP, TCP и UDP, технологии локальных вычислительных сетей.

Предназначено для студентов очной и заочной форм обучения, обучающихся по специальностям «Автоматизированные системы обработки информации и управления» и «Информационные технологии».

УДК СГАУ: 004(075)
ББК 32.97

ISBN 978-5-7883-0799-2

СОДЕРЖАНИЕ

1 ОБЩИЕ СВЕДЕНИЯ О КОМПЬЮТЕРНЫХ СЕТЯХ

1.1 Классификация компьютерных сетей

Компьютерная сеть представляет собой систему компьютеров, объединенных каналами передачи данных. Основное назначение компьютерной сети – обеспечение эффективного предоставления различных информационно-вычислительных услуг пользователям сети путем организации удобного и надежного доступа к ресурсам, распределенным в этой сети. Подавляющая часть услуг большинства сетей лежит в сфере информационного обслуживания.

Информационные системы, построенные на базе компьютерных сетей, обеспечивают эффективное выполнение следующих задач: хранение данных, обработка данных, организация доступа пользователей к данным, передача данных и результатов обработки пользователям.

Эффективность решения указанных задач обеспечивается: распределенными в сети аппаратными, программными и информационными ресурсами; возможным наличием централизованной базы данных наряду с распределенными базами данных; высокой надежностью функционирования системы, обеспечиваемой резервированием ее элементов; возможностью оперативного перераспределения нагрузки в пиковые периоды; специализацией отдельных узлов сети на решении задач определенного класса, решением сложных задач совместными усилиями нескольких узлов сети; оперативным дистанционным информационным обслуживанием клиентов.

Сеть должна обеспечивать выполнение всех предусмотренных для нее функций: по доступу ко всем ресурсам; совместной работе узлов; реализации всех протоколов и стандартов работы.

Основными показатели качества компьютерной сети являются:

– Производительность – среднее количество запросов пользователей сети, исполняемых за единицу времени.

– Надежность, характеризующаяся средним временем наработки на отказ.

– Безопасность – способность сети обеспечить защиту информации от взлома. Современные сети часто имеют дело с конфиденциальной информацией, безопасность информации является важной характеристикой сети.

– Масштабируемость – возможность расширения сети без заметного снижения ее производительности.

– Универсальность – возможность подключения к сети разнообразного техоборудования и программного обеспечения от разных производителей.

– Прозрачность сети – невидимость особенностей внутренней архитектуры сети для пользователя: в оптимальном случае он должен обращаться к ресурсам сети как к локальным ресурсам своего компьютера.

Компьютерные сети в зависимости от покрываемой ими территории делятся:

– на локальные вычислительные сети (ЛВС, LAN – Local Area Network),

– региональные (MAN – Metropolitan Area Network),

– глобальные (WAN – Wide Area Network).

Локальной называется сеть, абоненты которой находятся на небольшом (в пределах нескольких километров) расстоянии друг от друга. ЛВС объединяет абонентов, расположенных в пределах небольшой территории. Четких ограничений на территориальный разброс абонен-

тов локальной вычислительной сети не существует, обычно такая сеть привязывается к конкретному объекту – офису, зданию или комплексу зданий.

Региональные сети связывают абонентов города, района, области или небольшой страны. Расстояния между абонентами региональной сети – порядка десятков и сотен километров.

Глобальные сети объединяют абонентов, удаленных друг от друга на значительное расстояние, часто расположенных в различных странах или на разных континентах.

1.2 Сети одноранговые и «клиент-сервер»

Существуют две основные архитектуры сети: одноранговая (peer-to-peer) и «клиент/сервер» (client/server).

В одноранговой сети все компьютеры равноправны – имеют один ранг. Поэтому любой компьютер может выступать как в роли сервера, то есть предоставлять свои ресурсы (файлы, принтеры) другому компьютеру, так и в роли клиента – использовать предоставленные ему ресурсы.

В сети клиент/сервер существует один или несколько компьютеров-серверов, несущих дополнительную нагрузку по предоставлению определенных услуг другим компьютерам. Все остальные компьютеры сети называются клиентами или рабочими станциями.

В зависимости от видов предоставляемых услуг серверы делятся на серверы баз данных, файловые серверы, серверы печати, почтовые серверы, web-серверы и т.д.

1.3 Механизм «клиент-сервер»

Механизм «клиент-сервер» реализует доступ к информационным ресурсам, ввод и выполнение команд за счет использования двух взаимосвязанных программ. Первая принимает команды пользователя, на-

зывается «клиент» и использует вычислительные ресурсы пользователя. Вторая программа запускается на другом компьютере, который располагает информационными ресурсами и называется «сервер». Программа-сервер принимает заказ от своего удалённого клиента, обрабатывает его и отправляет обратно требуемую информацию с помощью соответствующего протокола передачи данных.

Таким образом, предоставлением услуг управляют программы, которые состоят, в общем случае, из двух компонент – клиента и сервера. Серверная и клиентская компоненты могут быть размещены и на одном компьютере. В большинстве случаев на одном компьютере, предоставляющем свои ресурсы пользователям, устанавливают не одну, а несколько программ-серверов. Для этого необходимо отличать отдельные службы приложений при помощи различных точек входа – портов. Каждой программе-серверу присваивается определённый номер порта (то есть идентификатор сетевого процесса), по которой к этой программе-серверу обращается соответствующий клиент.

Поскольку сеть Internet обеспечивает связь со множеством клиентских компьютеров, для наиболее распространенных служб установлены стандартные номера портов, для использования всеми пользователями. Например, служба Telnet связана с портом 23, служба передачи файлов FTP — с портами 20 и 21, служба WWW – с портом 80.

1.4 Способы коммутации

Основным требованием, предъявляемым к общедоступным сетям передачи данных, называемых сетями данных общего пользования, является способность поддержки оборудования от различных производителей, что требует разработки согласованных стандартов на доступ к этим сетям и их использованию. Эти стандарты (имеющие статус рекомендаций серий I и X) регламентируют скорость передачи данных и интерфейс пользователя с такими сетями. Существует два типа сетей

данных общего пользования: сети данных с коммутацией пакетов и сети данных с коммутацией каналов. Для каждого из этих типов разработаны различные стандарты.

В результате любого установления соединения в сети с коммутацией каналов образуется отдельный физический коммуникационный канал, соединяющий аппаратуру вызвавшего и вызванного абонентов и используемый в течение всего сеанса связи исключительно двумя этими абонентами. Использование отдельного физического канала подразумевает одинаковую скорость передачи и приема информации осуществляющими обмен абонентами. Примером сети с коммутацией каналов является коммутируемая телефонная сеть общего пользования.

В сети с коммутацией пакетов никакое физическое соединение не устанавливается, вместо этого сетевое оборудование исходного абонента сначала собирает все подлежащие передаче данные в один или несколько блоков сообщений, которые называются пакетами. Пакеты содержат адреса как исходного, так и приемного сетевого оборудования. Затем сетевое оборудование исходного абонента последовательно передает пакеты своему локальному центру коммутации пакетов (ЦКП). ЦКП при получении пакета запоминает его и исследует находящийся в пакете адрес получателя. Каждый ЦКП содержит справочник маршрутов, определяющий выходные пути каждого сетевого адреса. Таким образом, ЦКП, получив пакет, отправляет его дальше по соответствующему маршруту. По мере того, как каждый пакет поступает в каждый из расположенных вдоль выбранного маршрута ЦКП, его передача осуществляется вперемешку с другими пакетами. После поступления в конечный ЦКП пакеты передаются абоненту-адресату. В отличие от сетей с коммутацией каналов в сети с коммутацией пакетов взаимодействующие абоненты могут работать с различной скоростью, т.к. скорость, с которой данные передаются через интерфейс в сеть, определяется аппаратурой каждого из абонентов независимо.

Сеть с коммутацией каналов не позволяет управлять ошибками и потоком передаваемых данных; следовательно, это должно быть реализовано пользователем. В сети с коммутацией пакетов ЦПК реализуют в каждом звене сложные процедуры управления потоком и ошибками.

1.5 Эталонная модель взаимодействия открытых систем

На основе анализа распределённых информационно-вычислительных систем Международной организацией по стандартизации (ISO) была предложена концепция будущих систем, называемая архитектурой открытых систем.

В соответствии с этой концепцией применительно к распределенным информационно-вычислительным системам создана эталонная модель взаимодействия открытых систем (OSI – Open System Interconnection), на которой основывается взаимодействие различных разработчиков систем и которая дает основу для ввода необходимых междугородных стандартов.

Модель OSI представляет собой эталонную форму описания распределенной информационно-вычислительной среды, ее структуры, входящих в ее состав компонентов, функций информационных ресурсов, а также правил и процедур взаимодействия компонентов среды в процессе функционирования.

Компонентами модели OSI являются:

– системы, соответствующие основным компонентам информационно-вычислительной среды;

– прикладные процессы, характеризующие информационные ресурсы;

– соединения, обеспечивающие обмен информации между прикладными процессами.

Разнообразие функций, выполняемых распределенными информационно-вычислительными средами, привело к необходимости их

иерархического разделения на группы и созданию многоуровневой концепции сети. Согласно этой концепции создан ряд функциональных слоев, называющихся уровнями. Каждый уровень выполняет определенные логические функции и обеспечивает определенный набор услуг для расположенного над ними уровня. Границы между уровнями устанавливаются так, чтобы взаимодействие между соседними уровнями было минимальным, общее количество уровней достаточно небольшим, а изменения, производимые в пределах одного уровня, не требовали бы перестройки соседних уровней.

Совокупность правил взаимодействия объектов одноименных уровней называется протоколом. Правила взаимодействия объектов смежных уровней одной и той же системы определяет межуровневый интерфейс.

Основная идея, заложенная в модель OSI, заключается в том, что каждый уровень добавляет свои сервисные функции к тем, которые уже обеспечены находящимися ниже уровнями. Таким образом, верхний уровень, непосредственно взаимодействующий с приложением конечного пользователя, обеспечен полным набором сервисных функций, предлагаемых всеми нижними уровнями. Верхние уровни сообщают нижним, какие из услуг должны быть вызваны.

В рамках модели OSI было выделены семь уровней, которые имеют следующий смысл.

Уровень 1 – физический, реализует управление каналом связи и организацию дискретного канала, выполняет функции установления соединения, его поддержание и разъединение, преобразование кодов и синхронизацию по битам.

Уровень 2 – канальный, обеспечивает надёжную передачу информации через физический канал, является уровнем управления передачей данных, организует побайтовую синхронизацию и выбор типа канала – проводной, радио, спутниковый.

Уровень 3 – сетевой, обеспечивает сквозную передачу между системами. На этом уровне осуществляется выбор маршрута передачи данных по линиям, связывающим узлы сети.

Уровень 4 – транспортный, реализует процедуры сопряжения абонентов сети с базовой сетью передачи данных, производит разборку и сборку сообщений и транспортировку блоков сообщений от пользователя до пользователя.

Уровень 5 – сеансовый, организует сеансы связи на период взаимодействия процессов. На этом уровне создаются порты для приема и передачи сообщений, происходит синхронизация отдельных событий.

Уровень 6 – представления, обеспечивает представление данных в согласованном синтаксисе (трансляция языков, форматов и кодов, шифрация, сжатие данных, упаковка и т.д.).

Уровень 7 – прикладной, согласует семантику данных, задаёт требования по качеству обслуживания, опознаёт партнёра-пользователя и определяет его доступность в данный момент, выполняет обработку информации, представленной пользователем.

1.6 Топологии локальных сетей

Топология компьютерной сети – это физическое расположение компьютеров сети друг относительно друга и способ соединения их линиями связи. Понятие топологии относится прежде всего к локальным сетям, в которых структуру связей можно легко проследить. Топология определяет требования к оборудованию, тип используемого кабеля, возможные и наиболее удобные методы управления обменом информацией, надежность работы, возможности расширения сети.

Существуют три основных топологии сети:

- шина, при которой все компьютеры параллельно подключаются к одной линии связи и информация от каждого компьютера одновременно передается всем остальным компьютерам (рис. 1.1);

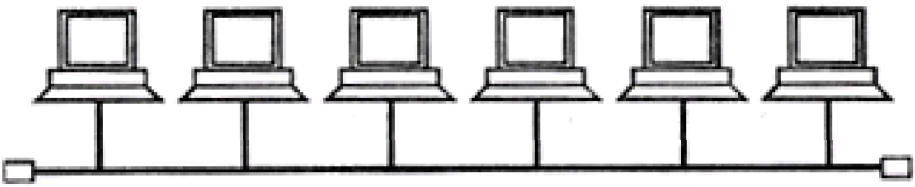

Рис. 1.1. Топология «шина»

- звезда, при которой к одному центральному компьютеру подключаются остальные периферийные компьютеры, каждый из которых использует свою отдельную линию связи (рис. 1.2);

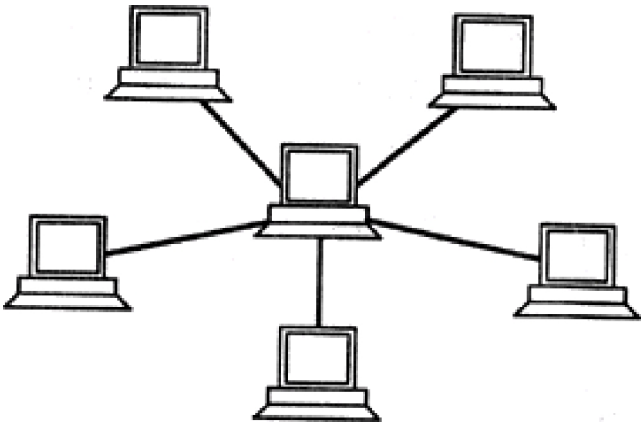

Рис. 1.2. Топология «звезда»

- кольцо, когда каждый компьютер передает информацию всегда только одному компьютеру, следующему за ним в цепочке, а получает информацию только от предыдущего, и эта цепочка замкнута в кольцо (рис. 1.3).

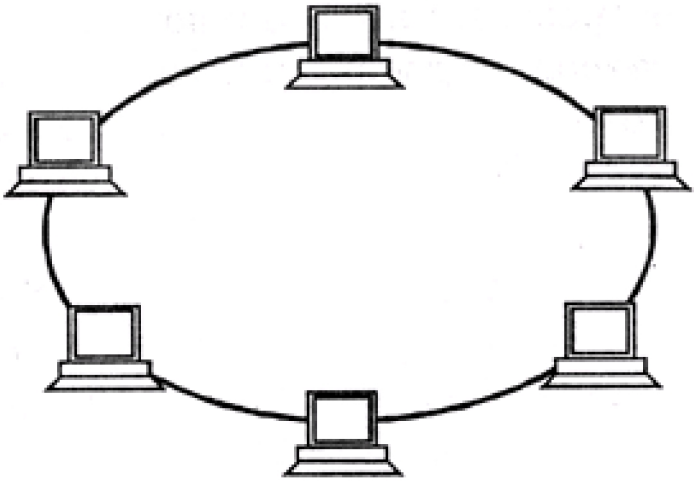

Рис. 1.3. Топология «кольцо»

На практике могут применяться и комбинации базовых топологий, но большинство сетевых стандартов ориентированы именно на эти три.

1.6.1 Топология «шина»

Топология «шина» (или «общая шина») своей структурой предполагает идентичность сетевого оборудования компьютеров и равноправие всех абонентов. При таком соединении компьютеры могут передавать данные только по очереди, так как линия связи единственная, и в противном случае передаваемая информация будет искажаться в результате наложения сигналов, называемого конфликтом или коллизией. Таким образом, в шине реализуется режим полудуплексного обмена информацией (в обоих направлениях, но не одновременно, а по очереди).

В топологии «шина» отсутствует центральный абонент, через которого передается вся информация, что увеличивает ее надежность. До-

бавление новых абонентов в шину довольно просто и обычно возможно во время работы сети. В большинстве случаев при использовании шины требуется минимальное количество соединительного кабеля по сравнению с другими топологиями.

Так как разрешение возможных конфликтов в шине ложится на сетевое оборудование каждого отдельного абонента, аппаратура сетевого адаптера при использовании шинной топологии получается сложнее, чем при других топологиях.

Шине не страшны отказы отдельных компьютеров, так как все остальные компьютеры сети могут нормально продолжать обмен. Может показаться, что шине не страшен и обрыв кабеля, поскольку в этом случае мы получим две вполне работоспособные шины. Однако из-за особенностей распространения электрических сигналов по длинным линиям связи необходимо предусматривать включение на концах шины специальных согласующих устройств – терминаторов. Без включения терминаторов сигнал отражается от конца линии и искажается так, что связь по сети становится невозможной. Так что при разрыве или повреждении кабеля нарушается согласование линии связи и прекращается обмен даже между теми компьютерами, которые остались соединенными между собой. Короткое замыкание в любой точке кабеля шины выводит из строя всю сеть. Любой отказ сетевого оборудования в шине очень трудно локализовать, так как все адаптеры включены параллельно.

При прохождении по линии связи сети с топологией "шина" информационные сигналы ослабляются и никак не восстанавливаются, что накладывает жесткие ограничения на суммарную длину линий связи. Кроме того, каждый абонент может получать из сети сигналы разного уровня в зависимости от расстояния до передающего абонента. Это предъявляет дополнительные требования к приемным узлам сетевого оборудования. Для увеличения длины сети с топологией «шина» часто используют несколько сегментов, каждый из которых представляет

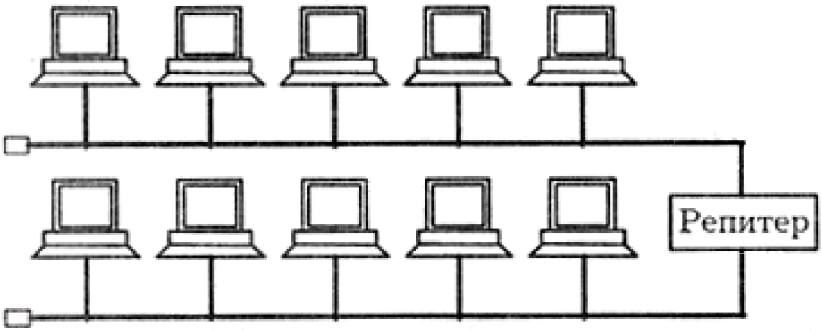

Рис. 1.4. Соединение сегментов сети с помощью повторителя

собой шину, соединенных между собой с помощью специальных восстановителей сигналов – репитеров, или повторителей (рис. 1.4).

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

1.6.2 Топология «звезда»

Топология «звезда» – это топология с явно выделенным центром, к которому подключаются все остальные абоненты. Весь обмен информацией производится исключительно через центральный компьютер, на который таким образом ложится большая нагрузка, поэтому центральный компьютер, как правило, занимается только управлением обменом. Появление конфликтов в сети с топологией «звезда» в принципе невозможно, так как управление полностью централизовано.

Выход из строя периферийного компьютера никак не отражается на функционировании оставшейся части сети, зато любой отказ центрального компьютера делает сеть полностью неработоспособной. Поэтому должны приниматься специальные меры по повышению надежности

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

В отличие от шины в звезде на каждой линии связи находятся только два абонента: центральный и один из периферийных. Чаще всего для их соединения используются две линии связи, каждая из которых передает информацию только в одном направлении. Таким образом, на каждой линии связи имеется только один приемник и один передатчик. Все это существенно упрощает сетевое оборудование по сравнению с шиной и избавляет от необходимости применения дополнительных внешних терминаторов. Проблема затухания сигналов в линии связи также решается в «звезде» проще, чем в «шине», ведь каждый приемник всегда получает сигнал одного уровня.

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

Описанная топология также носит название активной, или истинной, звезды. Существует также топология, называемая пассивной звездой, которая только внешне похожа на звезду.

В центре сети с данной топологией помещается не компьютер, а концентратор, или хаб (hub), выполняющий ту же функцию, что и репитер – он восстанавливает приходящие сигналы и пересылает их в другие линии связи. Хотя схема прокладки кабелей подобна истинной звезде, фактически это шинная топология, так как информация от каж-

дого компьютера одновременно передается ко всем остальным компьютерам, а центрального абонента не существует. Пассивная звезда предоставляет целый ряд дополнительных возможностей, связанных с преимуществами звезды. В связи с этим в настоящее время пассивная звезда распространена гораздо шире, чем активная. Эта топология используется в популярном семействе сетевых стандартов Ethernet.

Важное достоинство звезды (как активной, так и пассивной) состоит в том, что все точки подключения собраны в одном месте. Это позволяет легко контролировать работу сети, локализовать неисправности сети путем простого отключения от центра тех или иных абонентов (что невозможно, например, в случае шины), а также ограничивать доступ посторонних лиц к жизненно важным для сети точкам подключения. К каждому периферийному абоненту в случае звезды может подходить как один кабель (по которому идет передача в обоих направлениях), так и два кабеля (каждый из них передает в одном направлении), причем вторая ситуация встречается чаще.

Недостатком топологии «звезда» является больший, чем при других топологиях, расход кабеля.

1.6.3 Топология «кольцо»

В топологии «кольцо» на каждой линии связи, как и в случае звезды, работает только один передатчик и один приемник. Это позволяет отказаться от применения внешних терминаторов. Важная особенность кольца состоит в том, что каждый компьютер восстанавливает приходящий к нему сигнал, что позволяет бороться с затуханием сигнала в кольце. Выделенного центра в сети с кольцевой топологией нет, все компьютеры могут быть одинаковыми. Однако довольно часто в кольце выделяется специальный абонент, который управляет обменом или контролирует обмен.

Одни из компьютеров сети получают информацию от компьютера, ведущего передачу в данный момент, раньше, а другие – позже. Именно на этой особенности топологии и строятся методы управления обменом по сети, специально рассчитанные на «кольцо». В этих методах право на следующую передачу переходит последовательно к следующему по кругу компьютеру.

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

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

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

1.7 Среды передачи информации

Средой передачи информации называются линии связи (или каналы связи), по которым производится обмен информацией между компью-

терами. В подавляющем большинстве компьютерных сетей (особенно локальных) используются проводные каналы связи, хотя существуют и беспроводные сети.

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

Передача на большие расстояния при любом типе кабеля требует сложной передающей и приемной аппаратуры: необходимо формировать мощный сигнал при передаче и распознавать слабый сигнал приемником. При последовательной передаче для этого требуется всего один передатчик и один приемник. При параллельной же передаче количество передатчиков и приемников возрастает пропорционально разрядности используемого параллельного кода.

При параллельной передаче очень важно, чтобы длины отдельных кабелей были с высокой точностью равны друг другу, иначе в результате прохождения по кабелям разной длины между сигналами на приемном конце образуется временной сдвиг, который может привести к сбоям в работе или даже к полной неработоспособности сети.

В некоторых высокоскоростных локальных сетях все-таки используют параллельную передачу по 2-4 кабелям, что позволяет при заданной скорости передачи применять более дешевые кабели с меньшей полосой пропускания, но допустимая длина кабелей при этом не пре-

вышает сотни метров. Примером может служить спецификация 100BASE-T4 сети Fast Ethernet.

Все выпускаемые кабели можно разделить на три большие группы:

- кабели на основе витых пар проводов (twisted pair);
- коаксиальные кабели (coaxial cable);
- оптоволоконные кабели (fiber optic).

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

1.7.1 Кабели на основе витых пар

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

Обычно в кабель входят две (рис. 1.5) или четыре витые пары.

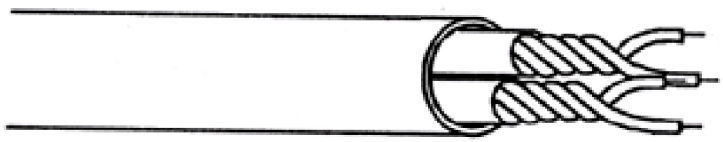

Рис. 1.5. Кабель с витыми парами

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

Кабели на основе витых пар делятся на экранированные (STP – Shielded Twisted Pair) и неэкранированные (UTP – Unshielded Twisted Pair).

В случае экранированной витой пары каждая из витых пар помещается в металлическую оплетку-экран для уменьшения излучений кабеля, защиты от внешних электромагнитных помех и снижения взаимного влияния пар проводов друг на друга. Такое взаимное влияние называется перекрестными наводками. Экранированная витая пара гораздо дороже, чем неэкранированная, а при ее использовании необходимо применять и специальные экранированные разъемы, поэтому встречается она реже, чем неэкранированная витая пара.

Основные достоинства неэкранированных витых пар – гибкость кабеля и простота монтажа разъемов на концах кабеля. Все остальные характеристики у них хуже, чем у других кабелей. Например, при заданной скорости передачи затухание сигнала (уменьшение его уровня по мере прохождения по кабелю) у них больше, чем у коаксиальных кабелей. Помехозащищенность витых пар также невысока, поэтому, линии связи на основе витых пар, как правило, довольно короткие (обычно в пределах 100 метров).

Кабели на основе неэкранированной витой пары (UTP) делятся на несколько категорий:

- Кабель категории 1 – это обычный телефонный кабель (пары проводов не витые), по которому можно передавать только речь, но не

данные. Данный тип кабеля имеет большой разброс параметров (волнового сопротивления, полосы пропускания, перекрестных наводок).

- Кабель категории 2 – это кабель из витых пар для передачи данных в полосе частот до 1 МГц. Кабель не тестируется на уровень перекрестных наводок. Этот тип кабеля практически не используется.
- Кабель категории 3 – это кабель для передачи данных в полосе частот до 16 МГц, состоящий из витых пар с девятью витками проводов на метр длины. Это самый простой тип кабелей, рекомендованный стандартом для локальных сетей.
- Кабель категории 4 – это кабель, передающий данные в полосе частот до 20 МГц. Используется редко, так как не слишком заметно отличается от категории 3. Стандартом рекомендуется вместо кабеля категории 3 переходить сразу на кабель категории 5. Кабель был разработан для работы в сетях по стандарту IEEE 802.5.
- Кабель категории 5 рассчитан на передачу данных в полосе частот до 100 МГц. Состоит из витых пар, имеющих не менее 27 витков на метр длины. Кабель 5 категории рекомендован к применению в сетях типа Fast Ethernet.

Для присоединения витых пар используются разъемы (коннекторы) типа RJ-45, похожие на используемые в телефонах разъемы RJ-11, но несколько большие по размеру и имеющие восемь контактов вместо четырех в случае RJ-11. Присоединяются разъемы к кабелю с помощью специальных обжимных инструментов. При этом золоченые игольчатые контакты разъема прокалывают изоляцию каждого провода, входят между его жилами и обеспечивают надежное и качественное соединение.

Чаще всего витые пары используются для передачи данных в одном направлении, то есть в топологиях типа «звезда» или «кольцо». Топология «шина» обычно ориентируется на коаксиальный кабель. Поэтому

внешние терминаторы, согласующие неподключенные концы кабеля, для витых пар практически никогда не применяются.

Кабели выпускаются с двумя типами внешних оболочек:

- кабель в поливинилхлоридной (ПВХ, PVC) оболочке дешевле и предназначен для работы кабеля в сравнительно комфортных условиях эксплуатации;
- кабель в тефлоновой оболочке дороже и предназначен для более жестких условий эксплуатации.

Кабель в ПВХ-оболочке называют также non-plenum, а кабель в тефлоновой оболочке – plenum. Термин plenum обозначает пространство под фальшполом и над подвесным потолком, где удобно размещать кабели сети. Для прокладки в этих скрытых от глаз пространствах лучше подходит кабель в тефлоновой оболочке.

Еще один важный параметр любого кабеля, который жестко не определяется стандартом, но может существенно повлиять на работоспособность сети, – скорость распространения сигнала в кабеле, то есть задержка распространения сигнала в кабеле в расчете на единицу длины. Производители кабелей иногда указывают величину задержки на метр длины, а иногда — скорость распространения сигнала относительно скорости света (или NVP – Nominal Velocity of Propagation).

Каждый из проводов, входящих в кабель на основе витых пар, как правило, имеет свой цвет изоляции, что существенно облегчает монтаж разъемов, особенно в том случае, когда концы кабеля находятся в разных комнатах и контроль с помощью приборов затруднен.

1.7.2 Коаксиальные кабели

Коаксиальный кабель представляет собой электрический кабель, состоящий из центрального провода и металлической оплетки, разделенных между собой слоем диэлектрика (внутренней изоляции) и помещенных в общую внешнюю оболочку (рис. 1.6).

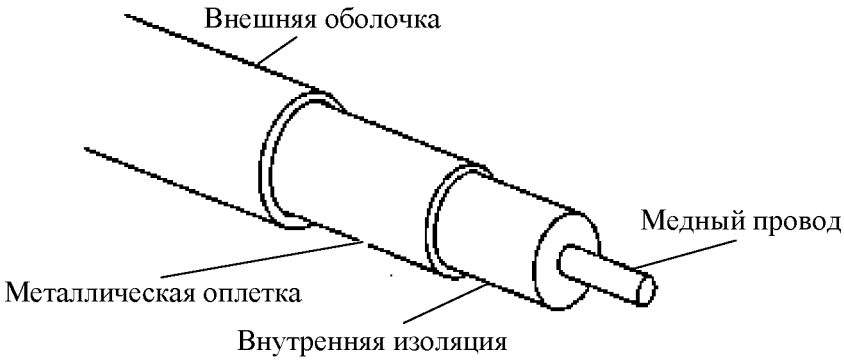

Рис. 1.6. Коаксиальный кабель

В ранних сетевых технологиях коаксиальный кабель был широко распространен, что связано с его высокой помехозащищенностью (благодаря металлической оплетке) и более высокими, чем в случае витой пары, допустимыми скоростями передачи данных и большими допустимыми расстояниями передачи (до километра и выше). К нему труднее механически подключиться для несанкционированного прослушивания сети, он также дает заметно меньше электромагнитных излучений. Однако монтаж и ремонт коаксиального кабеля существенно сложнее, чем витой пары, а стоимость его выше. Сложнее и установка разъемов на концах кабеля. Поэтому его сейчас применяют значительно реже, чем витую пару.

Основное применение коаксиальный кабель находит в сетях с топологией типа «шина». При этом на концах кабеля обязательно должны устанавливаться терминаторы для предотвращения внутренних отражений сигнала, причем один из терминаторов должен быть заземлен. Без заземления металлическая оплетка не защищает сеть от внешних электромагнитных помех и не снижает излучение передаваемой по сети информации во внешнюю среду.

Терминаторы должны быть обязательно согласованы с кабелем, то есть их сопротивление должно быть равно волновому сопротивлению кабеля. Например, если используется 50-омный кабель, для него подходят только 50-омные терминаторы.

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

Существуют два основных типа коаксиального кабеля:

- тонкий кабель, имеющий диаметр ¼ дюйма, более гибкий;
- толстый кабель, имеющий диаметр около ½ дюйма, значительно более жесткий. Он представляет собой классический вариант коаксиального кабеля.

Тонкий кабель используется для передачи на меньшие расстояния, чем толстый, так как в нем сигнал затухает сильнее. В то же время тонкий кабель можно оперативно проложить к каждому компьютеру, а толстый требует жесткой фиксации помещения. Подключение к тонкому кабелю проще и не требует дополнительного оборудования, а для подключения к толстому кабелю надо использовать специальные довольно дорогие устройства, прокалывающие его оболочки и устанавливающие контакт как с центральной жилой, так и с экраном. Толстый кабель примерно вдвое дороже, чем тонкий. Поэтому тонкий кабель применяется гораздо чаще.

Как и в случае витых пар важным параметром коаксиального кабеля является тип его внешней оболочки. Как и в случае витой пары применяются кабели в поливинилхлоридной и тефлоновой оболочках. Естественно, тефлоновый кабель дороже поливинилхлоридного. В настоящее время считается, что коаксиальный кабель устарел, в большинстве случаев его вполне может заменить витая пара или оптоволоконный кабель.

1.7.3 Оптоволоконные кабели

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

Структура оптоволоконного кабеля похожа на структуру коаксиального электрического кабеля (рис. 1.7), но вместо центрального медного провода здесь используется тонкое (диаметром порядка 1–10 мкм) стекловолокно, а вместо внутренней изоляции – стеклянная или пластиковая оболочка, не позволяющая свету выходить за пределы стекловолокна. Металлическая оплетка кабеля обычно отсутствует, так как экранирование от внешних электромагнитных помех здесь не требуется, однако иногда ее все-таки применяют для механической защиты от окружающей среды.

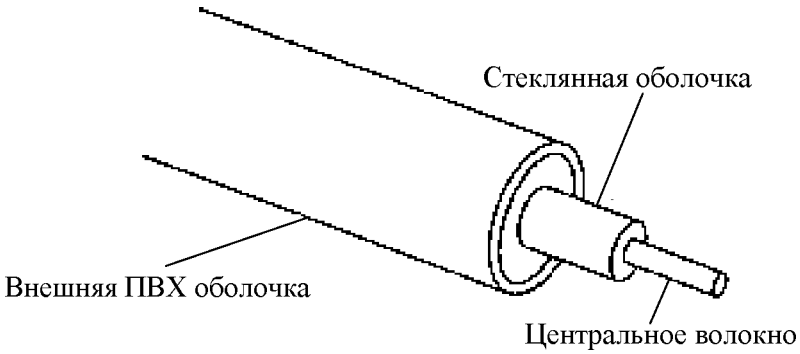

Рис. 1.7. Структура оптоволоконного кабеля

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

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

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

Оптоволоконный кабель менее прочен, чем электрический, и менее гибок (типичная величина допустимого радиуса изгиба составляет около 10—20 см). Чувствителен он и к ионизирующим излучениям, из-за которых снижается прозрачность стекловолокна, то есть увеличивается затухание сигнала, а также к резким перепадам температуры, в результате которых стекловолокно может треснуть.

Применяют оптоволоконный кабель в сетях с топологией «звезда» и «кольцо».

Существуют два типа оптоволоконных кабелей:

- многомодовый кабель, более дешевый;
- одномодовый кабель, более дорогой, но имеющий лучшие характеристики.

Основные различия между этими типами связаны с разными режимами прохождения световых лучей в кабеле.

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

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

1.8 Аналоговые каналы передачи данных. Способы модуляции

Типичным и наиболее распространенным типом аналоговых каналов являются телефонные каналы общего пользования (каналы тональной частоты). Для передачи дискретной информации по каналам тональной частоты необходимы устройства преобразования сигналов, согласующие характеристики дискретных сигналов и аналоговых линий.

Согласование параметров сигналов и среды при использовании аналоговых каналов осуществляется с помощью воплощения сигнала, выражающего передаваемое сообщение, в некотором процессе, называемом переносчиком и приспособленном к реализации в данной среде. Переносчик в системах связи представлен электромагнитными колебаниями U некоторой частоты, называемой несущей частотой:

$$U = U_{\text{m}} \cdot \sin(\nu t + y),$$

где U_{m} – амплитуда, ν – частота, y – фаза колебаний. Изменение параметров несущей по закону передаваемого сообщения называется модуляцией. Если это изменение относится к амплитуде U_{m}, то модуляцию называют амплитудной (АМ), если к частоте ν – частотной (ЧМ), и если к фазе y – фазовой (ФМ). Существуют и другие способы модуляции, например, квадратурно-амплитудная модуляция, основанная на передаче одним элементом модулированного сигнала n бит информации, где n = 4...8 (т.е. используются 16... 256 дискретных значений амплитуды). Однако для надежного различения этих значений амплитуды требуется малый уровень помех.

При приеме сообщения предусматривается обратная процедура извлечения полезного сигнала из переносчика, называемая демодуляцией. Модуляция и демодуляция выполняются в устройстве, называемом модемом.

1.9 Методы доступа к среде передачи информации

Метод доступа является способом определения того, какая из рабочих станций сможет следующей использовать ЛВС. То, как сеть управляет доступом к каналу связи, существенно влияет на ее характеристики. К наиболее распространенным методам доступа относятся:

– множественный доступ с передачей полномочия, или метод с передачей маркера;

– множественный доступ с разделением во времени;

– множественный доступ с разделением частоты;

– случайный доступ, развитием которого является множественный доступ с контролем несущей и обнаружением конфликтов.

1.9.1 Множественный доступ с передачей полномочия

Метод с передачей полномочия, или маркера (Token Passing Multiple Access – TPMA), – это метод доступа к среде, в котором от рабочей станции к рабочей станции передается маркер, дающий разрешение на передачу сообщения. При получении маркера рабочая станция может передавать сообщение, присоединяя его к маркеру, который переносит это сообщение по сети. Каждая станция между передающей станцией и принимающей видит это сообщение, но только станция-адресат принимает его. При этом она создает новый маркер. Маркер, или полномочие, – это уникальная комбинация битов, позволяющая рабочей станции начать передачу данных.

Когда рабочей станции необходимо передать пакет, ее адаптер дожидается поступления маркера, а затем преобразует его в пакет, содержащий данные, отформатированные по протоколу соответствующего уровня, и передает результат далее по сети.

Пакет распространяется по сети от адаптера к адаптеру, пока не найдет своего адресата, который установит в нем определенные биты для подтверждения того, что данные достигли адресата, и ретранслирует его вновь в сеть. После чего пакет возвращается в узел, из которого был отправлен. Здесь после проверки безошибочной передачи пакета узел освобождает сеть, выпуская новый маркер. Таким образом, в сети с передачей маркера невозможны коллизии (конфликты). Метод с передачей маркера в основном используется в кольцевой топологии.

Данный метод характеризуется следующими достоинствами:

– гарантирует определенное время доставки блоков данных в сети;

– дает возможность предоставления различных приоритетов передачи данных.

Вместе с тем он имеет существенные недостатки:

– в сети возможны потеря маркера, а также появление нескольких маркеров, при этом сеть прекращает работу;

– включение и отключение новых рабочих станций связано с изменением адресов всей системы.

1.9.2 Множественный доступ с разделением во времени

Множественный доступ с разделением во времени (Time Division Multiple Access – TDMA) основан на распределении времени работы канала между системами.

Доступ TDMA основан на использовании специального устройства, называемого тактовым генератором. Этот генератор делит время канала на повторяющиеся циклы. Каждый из циклов начинается сигналом-разграничителем. Цикл включает в себя пронумерованные временные интервалы, называемых ячейками. Интервалы предоставляются для загрузки в них блоков данных.

Простейший вариант использования интервалов заключается в том, что их число делается равным количеству абонентских систем, подключенных к рассматриваемому каналу. Тогда во время цикла каждой системе предоставляется один интервал, в течение которого она может передавать данные. При использовании рассмотренного метода доступа часто оказывается, что в одном и том же цикле одним системам нечего передавать, а другим не хватает выделенного времени. В результате пропускная способность канала используется неэффективно.

Более сложный, но высокоэкономичный вариант заключается в том, что система получает интервал только тогда, когда у нее возникает необходимость в передаче данных, например при асинхронном способе передачи. Для передачи данных система может в каждом цикле получать интервал с одним и тем же номером. В этом случае передаваемые системой блоки данных появляются через одинаковые промежутки времени и приходят с одним и тем же временем запаздывания. Этот способ особенно удобен при передаче речи.

1.9.3 Множественный доступ с разделением частоты

Множественный доступ с разделением частоты (Frequency Division Multiple Access – FDMA) основан на разделении полосы пропускания канала на группу полос частот, образующих логические каналы.

Широкая полоса пропускания канала делится на ряд узких полос, разделенных защитными полосами. Размеры узких полос могут быть различными.

Передаваемые по логическим каналам сигналы накладываются на разные несущие и поэтому в частотной области не должны пересекаться. Вместе с этим, иногда, несмотря на наличие защитных полос, спектральные составляющие сигнала могут выходить за границы логического канала и вызывать шум в соседнем логическом канале.

В оптических каналах разделение частоты осуществляется направлением в каждый из них лучей света с различными частотами. Благодаря этому пропускная способность физического канала увеличивается в несколько раз. При осуществлении этого мультиплексирования в один световод излучает свет большое число лазеров (на различных частотах). Через световод излучение каждого из них проходит независимо от другого. На приемном конце разделение частот сигналов, прошедших физический канал, осуществляется путем фильтрации выходных сигналов.

Метод доступа FDMA относительно прост, но для его реализации необходимы передатчики и приемники, работающие на различных частотах.

1.9.4 Множественный доступ с контролем несущей и обнаружением конфликтов

Метод множественного доступа с прослушиванием несущей и обнаружением конфликтов (CSMA/CD – Carrier Sense Multiple Access with Collision Detection) устанавливает следующий порядок работы сети: если рабочая станция собирается воспользоваться сетью для передачи данных, она сначала должна проверить состояние канала: начинать передачу станция может, если канал свободен. В процессе передачи станция продолжает прослушивание сети для обнаружения возможных конфликтов. Если возникает конфликт из-за того, что два узла попытаются занять канал, то обнаружившая конфликт интерфейсная плата выдает в сеть специальный сигнал (jam-сигнал) и обе станции одновременно прекращают передачу. Назначением jam-сигнала является усиление коллизии. Принимающая станция отбрасывает частично принятое сообщение, а все рабочие станции, желающие передать сообще-

ние, в течение некоторого случайно выбранного промежутка времени выжидают, прежде чем начать сообщение.

Все сетевые интерфейсные платы запрограммированы на разные псевдослучайные промежутки времени. Если конфликт возникнет во время повторной передачи сообщения, этот промежуток времени будет увеличен.

1.10 Кодирование информации в локальных сетях

Кодирование передаваемой по сети информации имеет непосредственное отношение к соотношению максимально допустимой скорости передачи и пропускной способности используемой среды передачи. При использовании различных кодов максимальная скорость передачи по одному и тому же кабелю может отличаться в два раза. Выбор кода влияет также на сложность сетевой аппаратуры и надежность передачи информации.

Код NRZ (Non Return to Zero – без возврата к нулю) – это простейший код, представляющий собой практически обычный цифровой сигнал (рис. 1.8). В коде NRZ допускается изменение полярности на обратную, а также изменение уровней, соответствующих нулю и единице. К несомненным достоинствам кода NRZ относятся его очень простая реализация (исходный сигнал не требуется кодировать на передающем конце и декодировать на приемном), а также минимальная среди других кодов пропускная способность линии связи, требуемая при данной скорости передачи.

Существенным недостатком кода NRZ является возможность потери синхронизации приемником при приеме слишком длинных блоков информации (пакетов). Приемник может привязать момент начала приема только к стартовому биту пакета, а в течение приема пакета вынужден пользоваться только собственным внутренним тактовым гене-

ратором. Если часы приемника расходятся с часами передатчика в ту или иную сторону, то временной сдвиг к концу приема пакета может превысить длительность одного или нескольких бит и в результате произойдет потеря переданных данных. Например, при длине пакета, равной 10000 бит, даже при идеальной передаче формы сигнала по кабелю допустимое расхождение часов приемника и передатчика составит не более 0,01%.

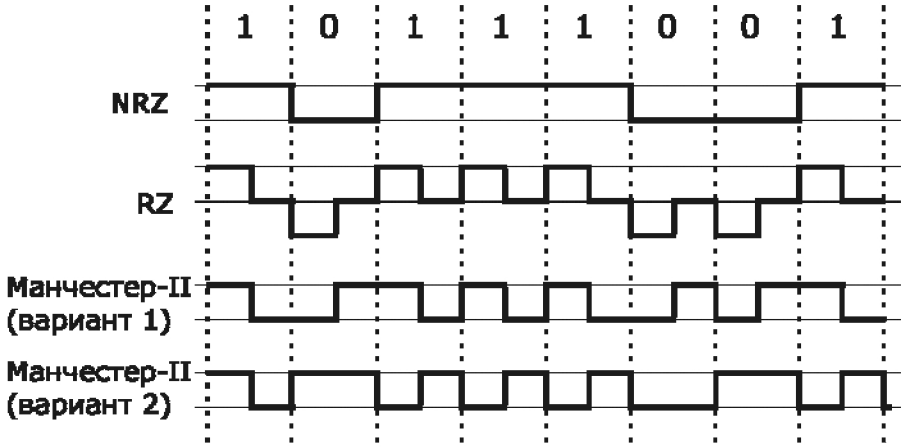

Рис. 1.8. Некоторые коды передачи информации

Во избежание потери синхронизации можно было бы ввести вторую линию связи для передачи синхронизирующего сигнала. Но при этом требуемое количество кабеля, приемников также увеличивается в два раза, что невыгодно при большой длине сети и большом количестве абонентов.

Поэтому код NRZ используется только для передачи короткими пакетами (обычно до 1 Кбита). Для синхронизации начала приема пакета используется стартовый служебный бит, уровень которого отличается от пассивного состояния линии связи (например, если пассивное со-

стояние линии связи при отсутствии передачи равно нулю, то стартовый бит равен единице). Наиболее известным применением кода NRZ является последовательный порт персонального компьютера. Передача информации в нем ведется по 8 бит (т.е. побайтно), сопровождаемыми стартовым и стоповым битами.

Код RZ (Return to Zero – с возвратом к нулю) представляет собой трехуровневый код, получивший такое название из-за того, что после значащего уровня сигнала в первой половине передаваемого бита информации следует возврат к некоему «нулевому» уровню (например, к нулевому потенциалу). Переход к нему происходит в середине каждого бита (см. рис. 1.8).

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

Недостаток кода RZ заключается в том, что для него требуется вдвое большая полоса пропускания канала при той же скорости передачи по сравнению с кодом NRZ: на один бит приходится два изменения уровня напряжения.

Код RZ применяется не только в сетях на основе электрического кабеля, но и в сетях на основе оптоволоконного кабеля. Поскольку в оптоволоконных линиях связи не существует положительных и отрицательных уровней сигнала, используются уровни: отсутствие света, «средний» свет, «сильный» свет. В этом случае, даже когда передача информации не производится, свет все равно присутствует, что позволяет легко определить целостность оптоволоконной линии связи без принятия каких-либо дополнительных мер.

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

Обязательное наличие перехода в центре бита позволяет приемнику кода Манчестер-II легко выделить из пришедшего сигнала синхросигнал, что дает возможность передавать информацию сколь угодно большими пакетами без потерь из-за рассинхронизации. Допустимое расхождение часов приемника и передатчика достигает 25%. Как и в случае кода RZ, пропускная способность линии требуется в два раза выше, чем при использовании простейшего кода NRZ. Код Манчестер-II используется как в электрических, так и в оптоволоконных кабелях (в последнем случае один уровень соответствует отсутствию света, а другой – его наличию).

Если один из уровней сигнала в манчестерском коде нулевой (как, например, в сети Ethernet), то величина постоянной составляющей в течение передачи будет равна примерно половине амплитуды сигнала. Это позволяет легко фиксировать столкновения пакетов в сети (конфликт, коллизию) по отклонению величины постоянной составляющей за установленные пределы.

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

ходимо, например, для определения момента начала и конца принимаемого пакета, а также для предотвращения начала передачи в случае занятости сети (когда передает какой-то другой абонент).

Стандартный манчестерский код имеет несколько вариантов, один из которых показан на рис. 1.8 (вариант 2 манчестерского кода). Этот код используется в сетях Token Ring компании IBM. Принцип данного кода прост: в начале каждого битового интервала сигнал меняет уровень на противоположный предыдущему, а в середине единичных (и только единичных) битовых интервалов уровень изменяется еще раз. Таким образом, в начале битового интервала всегда есть переход, который используется для самосинхронизации.

Разрабатываемые в настоящее время коды должны соблюдать компромисс между требуемой при заданной скорости передачи полосой пропускания канала связи и возможностью самосинхронизации. Обычно для этого в поток передаваемых битов добавляют биты синхронизации, например, один бит синхронизации на 4, 5 или 6 информационных битов или два бита синхронизации на 8 информационных битов. В действительности кодирование не сводится к простой вставке в передаваемые данные дополнительных битов. Группы информационных битов преобразуются в передаваемые по сети группы с количеством битов на один или два больше. Приемник осуществляет обратное преобразование, восстанавливая исходные информационные биты. Довольно просто осуществляется в этом случае и обнаружение несущей частоты (то есть детектирование передачи).

Например, в сети FDDI применяется код 4B/5B, преобразующий 4 информационных бита в 5 передаваемых. При этом синхронизация приемника осуществляется один раз на 4 бита, а не в каждом бите, как в случае манчестерского кода. Коды преобразования подобраны таким образом, чтобы изменение сигнала было как можно более частым независимо от вида передаваемых данных (табл. 1.1).

Таблица 1.1. ***Кодирование в сетях FDDI***

Информационные биты	Передаваемые биты
0000	11110
0001	01001
0010	10100
0011	10101
0100	01010
0101	01011
0110	01110
0111	01111
1000	10010
1001	10011
1010	10110
1011	10111
1100	11010
1101	11011
1110	11100
1111	11101

Требуемая полоса пропускания увеличивается по сравнению с кодом NRZ не в два раза, а всего в 1,25 раза. По тому же принципу строятся и другие коды, например 5B/6B, используемый в сетях 100VG-AnyLAN, или 8B/10B, используемый в сетях Gigabit Ethernet.

В сегменте 100BASE-T4 сетей Fast Ethernet используется код 8B/6T, предусматривающий параллельную передачу трех трехуровневых сигналов по трем витым парам. Это позволяет достичь скорости передачи 100 Мбит/с на дешевых кабелях с витыми парами категории 3. При этом требуется больший расход кабеля и увеличение количества приемников и передатчиков, а кабели должны быть одинаковой длины, чтобы задержки сигнала в них не различались на заметную величину.

1.11 Методы контроля правильности передачи информации

При передаче информации по некачественным каналам связи возможно появление ошибок, то есть искажений передаваемой информа-

ции. Эти ошибки необходимо выявлять и исправлять. Контроль принимаемой информации может быть побайтным и пакетным.

Побайтный метод предполагает, что каждый передаваемый байт дополняется битом четности (или нечетности), то есть в случае, когда количество единиц в передаваемом информационном байте четное, то бит равен 0, а если нечетное – то 1. Метод может применяться как при байтовой, так и при пакетной передаче. Вероятность того, что ошибка не будет обнаружена, довольно велика. К этому может привести наличие четного количества ошибок в информационных битах, а также одновременное искажение информационного и контрольного битов.

Пакетный метод сводится к тому, что в конце каждого передаваемого пакета добавляется контрольная сумма (длиной 8, 16 или 32 бита), которая включает в себя информацию обо всех информационных битах пакета. Метод подсчета контрольной суммы выбирается так, чтобы, с одной стороны, ее просто было вычислить, а с другой стороны, чтобы она достаточно надежно выявляла ошибки. Обычно используются контрольные суммы трех видов.

1. *Сумма по модулю 2 всех байтов (или слов) пакета.* Вычисление идет по правилам: 0 + 0 = 0, 0 + 1 = 1, 1 + 1 = 0. При этом однократные ошибки (то есть одна ошибка на пакет) обнаруживаются с вероятностью 100%, двукратные (две ошибки на пакет) – с вероятностью 7/8 (так как в случае, когда две ошибки попадают в один и тот же разряд, они не могут быть обнаружены). Надо также учесть, что случаются искажения нескольких битов, которые данным методом выявляются довольно плохо. Этот вид контрольной суммы легко и быстро считается программным путем, так как соответствующая команда вычисления суммы по модулю 2 имеется практически у всех микропроцессоров.

2. *Арифметическая сумма всех байтов (или слов) пакета.* При ее вычислении отбрасываются старшие разряды для сохранения заданной разрядности контрольной суммы (обычно 8 или 16). Однократные

ошибки обнаруживаются с вероятностью 100%. Вероятность необнаружения двукратных ошибок в наихудшем случае составляет 1/8 · 1/4 = 1/32. Такая наихудшая ситуация наблюдается, когда в каждом из 8 разрядов всех байт пакета или в каждом из 16 разрядов всех слов пакета присутствует половина логических единиц и половина логических нулей. При этом двукратные ошибки не выявляются, когда в одном разряде один из битов из 0 переходит вследствие ошибки в 1, а другой бит в этом же разряде из 1 переходит в 0, что не изменяет общей суммы.

3. *Циклическая контрольная сумма (или циклический контроль по избыточности, CRC – Cyclic Redundancy Check).* Применение циклической контрольной суммы вызвано стремлением повысить качество контроля, то есть увеличить вероятность обнаружения ошибок. Циклическая контрольная сумма существенно сложнее в вычислении, однако надежность данного метода контроля неизмеримо выше. При вычислении циклической контрольной суммы весь пакет рассматривается как N-разрядное двоичное число, где N – количество бит в пакете. Для вычисления контрольной суммы это число делится по модулю 2 на некоторое постоянное простое число. Частное от этого деления отбрасывается, а остаток используется в качестве контрольной суммы. Данный метод выявляет однократные ошибки с вероятностью 100%, а любое другое количество ошибок с вероятностью $p \approx 1 - 2^{-n}$, где n – количество разрядов контрольной суммы (формула верна при условии, что $N >> n$). Разрядность полинома берется на единицу большая, чем требуемая разрядность контрольной суммы (остатка от деления).

2 АРХИТЕКТУРА TCP/IP

TCP/IP является одним из самых популярных стеков коммуникационных протоколов. Стек TCP/IP появился до появления модели взаимодействия открытых систем, и соответствие уровня стека TCP/IP уровням модели OSI достаточно условно.

Протоколы TCP/IP делятся на 4 уровня. Самый нижний (4 уровень) называется уровнем межсетевых интерфейсов и соответствует физическому и канальному уровням модели OSI. Функции этого уровня включают в себя:

- отображение IP-адресов в физические адреса сети;
- инкапсуляция IP-дейтаграмм в кадры для передачи по физическому каналу и извлечение дейтаграмм из кадров. Контроль безошибочности передачи не требуется;
- определение метода доступа к среде передач;
- определение представления данных в физической среде;
- прием и пересылка кадров.

Этот уровень не регламентируется в протоколах TCP/IP, но поддерживает все популярные стандарты физического и канального уровней.

Третий уровень, называемый уровнем межсетевого взаимодействия, отвечает за передачу дейтаграмм с использованием различных локальных сетей, территориальных сетей и линий специальных связей. Этот уровень соответствует третьему уровню модели OSI. В качестве основного протокола этого уровня используется протокол IP. Протокол IP изначально создавался как протокол передачи пакетов в составных се-

тях, состоящих из большого количества локальных сетей, объединенных между собой. Поэтому протокол IP хорошо работает в сетях со сложной структурой. К третьему уровню также относятся все протоколы, связанные с составлением ими модификации и таблиц с маршрутизацией, т.е. такие протоколы RIP (Routing Internet Protocol), OSPF(Open Shortest Path First) – протоколы сбора маршрутной информации, ICMP (Internet Control Message Protocol) – протокол межсетевых управляющих сообщений.

Протоколы ICMP служат для обеспечения обратной связи, т.е. сообщение об ошибках при передаче, например, между двумя компьютерами, шлюзом и маршрутизатором.

На втором уровне работают протоколы TCP и UDP. Этот уровень называется основным. TCP – протокол управления передачи. UDP – протокол пользовательских дейтаграмм. Протокол TCP обеспечивает устойчивое виртуальное соединение между удаленными сетевыми процессами, а протокол UDP – передачу прикладных пакетов методом дейтаграмм, т.е. без установления соединений. Протокол UDP требует меньше накладных расходов, чем протокол TCP.

Протоколы UDP практически не выполняют никаких особых функций дополнительно к функциям межсетевого уровня. Протокол UDP используется в двух основных случаях:

- при пересылке коротких сообщений, т.е. когда накладные расходы на установление соединения и проверку успешной доставки данных выше расходов на повторную передачу сообщений;
- если сам процесс приложения обеспечивает установление соединения и проверку доставки пакетов (NFS, TFTP, DNS).

Верхний уровень называется прикладным и обеспечивает взаимодействие с пользователем. За время своего использования стек TCP/IP накопил большое количество протоколов и сервисов прикладного уровня: FTP, TFTP, HTTP, SMTP, POP3, Telnet и т.д.

2.1 Протокол IP. Адресация

Функции протокола IP определены в стандарте RFC-791 и заключаются в том, что протокол IP обеспечивает передачу блоков данных, называемых дейтаграммами, от отправителя к получателю, где отправители и получатели являются компьютерами, идентифицируемыми адресами фиксированной длины (IP-адресами). Протокол IP обеспечивает также при необходимости фрагментацию и сборку дейтаграмм для передачи данных через сети с малым размером пакетов.

Протокол IP не подтверждает доставку данных, не контролирует целостность данных и не производит операции обмена служебными сообщениями, подтверждающими установление соединения с узлом назначения и его готовность к приему данных. Протокол IP обрабатывает каждую дейтаграмму как не имеющую связи с другими дейтаграммами сети. После отправки дейтаграммы она никак не контролируется отправителем на уровне протокола IP. Если дейтаграмма не может быть доставлена, то она уничтожается, а узел, уничтоживший дейтаграмму, может отправить отправителю специальное ICMP-сообщение, содержащее информацию о причине сбоя. Гарантию правильной передачи данных предоставляют протоколы вышестоящего уровня. Протоколом IP осуществляется маршрутизация дейтаграмм, т.е. определение пути следования дейтаграммы от одного узла сети к другому на основании адреса получателя.

IP-адрес является некоторым числом, выраженным в двоичной системе. Этот адрес содержит 4 байта или 32 двоичных разряда. Принято каждый байт адресной последовательности записывать в виде десятичного числа.

Каждое из этих чисел содержит определённую адресную информацию: адрес сети и номер хоста.

Существует 5 классов IP-адресов, которые описываются количеством разрядов в сетевом номере и номере хост-ЭВМ. Класс адреса опре-

деляется значением его первого байта. В табл. 2.1 и 2.2 приведены существующие классы IP-адресов и их сравнение.

Т а б л и ц а 2.1. ***Классы IP-адресов***

Разряд адреса	0	1	2	3	4	5	6	7	8 15	16 23	24 31
A	0	номер сети (7 бит)							номер хоста (24 бита)		
B	1	0	номер сети (7 бит)							номер хоста (16 бит)	
C	1	1	0	номер сети (7 бит)							номер хоста (8 бит)
D	1	1	1	0	групповой адрес (28 бит)						
E	1	1	1	1	0	зарезервировано					

Т а б л и ц а 2.2. ***Сравнение классов IP-адресов***

Класс	**Диапазон значений первого байта адреса**	**Возможное количество сетей**	**Максимальное количество хостов в сети**	**Предназначение**
A	1÷126	126	16 777 214	Распределение IP-адресов в зависимости от размеров сетей
B	128÷191	16 382	65 534	
C	192÷223	2 097 150	254	
D	224÷239	-	-	Групповые обращения
E	240÷247	-	-	Зарезервировано

Адреса класса A предназначены для использования в больших сетях, содержащих более чем 2^{16} хост-машин. Адреса класса B предназначены для сетей среднего размера, содержащих от 28 до 216 хост-машин. Адреса класса C применяются в сетях с небольшим количеством ПЭВМ

(до 254), например, в ЛВС. Адреса класса D предназначены для обращения к группам хост-машин. Адреса класса E были зарезервированы на будущее.

В настоящее время международные организации, занимающиеся распределением адресного пространства, отказались от применения классов адресов, так как в случае выделения адресного пространства малым по объёму сетям (16, 32, 64 хоста) слишком много адресного пространства расходуется впустую.

Рассмотрим некоторые особенности адресации в Internet.

Согласно принятому в Internet правилу хост-ЭВМ нельзя присваивать номер 0 (он описывает всю сеть в целом) и 255 — адрес широковещательной передачи. Кроме того, IP-адрес, первый байт которого равен 127, используется для тестирования программ и взаимодействия процессов в рамках одной хост-ЭВМ, поэтому запрещается присваивать хостам номера, начинающиеся со 127.

Помимо этого существует ряд адресов, которые используются для организации частных сетей, то есть локальных сетей, осуществляющих обмен данными по протоколам TCP/IP. Применение таких адресов также позволяет легко интегрировать подобную локальную сеть в Internet при помощи только одного «реального» IP-адреса, выделенного маршрутизатору сети. Все пакеты, проходящие через этот маршрутизатор, автоматически получают в качестве адреса отправителя адрес маршрутизатора и, таким образом, могут быть корректно обработаны другими маршрутизаторами сети. При этом маршрутизатор, занимающийся преобразованием адресов, ведёт специальную таблицу, в которой записывается с какого адреса «внутренней» сети на какой адрес «внешней» сети был послан запрос (а также ряд других сведений). При получении от «внешнего» сервера ответа (пакета с некоторыми данными), маршрутизатор сверяется с таблицей и если находит тот адрес, который запросил пакет, то перенаправляет его получателю. В противном случае пакет уничтожается и противоположная сторона информируется об

этом по протоколу ICMP. Данный подход может быть также полезен для защиты от несанкционированного доступа как «снаружи» сети, так и «изнутри» (имеется в виду несанкционированная передача некой информации из сети «наружу»). В соответствии с RFC 1918 это диапазоны 10.0.0.0 ÷ 10.255.255.255, 172.16.0.0 ÷ 172.31.255.255 и 192.168.0.0 ÷ 192.168.255.255.

2.2 Доменная система адресов

На начальном этапе создания сети Internet составлялся полный список, куда включались имена всех хостов, подключаемых к сети. Однако вследствие развития Internet, а также частого изменения её топологии, оказалось невозможным постоянно обновлять такой список. Это привело к созданию доменной системы адресов (имён): DNS (Domain Name System). Эта система адресации разделяет все адреса по иерархическому принципу, объединяя их в домены (от английского domain – область). Каждый домен представляет определённую группу хостов, объединенных по географическому или тематическому признаку. Полный доменный адрес обозначается как FQDN (Fully Qualified Domain Name) и читается в обратном порядке относительно цифрового адреса: если IP-адрес начинается с номера сети, то доменный адрес начинается с имени хост-машины. Например, адрес вида

hostname.lab.university.ru

означает: хост hostname сети lab, входящей в домен university, который, в свою очередь, входит в состав домена верхнего (первого) уровня ru. Домен ru означает Российскую Федерацию. Существуют домены верхнего уровня, выделенные по географическим и тематическим признакам:

- arpa – обратный (reverse) DNS;
- com – коммерческие организации;

- edu – образовательные учреждения и университеты;
- gov – невоенные правительственные учреждения;
- info – информационные ресурсы;
- mil – военные правительственные учреждения;
- net – сети (крупные сети, входящие в сеть Интернет);
- org – некоммерческие организации;
- двухбуквенные обозначения стран (ru, uk, cn и т.д.).

Для обработки траектории поиска в отдельных доменах имеются специальные серверы имен, которые обеспечивают преобразование адресов доменной системы имен в цифровую.

Возможны случаи, когда один IP-адрес соответствует двум доменным именам. Это характерно, например, для web-серверов, предоставляющих услуги хостинга. В некоторых случаях несколько IP-адресов могут ассоциироваться с одним доменным именем. Однако наличие доменного имени не является обязательным в отличие от цифрового IP-адреса, без которого хост-машина не может подключиться к сети.

2.3 Бесклассовая модель

Предположим, что требуется подключить к сети Интернет сеть, состоящую из 2000 компьютеров. Для получения адресного пространства требуется либо 8 сетей класса С, либо одна сеть класса В. Использование одной сети класса В нерационально, т.к. она вмещает 65534 адреса. В свою очередь при использовании 8 сетей класса С каждая такая IP сеть должна быть представлена отдельной строкой в таблице маршрутов на маршрутизаторах, т.к. эти 8 сетей с точки зрения маршрутизаторов никак не связаны между собой, хотя сети находятся в одной локальной сети и маршрут к ним одинаковый.

Таким образом, за счет экономии адресного пространства многократно увеличивается служебный трафик в сети, затраты по поддержа-

нию и обработке маршрутных таблиц. Однако нет причин проводить границу между сетью и хостом в IP-адрес по границе байта. Если выбрать длину сетевой части 21 бит, а на номер хоста отвести оставшиеся 11, то получится сеть, адресное пространство которой включает в себя 2046 IP-адресов, что максимально точно соответствует поставленному требованию. В результате получится одна сеть, определяемая своим уникальным 21-битным номером, и, следовательно, для ее обслуживания потребуется только одна запись в таблице маршрутов. В случае адресации вне классов с произвольным положением границы между сетью и хостом внутри IP-адреса к IP-адресу прилагается 32-битная маска, которую называют маской сети или маской подсети. Сетевая маска получается следующим образом: на позициях, соответствующих номеру сети, биты равны 1, а на позициях, соответствующих номеру хоста, биты равны 0.

Для удобства записи IP-адрес бесклассовой модели часто представляется в виде a.b.c.d/n, где a.b.c.d – это IP-адрес, а n – количество бит в сетевой части. Например, для IP-адреса 89.186.244.16/23 маска подсети равна

$$11111111.1111111.11111110.00000000_2 = 255.255.254.0$$

Такая модель адресации называется бесклассовой (CIDR – Classless Internet Direct Routing). В настоящее время классовая модель считается устаревшей и маршрутизация осуществляется по бесклассовой модели.

2.4 Протокол TCP

Протокол TCP (Transmission Control Protocol) обеспечивает сквозную доставку данных между прикладными процессами, запущенными на узлах, взаимодействующих по сети. Описание протокола TCP содержится в стандарте RFC-793. TCP является надежным байт-ориентированным протоколом, устанавливающим соединение. Прото-

кол TCP находится между протоколом IP и собственно приложением. Протокол IP обеспечивает пересылку дейтаграмм по сети, но не гарантирует доставку, целостность, порядок прибытия информации. Эти задачи возложены на протокол TCP.

При получении IP-дейтаграммы, в поле Protocol которой указан код протокола TCP (6), модуль IP передает данные этой дейтаграммы модулю TCP. Эти данные представляют собой TCP-сегмент, содержащий TCP-заголовок и данные пользователя. Модуль TCP анализирует служебную информацию заголовка, определяет, какому именно процессу предназначены данные пользователя, проверяет целостность и порядок прихода данных и подтверждает их прием другой стороне. По мере получения правильной последовательности неискаженных данных пользователя они передаются прикладному процессу.

Основными функциями TCP являются:

1. Базовая передача данных.

TCP выполняет передачу потоков данных между своими клиентами в обоих направлениях. Клиенты TCP – это прикладные процессы, вызывающие модуль TCP при необходимости получить или отправить данные процессу-клиенту на другом узле.

2. Обеспечение достоверности.

Модуль TCP обеспечивает защиту от повреждения, потери, дублирования и нарушения очередности получения данных. Для выполнения этих задач все октеты в потоке данных сквозным образом пронумерованы в возрастающем порядке. Заголовок каждого сегмента содержит число октетов данных в сегменте и порядковый номер первого октета той части потока данных, которая пересылается в данном сегменте. Номер первого байта в потоке определяется на этапе установления соединения. Для каждого сегмента вычисляется контрольная сумма, позволяющая обнаружить повреждение данных.

При удачном приеме октета данных принимающий модуль посылает отправителю подтверждение о приеме – номер удачно принятого

октета. Если в течение некоторого времени отправитель не получит подтверждения, считается, что октет не дошел или был поврежден, и он посылается снова. Этот механизм контроля надежности называется PAR (Positive Acknowledgment with Retransmission). В действительности подтверждение посылается не для одного октета, а для некоторого числа последовательных октетов.

Нумерация октетов используется также для упорядочения данных в порядке очередности и обнаружения дубликатов (которые могут быть посланы из-за большой задержки при передаче подтверждения или потери подтверждения).

3. Разделение каналов.

Протокол TCP обеспечивает работу нескольких соединений одновременно. Каждый прикладной процесс идентифицируется номером порта; заголовок TCP-сегмента содержит номера портов процесса-отправителя и процесса-получателя. При получении сегмента модуль TCP извлекает номер порта и перенаправляет данные соответствующему процессу.

Наиболее распространенные сервисы сети Internet имеют свои стандартные номера портов, например 80 – WWW, 21 – FTP, и т.д.

Совокупность IP-адреса и номера порта называется сокетом. Сокет уникальным образом идентифицирует прикладной процесс в сети Internet. Сокет обычно записывают как a.b.c.d:n, где a.b.c.d – IP-адрес, n – номер порта.

4. Управление соединением.

Соединение – это совокупность информации о состоянии потоков данных, включающая в себя сокеты, номера отправленных, принятых и подтвержденных октетов, а также размеры окон. Каждое соединение в сети Интернет уникально идентифицируется парой сокетов.

Различают два типа открытия соединения: активное и пассивное. При активном открытии TCP-модуль начинает процедуру установления соединения с указанным сокетом, при пассивном – ожидает, что уда-

ленный TCP-модуль начнет процедуру установления соединения с указанного сокета. Указание 0.0.0.0:0 в качестве сокета при пассивном открытии означает, что ожидается соединение с любого сокета. Такой способ применяется в серверных приложениях сети Интернет (почтовые, web- и ftp-серверы), которые ждут установления соединения от клиента. Клиент же применяет процедуру активного открытия; сокет при этом формируется из IP-адреса сервера и стандартного номера порта для данного сервиса.

5. Управление потоком данных.

Для ускорения и оптимизации процесса передачи больших объемов данных протокол TCP применяет метод управления потоком, называемый методом скользящего окна, который позволяет отправителю посылать очередной сегмент, не дожидаясь подтверждения о получении в пункте назначения предыдущего сегмента. Размер окна выбирается таким образом, чтобы подтверждения приходили вовремя и не происходила остановка передачи. Размер окна может динамически изменяться получателем.

Для временной остановки посылки данных без разрыва соединения достаточно объявить нулевое окно. Но даже и в этом случае через определенные промежутки времени будут отправляться сегменты с одним октетом данных. Это делается для того, чтобы отправитель гарантированно узнал о том, что получатель вновь объявил ненулевое окно, поскольку получатель обязан подтвердить получение «пробных» сегментов, а в этих подтверждениях он укажет также и текущий размер своего окна.

Модуль TCP может использовать алгоритм «медленного старта», формируя при установлении соединения окно перегрузки, размер которого изначально равен размеру одного сегмента. Это окно показывает, сколько сегментов TCP-модуль, с его собственной точки зрения, может отправить без получения подтверждения. Скользящее же окно показывает, какой объем неподтвержденных данных модулю разрешено от-

править с точки зрения удаленного модуля, получателя его данных. После прихода подтверждения от получателя окно перегрузки увеличивается на один сегмент и отправитель может выслать уже два сегмента, не дожидаясь подтверждения. Такой подход позволяет постепенно увеличивать нагрузку на сеть. Если окно перегрузки становится больше скользящего окна, объявляемого получателем, ограничение на передачу неподтвержденных данных устанавливает уже скользящее окно получателя.

В случае, если никакие данные приложениями не передаются, а соединение открыто, модуль TCP может периодически посылать сегменты для выяснения того, не отключилась ли другая сторона без уведомления партнера.

TCP-сегмент состоит из заголовка и данных.

Заголовок сегмента состоит из 32-разрядных слов и имеет переменную длину, зависящую от размера поля Options, но всегда кратную 32 битам. За заголовком непосредственно следуют данные – часть потока данных пользователя, передаваемая в данном сегменте. Формат TCP-заголовка приведен на рис. 2.1.

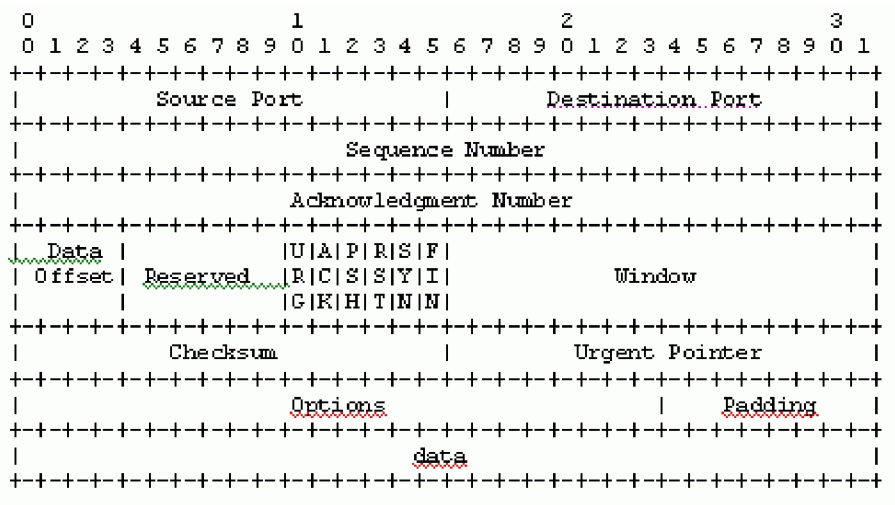

Рис. 2.1. Формат TCP-заголовка

Значения полей заголовка следующие.

Source Port, Destination Port – номера портов процесса-отправителя и процесса-получателя.

Sequence Number (SN) (32 бита) – порядковый номер первого октета в поле данных сегмента среди всех октетов потока данных для текущего соединения. Если в заголовке сегмента установлен бит SYN (фаза установления соединения), то в поле SN записывается начальный номер (ISN), например, 0. Номер первого октета данных, посылаемых после завершения фазы установления соединения, равен ISN+1.

Acknowledgment Number (ACK) (32 бита) – если установлен бит ACK, то это поле содержит порядковый номер октета, который отправитель данного сегмента желает получить. Это означает, что все предыдущие октеты (с номерами от ISN+1 до ACK-1 включительно) были успешно получены.

Data Offset – длина TCP-заголовка в 32-битных словах.

Reserved – поле зарезервировано, заполняется нулями.

Control Bits – управляющие биты.

Флаг URG – поле срочного указателя задействовано.

Флаг ACK – поле номера подтверждения (Acknowledgment Number) задействовано.

PSH – осуществить "проталкивание" – если модуль TCP получает сегмент с установленным флагом PSH, то он немедленно передает все данные из буфера приема процессу-получателю для обработки, даже если буфер не был заполнен.

RST – перезагрузка текущего соединения.

SYN – запрос на установление соединения.

FIN – нет больше данных для передачи.

Window – размер окна в октетах.

Checksum – контрольная сумма.

Urgent Pointer – используется для указания длины срочных данных, которые размещаются в начале поля данных сегмента. Указывает сме-

щение октета, следующего за срочными данными, относительно первого октета в сегменте. Протокол TCP не определяет, как именно должны обрабатываться срочные данные, но предполагает, что прикладной процесс будет предпринимать усилия для их быстрой обработки. Поле Urgent Pointer задействовано, если установлен флаг URG.

Options – поле переменной длины; может отсутствовать или содержать одну опцию или список опций, реализующих дополнительные услуги протокола TCP.

Padding – выравнивание заголовка по границе 32-битного слова, если список опций занимает нецелое число 32-битных слов. Поле Padding заполняется нулями.

2.5 Протокол UDP

Данный протокол иногда называют протоколом ненадёжной доставки. Этот протокол предоставляет прикладным процессам транспортные услуги, которые немногим отличаются от услуг протокола IP (сетевого уровня).

Протокол UDP обеспечивает только доставку дейтаграммы и не гарантирует её выполнение. Протокол не поддерживает виртуального соединения с удалённым модулем UDP. Основное достоинство – простота.

UDP-заголовок состоит из двух 32-битных слов и содержит следующие поля: «порт источника» указывает порт процесса источника, куда может быть адресован ответ на данное сообщение. «порт получателя» является частью межсетевого адреса. В поле «длина» указывается размер данной дейтаграммы с учётом длины заголовка в байтах. Поле «контрольная сумма» обеспечивает контроль правильности данных в заголовке.

За заголовком UDP-пакета следуют пользовательские данные. Протокол UDP рассматривает эти данные как целостное сообщение, т.е.

никогда не разбивает его для передачи в нескольких пакетах и никогда не объединяет несколько сообщений для передачи в одном пакете. При получении пакетов модуль UDP проверяет контрольную сумму и в случае удачной проверки передает содержимое сообщения прикладному процессу, номер порта которого указан в заголовке. В случае, если проверка контрольной суммы выявила ошибку или процесса с указательным номером порта не существует, то UDP-пакет игнорируется. Если UDP-пакеты поступают быстрее, чем модуль UDP успевает их обработать, то они также игнорируются.

Протокол UDP не имеет никаких средств для подтверждения безошибочного приема данных или получения сообщений об ошибке, не обеспечивает поступление сообщений в порядке их отправки, не производит предварительные установления сеанса связи между прикладными процессами и поэтому является ненадежным протоколом без установления соединения. Если приложение нуждается в этих услугах, то оно должно использовать протокол TCP. Максимальная длина передаваемого по протоколу UDP сообщения равна максимальной длине IP-дейтаграммы (64 Кб) за вычетом IP-заголовка минимальной длины (20 байт) и UDP-заголовка (8 байт). Таким образом, максимальная длина передаваемого с использованием протокола UDP сообщения равна 65507 байтам. Обычно используются UDP-сообщения длиной 8 Кб. Протокол UDP использует в таких прикладных процессах, как NFS, TFTP, SNMP, DNS.

2.6 Маршрутизация

В архитектуре TCP/IP сети соединяются друг с другом коммутаторами IP-пакетов, которые называются шлюзами или IP-маршрутизаторами. Основная задача IP-маршрутизатора — определение по специальному алгоритму адреса следующего IP-маршрутизатора. Для реше-

ния этой задачи каждый IP-маршрутизатор должен располагать матрицей маршрутов (специальной базой данных, обеспечивающей маршрутизацию), которую необходимо регулярно обновлять. Это связано с тем, что в сети Интернет используется дейтаграммный режим коммутации пакетов, и пакеты одного сообщения могут доставляться различными маршрутами, причём для каждого пакета должен выбираться маршрут, оптимальный для ситуации, сложившейся в данный момент на сети.

Алгоритм маршрутизации является тем фундаментом, на котором строится вся работа базовой сети с архитектурой TCP/IP. Неожиданные изменения в связности базовой сети должны рассматриваться как обычные явления и соответствующим образом обрабатываться, так же как и перегрузки отдельных направлений и каналов. Существует ряд свойств, которые считаются необходимыми для приемлемого алгоритма маршрутизации:

– алгоритм маршрутизации должен распознавать отказ и восстановление каналов связи или других IP-маршрутизаторов и переключаться на другие, подходящие маршруты, причём время переключения маршрутов должно быть меньшим, чем типичный тайм-аут пользователя протокола TCP (около 1 минуты);

– алгоритм должен исключать образование циклов в назначаемых маршрутах как между соседними, так и между удаленными маршрутизаторами, а время существование циклов в случае их возникновения не должно превышать типичного тайм-аута пользователя протокола TCP (примерно 1 минута);

– нагрузка, создаваемая управляющими сообщениями, необходимыми для работы алгоритма маршрутизации, не должна ощутимо сказываться на нормальной работе сети. Изменение состояния сети, которое может прервать нормальную работу в некоторой локальной области сети, не должно оказывать воздействия на удалённые участки;

– использование маршрутов по умолчанию, вводимых обычно как средство сокращения размеров базы данных по маршрутизации, должно быть ограничено, так как наличие маршрутов по умолчанию может вызвать множество проблем, связанных с возможностью появления циклов и ошибочных конфигураций.

Маршрутизатор должен обеспечивать эффективное распределение собственных ресурсов как по пропускной способности каналов, так и по объёму буферных запоминающих устройств, используемых для хранения ожидающих передачу пакетов. Например, нельзя допустить, чтобы высокоскоростной канал захватил весь объём буферных запоминающих устройств, ничего не оставив низкоскоростному каналу. Маршрутизатор может назначить больший приоритет IP-пакетам, передающим управляющую или служебную информацию.

Наконец, алгоритм маршрутизации должен обеспечивать надёжный алгоритм определения состояния каждого канала связи и узла в базовой сети и, если требуется, состояние хостов сети.

По техническим, административным, географическим, а также иногда и политическим соображениям IP-маршрутизаторы группируются в так называемые автономные системы. Маршрутизаторы, входящие в одну автономную систему, контролируются одной организацией, обеспечивающей их сопровождение, и используют общие для данной автономной системы алгоритмы маршрутизации.

Конкретный вариант протокола маршрутизации, действующий внутри одной автономной системы, называется внутренним протоколом маршрутизации (IGP — Interior Gateway Protocol).

Возможно, что некоторому IP-пакету, чтобы достичь места назначения, придётся пройти через ЦКП двух или более автономных систем. Поэтому автономные системы должны иметь возможность обмениваться информацией о своём состоянии.

Протокол для обмена служебной информацией между автономными системами называется внешним протоколом маршрутизации (EGP — Exterior Gateway Protocol).

IP-маршрутизатору необходима реализация некоторого алгоритма выбора маршрута по таблице маршрутизации, а также алгоритма обновления этой таблицы.

Процедура выбора пути заложена в протоколе IP, причём IP-уровень не знает всего пути, а владеет лишь информацией о том, какому маршрутизатору передать IP-пакет с конкретным адресом места назначения.

Просмотр маршрутной таблицы происходит в три этапа:

– На первом производится поиск соответствия адреса, записанного в IP-пакете, адресу места назначения в маршрутной таблице. В случае успеха пакет посылается соответствующему маршрутизатору или непосредственно хосту.

– На втором ищется соответствие адреса, записанного в IP-пакете, адресу некоторой региональной сети места назначения. Одна запись в таблице маршрутизации соответствует всем хостам, входящим в данную региональную сеть. В случае успеха пакет посылается соответствующему маршрутизатору.

– Ищется маршрут «по умолчанию». Если таковой предусмотрен, дейтаграмма посылается в соответствующий маршрутизатор.

Существуют статические и динамические алгоритмы маршрутизации.

Статический алгоритм есть способ маршрутизации, не изменяющийся при изменении топологии и состояния сети. Простая маршрутизация обеспечивается разными алгоритмами, типичными из которых являются алгоритмы случайной и лавинной маршрутизации. Случайная маршрутизация — передача данных из узла в любом, случайным образом выбранном направлении, кроме направления, по которому данные

поступили в узел. Данные, передаваемые по сети, с конечной вероятностью когда-либо достигают адресата. Лавинная маршрутизация — передача данных из узла во всех направлениях, кроме того, по которому поступили данные. Очевидно, что хотя бы одно направление обеспечит доставку пакета за минимальное время, т.е. лавинная маршрутизация гарантирует малое время доставки.

Шлюзы, входящие в состав одной автономной системы, могут работать по алгоритмам динамической маршрутизации. Наиболее известными из них являются протоколы на основе алгоритма Беллмана-Форда и протоколы на основе алгоритма Дейкстры. Шлюзы, работающие по алгоритму Беллмана-Форда, хранят вектор длин кратчайших маршрутов до всех сетей, входящих в состав объединённой сети. Периодически каждый шлюз передаёт свой вектор соседним шлюзам автономной системы, а элементы вектора, принятого от соседнего шлюза, складываются с длинами исходящих линий связи. На основе полученной таблицы строится новый вектор длин кратчайших маршрутов.

Протоколы на основе алгоритма Беллмана-Форда достаточно просто реализуются, требуют мало памяти и процессорного времени, однако они обладают рядом общих недостатков. При увеличении количества сетей, входящих в состав автономной системы, резко возрастает количество передаваемой информации, т.к. алгоритм требует, чтобы все шлюзы периодически передавали свои векторы длин маршрутов.

Шлюзы, работающие по алгоритму Дейкстры (или SPF-алгоритм – Shortest Path First), сначала определяют кратчайшие маршруты по всем сетям автономной системы. Для этого в каждом шлюзе строится полное дерево кратчайших путей с корнем в данном шлюзе. Процедура построения дерева кратчайших путей использует принцип, согласно которому в дерево кратчайших путей первой включается дуга с наименьшей длиной. После того, как в шлюзе построено дерево кратчайших путей, изменения характеристик линий связи, определяющих длины соответствующих дуг графа, изменения топологии сети приводят к небольшим

дополнительным вычислениям для корректирования дерева кратчайших путей. Шлюзы обмениваются только сведениями о длинах исходящих линий связи, а не векторами длин маршрутов, как в случае алгоритма Беллмана-Форда. Размер корректирующих пакетов со служебной информацией для маршрутизации мал и не зависит от числа сетей в автономной системе. Каждый шлюз посылает такие пакеты с помощью лавинной маршрутизации. При появлении в сети нового шлюза или включении новой линии связи изменения в топологии сети не учитываются при маршрутизации в течение некоторого времени для того, чтобы информация о происшедших изменениях успела достигнуть всех шлюзов автономной системы.

Алгоритм Дейкстры по сравнению с алгоритмом Беллмана-Форда обеспечивает более реальную оценку ситуации в сети, более быструю реакцию на важные изменения в сети (такие, как включение новой линии связи) и уменьшает зацикливание пакетов; однако алгоритм Дейкстры сложнее в реализации и требует в несколько раз больше памяти.

3 ТЕХНОЛОГИИ ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

3.1 Сети Ethernet и Fast Ethernet

Под Ethernet обычно понимают любой из вариантов этой технологии, хотя изначально Ethernet это сетевой стандарт, основанный на технологии экспериментальной сети Ethernet Network, разработанной и реализованной фирмой Xerox в 1975 году. Позже в 1980 году компаниями DEC, Intel и Xerox был совместно разработан и опробован стандарт Ethernet версии 2 для сети, построенной на основе коаксиального кабеля. Поэтому стандарт Ethernet также называют стандартом DIX.

На основе стандарта Ethernet DIX был разработан стандарт с названием IEEE 802.3. В зависимости от типа физической среды этот стандарт имеет различную модификацию: 10Base-5, 10Base-2, 10Base-T, 10Base-F.

В качестве метода доступа к среде передачи данных в сетях Ethernet используется метод коллективного доступа с опознаванием несущих и обнаружением коллизий (CSMA/CD). Этот метод используется исключительно в сетях с общей шиной.

Первые сети, построенные на технологии Ethernet, были созданы на коаксиальном кабеле диаметром 1/2 дюйма. Позже были определены другие спецификации физического уровня для стандарта Ethernet, которые позволили использовать различные среды передачи данных в качестве общей шины. При этом метод доступа CSMA/CD и все временные параметры Ethernet остаются неизменными для любой спецификации физической среды. Физические спецификации технологии

Ethernet в настоящее время включают следующие среды передачи данных:

- 10Base-5 – это коаксиальный кабель диаметром 1/2 дюйма, имеющий волновое сопротивление 50 Ом. Максимальная длина сегмента кабеля 500 м. Этот кабель также называют толстым коаксиалом.
- 10Base-2 – это коаксиальный кабель диаметром 1/4 дюйма с волновым сопротивлением 50 Ом. Максимальная длина сегмента 185 м. Этот кабель также называется тонким коаксиалом.
- 10Base-T – это кабель на основе неэкранированной витой пары. По данной спецификации образуется звездообразная топология с концентратором. Максимальное расстояние между концентратором и конечным узлом 100м.
- 10Base-F – это оптоволоконный кабель. Топология аналогична предыдущему случаю. Существует несколько вариантов этой спецификации, например 10Base-FL, 10Base-FB.

Сети, построенные на основе стандарта 10Base-T, имеют преимущество перед коаксиальными вариантами Ethernet, что связано с разделением общего физического кабеля на отдельные отрезки, подключенные к центральному коммуникационному устройству. Хотя эти отрезки, как и прежде, образуют общий домен коллизий, их физическое разделение позволяет контролировать их состояние и отключать в случае обрыва, замыкания или неисправностей сетевого адаптера. Этот момент существенно упрощает эксплуатацию больших сетей Ethernet, т.к. концентратор обычно автоматически выполняет такие функции.

Стандарт 10Base-FL предназначен для соединения конечных узлов с концентраторами и работает с сегментами оптоволокна длиной не более 2000 м при общей длине сети не более 2500 м.

Замечание. Мост, сетевой мост, бридж (Bridge) — сетевое оборудование для объединения сегментов локальной сети. Сетевой мост рабо-

тает на втором уровне модели OSI, обеспечивая ограничение домена коллизий (в случае сети Ethernet). Коммутатор (свитч) и мост аналогичны по функциональности. Мосты обрабатывают IP-пакеты, используя центральный процессор, коммутатор использует аппаратную схему для коммутации пакетов.

Технология *Fast Ethernet* является развитием классической технологии Ethernet. В 1992 году группа производителей сетевого оборудования для разработки стандарта на новую технологию образовали некоммерческое объединение под названием Fast Ethernet Alliance. В 1995 году спецификация Fast Ethernet была принята в качестве стандарта 802.3u, который представляет собой дополнение к существующему стандарту 802.3. Отличие Fast Ethernet от Ethernet сосредоточено на физическом уровне. В технологии Fast Ethernet используются 3 вида кабельных систем:

– 100Base-TX – двухпарный кабель на неэкранированной витой паре.

– 100Base-T4 – четырехпарный кабель на неэкранированной витой паре.

– 100Base-FX – многомодовый оптоволоконный кабель.

Основными достоинствами технологии Fast Ethernet являются:

- увеличение пропускной способности сегментов сети до 100 Мбит/с;
- сохранение метода случайного доступа;
- сохранение звездообразной топологии сети и поддержка традиционных сред передачи данных.

Эти преимущества позволили осуществлять постепенный переход от сетей 10Base-T к скоростным сетям Fast Ethernet, не требуя коренной переподготовки обслуживающего персонала и замены оборудования во всех узлах сети.

3.2 Сети Token Ring и FDDI

Сети стандарта Token Ring, так же как и сети Ethernet, используют разделяемую среду передачи данных, которая состоит из отрезков кабеля, соединяющих все станции сети в кольцо. Кольцо при этом рассматривается как общий разделяемый ресурс и для доступа к нему используется детерминированный алгоритм, основанный на передаче станции права на использование кольца в определенном порядке. Право на использование кольца передается с помощью кадра специального формата – маркера или токена.

Стандарт Token Ring был принят в 1985 году, тогда же компания IBM приняла этот стандарт в качестве своей основной сетевой технологии. Сети стандарта Token Ring работают с двумя битовыми скоростями 4 и 16 Мбит/с. Первая скорость определена в стандарте 802.5, а вторая появилась в результате развития технологии Token Ring. Смешение в одном кольце станций, работающих на различных скоростях, не допускается. Сети Token Ring, работающие со скоростями 16 Мбит/с, имеют также некоторые усовершенствованные алгоритмы доступа. В сетях с маркерным методом доступа, каковыми являются сети Token Ring, право на доступ к среде передается циклически от станции к станции по логическому кольцу, образуемому отрезками кабеля, соединяющими соседние станции.

Таким образом, каждая станция связана с предшествующей и последующей и может обмениваться данными напрямую только с ними.

Для обеспечения доступа станциям к физической среде по кольцу циркулирует кадр специального формата и назначения – маркер (токен). При получении маркера станция анализирует его, при необходимости модифицирует и в случае отсутствия у нее данных для передачи обеспечивает его передачу следующей станции.

В сетях Token Ring со скоростью 16 Мбит/с используется также другой алгоритм доступа к кольцу, называемый алгоритмом раннего

освобождения маркера. По этому алгоритму станция передает маркер доступа следующей станции сразу же после окончания передачи последнего бита кадра, не дожидаясь возвращения по кольцу этого кадра с битом подтверждения приема. В этом случае пропускная способность кольца используется более эффективно и составляет около 80% от номинальной.

Для различных видов сообщений передаваемым данным могут назначаться различные приоритеты. Каждая станция в кольце имеет механизм обнаружения и устранения неисправностей в сети, возникающих в результате ошибок передачи или переходных явлений. Например, включение и отключение станций. Не все станции в сети являются равноправными. Одна из станций является активным монитором, что означает дополнительную ответственность по управлению кольцом. Активный монитор осуществляет управление таймаутом в кольце, при необходимости порождает новые маркеры и генерирует диагностические кадры при возникновении неполадки. Активный монитор выбирается при инициализации кольца. Существует механизм, при помощи которого может быть назначен новый активный монитор, если на станции, являвшейся им, по какой-либо причине произошел отказ.

Стандарт Token Ring предусматривает построение связей в сети как с помощью непосредственного соединения станций друг с другом, так и образование кольца с помощью концентраторов. Максимальное количество станций в одном кольце 250.

Помимо поддержки экранированной витой пары существуют сетевые адаптеры и концентраторы Token Ring, поддерживающие неэкранированную витую пару и оптоволокно.

Технология FDDI – это первая технология локальных сетей, которая использовала в качестве среды передачи данных оптоволоконный ка-

бель. Технология FDDI во многом основывается на технологии Token Ring. При разработке технологии в качестве основных ставились следующие цели:

- повышение битовой скорости передачи данных до 100 Мбит/с;
- повышение отказоустойчивости сети за счет стандартных процедур ее восстановления после отказов различного рода;
- максимально эффективное использование пропускной способности сети.

Сети FDDI строятся на основе двух оптоволоконных колец, образующих основной и резервные пути передачи данных между узлами сети. Использование двух колец вместо одного является основным способом повышения отказоустойчивости в сети FDDI. В нормальном режиме работы сети данные проходят через все узлы и участки кабеля первичного кольца. Вторичное кольцо в этом режиме не используется. В случае возникновения отказа, когда часть первичного кольца не может передавать данные, первичное кольцо объединяется со вторичным, вновь образуя единое кольцо. Таким образом, сеть FDDI может полностью восстановить свою работоспособность в случае единичных отказов ее элементов. При множественных отказах сеть распадается на несколько не связанных между собой сетей.

3.3 Стандарт Gigabit Ethernet

Технология Gigabit Ethernet использует тот же формат кадров, тот же метод доступа к среде передачи CSMA/CD, те же механизмы контроля потоков и те же управляющие объекты. Но в то же время Gigabit Ethernet отличается от Fast Ethernet больше, чем Fast Ethernet от Ethernet. Gigabit Ethernet ставит несравнимо более сложные технические задачи и предъявляет гораздо более высокие требования к качеству проводки.

За основу физических стандартов для Gigabit Ethernet был взят стандарт ANSI X3T11 Fibre Channel. Зависимая от физической среды спецификация Fibre Channel определяет в настоящее время скорость 1,062 гигабод в секунду. В Gigabit Ethernet она была увеличена до 1,25 гигабод в секунду. С учетом кодирования по схеме 8В/10В получается скорость передачи данных 1 Гбит/с.

Спецификация Gigabit Ethernet предусматривает следующие среды передачи: одномодовый и многомодовый оптический кабель с длинноволновыми лазерами 1000BaseLX для длинных магистралей, для зданий и комплексов зданий, многомодовый оптический кабель с коротковолновыми лазерами 1000BaseSX для недорогих коротких магистралей, симметричный экранированный короткий 150-омный медный кабель 1000BaseCX для межсоединения оборудования в аппаратных и серверных, 1000BaseT для четырехпарных кабелей с неэкранированными витыми парами категории 5 длиной 100 м (т. е. для сетей с диаметром 200 м, как и в 100BaseT).

При разработке стандарта Gigabit Ethernet была обнаружена проблема дифференциальной задержки, которая проявляется только при определенных комбинациях излучателей (лазеров) и многомодового оптического кабеля невысокого качества и не свойственна менее скоростным технологиям.

Эффект дифференциальной задержки состоит в том, что один излучаемый лазером импульс света возбуждает несколько мод в многомодовом волокне. Эти моды, или пути распространения света, могут иметь разную длину и разную задержку. В результате при распространении по волокну отдельный импульс может даже разделиться на несколько импульсов, а последовательные импульсы могут накладываться друг на друга, так что исходные данные будет невозможно восстановить.

Предложенное решение заключается в том, что световой сигнал источника формируется предварительно специальным образом, а именно

свет от лазера распределяется равномерно по диаметру волокна. Цель подобной процедуры состоит в более равномерном распределении энергии сигнала между всеми модами.

Один из ключевых вопросов для Gigabit Ethernet – это максимальный размер сети. При переходе от Ethernet к Fast Ethernet сохранение минимального размера кадра привело к уменьшению диаметра сети с 2 км для 10Base-T до 200 м для 100Base-T. Однако перенос без изменения всех отличительных составляющих Ethernet – минимального размера кадра, времени обнаружения коллизии и метода CSMA/CD – на Gigabit Ethernet обернулся бы сокращением диаметра сети до 20 м. Поэтому было предложено увеличить время обнаружения коллизии с тем, чтобы сохранить прежний диаметр сети в 200 м. Такое переопределение подуровня MAC необходимо для Gigabit Ethernet, иначе отстоящие друг от друга на расстоянии 200 м станции не смогут обнаружить конфликт, когда они обе одновременно передают кадр минимально допустимой длиной 64 байта.

Такое решение было названо расширением несущей. Суть его в следующем. Если сетевой адаптер Gigabit Ethernet передает кадр длиной менее 512 байт, то он посылает вслед за ним биты расширения несущей, т.е. время обнаружения конфликта увеличивается. Если за время передачи кадра и расширения несущей отправитель зафиксирует коллизию, то он реагирует традиционным образом, подавая сигнал усиления коллизии (jam-сигнал) и отбрасывая принятые данные.

Однако если все станции (узлы) передают кадры минимальной длины (64 байта), то реальное повышение производительности по сравнению с Fast Ethernet будет незначительным – 125 Мбит/с вместо 100 Мбит/с. Это худший вариант, но с учетом того, что средняя длина кадра составляет на практике 200-500 байт, пропускная способность возрастет всего лишь до 300-400 Мбит/с. Поэтому подобное решение довольно неэффективно.

С целью повышения эффективности Gigabit Ethernet комитет предложил метод пакетной передачи кадров. В соответствии с этим методом короткие кадры накапливаются и передаются вместе. Передающая станция заполняет интервал между кадрами битами расширения несущей, поэтому другие станции будут воздерживаться от передачи, пока она не освободит линию.

Проведенное компанией AMD моделирование показало, что в полудуплексной топологии с коллизиями сеть Gigabit Ethernet позволяет достичь пропускной способности 720 Мбит/с при полной нагрузке сети. Тем не менее, необходимость применения подобных ухищрений свидетельствуют о том, что метод доступа к среде CSMA/CD на высоких скоростях передачи является неэффективным.

В то же время подобные усовершенствования метода доступа необходимы только для полудуплексного режима, так как для полнодуплексной передачи метод CSMA/CD не нужен.

Одним из способов обойти ограничения, связанные с расширением несущей, является использование так называемых буферных распределителей. Этот новый класс устройств (иногда их еще называют полнодуплексными повторителями) представляет собой нечто среднее между повторителем и коммутатором.

Все порты гигабитного буферного распределителя работают в полнодуплексном режиме. Как обычный повторитель Ethernet – он передает поступивший кадр на все свои порты; как коммутатор Ethernet – способен принимать кадры на нескольких портах одновременно, при этом поступившие кадры помещаются в буферы. При заполнении буферов распределитель задействует механизмы управления потоками для информирования передающего узла о необходимости приостановить передачу. Такой подход позволяет достичь пропускной способности, близкой к номинальной.

3.4 Беспроводные сети

Стандарт 802.11 определяет физический уровень эталонной модели взаимодействия открытых систем и нижний подуровень канального уровня, который носит название MAC. В качестве физической среды передачи данных стандарт 802.11 позволяет использовать как радиоволны, так и инфракрасное излучение.

Стандарт 802.11 иногда называют стандартом беспроводных сетей Ethernet. Разработка стандарта была начата в начале 90-х годов, а окончательная версия принята в июне 1997 года.

В России применение беспроводных сетей сдерживалось из-за того, что частоты 2.4–2,4835 ГГц, используемые в 802.11, не были открыты для широкого использования.

Из-за особенностей среды передачи беспроводные локальные сети имеют свойства, отличные от традиционных кабельных сетей. Поэтому использование на подуровне MAC метода множественного доступа с контролем несущей (CSMA – Carrier Sense Multiple Access) невозможно в том виде, какой он имеет в проводных сетях Ethernet, и вместо обнаружения коллизий (CSMA/CD – Collision Detect) используется их предотвращение (CSMA/CA – Collision Avoidance).

Типичная беспроводная сеть представляет собой совокупность распределенных базовых станций и мобильных клиентов, представляя, таким образом, сотовую систему, состоящую из отдельных ячеек. В отличие от телефонных сотовых систем каждая ячейка занимает весь доступный диапазон рабочих частот. Особенностью беспроводных сетей является то, что при нахождении приемника в радиусе действия двух активных передающих устройств сигнал оказывается испорченным вследствие наложения. Помимо этого станции беспроводной сети могут находиться за пределами зоны действия друг друга, что, в свою очередь, приводит к дополнительным сложностям.

Воспользоваться методом множественного доступа с контролем несущей при этом не представляется возможным.

Предположим, что станция А беспроводной сети ведет передачу информации на станцию В, а станция С находится вне зоны действия станции А. Тогда станция С не сможет зафиксировать передачу и сделает ошибочный вывод, что она может передавать данные. В результате передача станции С наложится на передачу станции А и станция В не сможет принять информацию от станции А. Невозможность зафиксировать передачу потенциального конкурента вследствие его удаленности называется проблемой скрытого узла.

Возможна также обратная ситуация. Если станция В передает информацию на станцию А, а станция С слышит эту передачу, то станция С может отказаться от передачи вообще, хотя её передача никаким образом не повлияет на прием информации станции А, т.к. станция А находится вне зоны действия передатчика станции С. Такая проблема называется проблемой слышащей станции.

Метод доступа CSMA/CA позволяет определить отсутствие активности в эфире вблизи передающей станции, в то время как передающей станции требуется знать об отсутствии активности вблизи принимающей станции. В проводных сетях сигналы достигают всех станций, поэтому в каждый временной интервал передачу может вести только одна станция. В беспроводных системах с небольшим радиусом действия передатчиков несколько станций могут вести передачу одновременно в том случае, если у них разные адресаты и эти адресаты находятся вне зоны действия друг друга.

Стандарт 802.11 основывается на предложенном в 1990 году методе множественного доступа с предотвращением коллизий – MACA (Multiple Access with Collision Avoidance). Идеи этого метода доступа заключаются в следующем: станция, которая собирается передать информацию, посылает сначала короткий кадр RTS (Request to Send – запрос на передачу данных); в ответ на запрос RTS принимающая станция от-

правляет подтверждение о готовности к приему данных CTS (Clear to Send – запрос о готовности принятия данных). Все находящиеся вблизи станции, услышав этот обмен пакетами, должны воздержаться от собственной передачи. Если станция слышит RTS, то она находится вблизи передающей и должна воздержаться от собственной передачи до получения передающей станцией подтверждения о возможности передачи. Если станция слышит CTS, то она находится вблизи принимающей станции и должна воздерживаться от собственной передачи на протяжении всей последующей передачи данных. Однако это не предотвращает коллизий, т.к. два запроса RTS могут быть отправлены одновременно различными станциями и в результате одна или обе из них не получат ответа CTS за заранее установленный интервал времени. После этого такая станция должна ожидать в течение псевдослучайного промежутка времени в соответствии с алгоритмом, аналогичным используемому в проводных сетях Ethernet.

Стандарт 802.11a регламентирует передачу данных со скоростью до 54 Мбит/с в частотном диапазоне 5,150 ГГц – 5,350 ГГц и 5,750 Ггц – 5,850 ГГц. Данный частотный диапазон разбит на 3 диапазона по 100 МГц, которые различаются ограничениями на максимальную мощность передачи (табл. 3.1).

Т а б л и ц а 3.1. ***Допустимые мощности передачи***

Частота, ГГц	Мощность, мВт
5,150 – 5,250	50
5,250 – 5,350	250
5,750 – 5,850	1000

Использование 3 частотных поддиапазонов общей шириной 300 МГц делает стандарт 802.11a самым широкополосным из всего семейства стандартов 802.11, а также позволяет разбить весь частотный диапазон на 12 каналов, каждый из которых имеет ширину 20 МГц. Ос-

тавшаяся часть диапазона предназначена для разделения частот. При этом четыре верхних частотных канала, предусматривающие наибольшую мощность передачи, используются в основном для передачи данных вне помещений. Предусмотренная стандартом ширина канала, равная 20 МГц, достаточна для организации высокоскоростной передачи. Использование более высоких частот и ограничения мощности приводит к возникновению ряда проблем при организации высокоскоростной передачи данных. Распространение любого сигнала сопровождается его затуханием, причем величина затухания зависит как от расстояния от точки передачи, так и от частоты сигнала:

$$L = K \lg \frac{4\pi\omega d}{c},$$

где L – величина сигнала, выраженная в децибелах; K – коэффициент ослабления (для открытого пространства равен 20); ω – частота сигнала; d – расстояние от точки передачи; c – скорость света.

Использование более высоких частот в протоколах 802.11a приводит к меньшему радиусу действия сети по сравнению с протоколом 802.11b.

Помимо учета большого затухания при использовании высокочастотного сигнала необходимо принимать во внимание возникновение эффекта многолучевой интерференции. Он заключается в том, что в результате многократных отражений сигнал может попасть в приемник различными путями, которые оказывают разное влияние на время распространения, длину и ослабление сигналов. Таким образом, в точке приема результирующий сигнал представляет собой суперпозицию нескольких сигналов, смещенных друг относительно друга по времени и имеющих различные амплитуды, что также накладывает ограничение на максимальный радиус.

Для доступа к среде передачи данных в стандарте 802.11b используется метод множественного доступа с контролем несущей и предот-

вращением коллизий CSMA/CA (CA – Collision Avoidance). Отличие этого метода от метода множественного доступа с обнаружением коллизий заключается в том, что вместо обнаружения коллизий используется технология их предотвращения/избегания.

С помощью четырехступенчатого протокола передачи данных реализуется регламентирование коллективного доступа с минимизацией вероятности возникновения коллизий. Каждый пересылаемый пакет данных содержит контрольную сумму, которая позволяет обнаружить ошибку при передаче. Кроме того, стандарт предусматривает разбивку больших пакетов данных на малые, что, в свою очередь, снижает вероятность повторной передачи блоков данных, т.к. с увеличением длины передаваемых данных возрастает вероятность возникновения ошибки.

Стандарт 802.11b предписывает разбивку данных на пакеты, дополненные контрольной и адресной информацией длиной 30 байт и 4-байтной контрольной суммой. Рекомендуемый стандартный размер пакетов составляет 1500 байт и 2048 байт.

Стандарт 802.11b обеспечивает передачу данных на скоростях 1; 2; 6; 11 Мбит/с в частотном диапазоне 2.4ГГц (2.4ГГц - 2.4835ГГц). При использовании технологии расширения спектра (DSSS) возможно появление проблем из-за помех от бытовых беспроводных приборов (микроволновых печей и радиотелефонов).

Наиболее существенным недостатком стандарта 802.11b является его невысокая для многих современных приложений пропускная способность.

Стандарт 802.11g предусматривает различные скорости передачи данных: 1; 1,5; 2; 6; 9; 11; 12; 18; 22; 24; 33; 36; 48; 54 Мбит/с. Для различных скоростей соединения применяются разные методы модуляции сигнала.

Стандартом 802.11g предусмотрено использование частотного диапазона 2.4 ÷ 2,4835 ГГц. Несмотря на возможности использования этого частотного диапазона без получения лицензии существует ограничение

на максимальную мощность передатчика, поэтому при выборе методов кодирования и модуляции сигналов необходимо решение двух основных проблем.

Во-первых, скорость передачи в беспроводной сети должна быть как можно более высокой для того, чтобы эта сеть могла успешно конкурировать с традиционными проводными сетями. Увеличение скорости передачи приводит к увеличению ширины спектра, что нежелательно из-за ограничения частотного диапазона передачи.

Во-вторых, для того, чтобы не создавать помех другим устройствам, работающим в используемом диапазоне частот, уровень полезного сигнала должен быть достаточно низким. В идеальном случае полезный сигнал должен быть едва различим на уровне шума, что требует наличия алгоритма безошибочного распознания сигнала. Уменьшение мощности передаваемого сигнала обеспечивается за счет применения технологии расширения спектра и распределения сигнала по всей ширине спектра.

В-третьих, беспроводная сеть должна обеспечивать надлежащий уровень помехозащищенности.

Одновременное выполнение всех перечисленных условий невозможно из-за их противоречивости, поэтому выбор конкретного метода кодирования и модуляции сигнала является компромиссом между требованием высокой скорости передачи, помехоустойчивости и ограничения по мощности передатчика.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – Спб.: Питер, 2010 – 944 с.

2. Камышников В.В. Основы сетевой архитектуры Internet: Учеб. пособие. – Самара: Изд-во «Самарский университет», 2001. – 107 с.

3. Новиков Ю.В., Кондратенко С.В. Основы локальных сетей. – М.: Изд-во "Интернет-университет информационных технологий – Интуит.ру", 2005. – 360 с.

4. Олифер В.Г., Олифер Н.А. Основы сетей передачи данных: Курс лекций. – М.: Интуит.ру, 2005 – 176 с.

5. Жеретинцева Н.Н. Курс лекций по компьютерным сетям – Владивосток: ДВГМА, 2000. – 158 с.

6. Нанс Б. Компьютерные сети: Пер. с англ. – М.: БИНОМ, 1996. – 400 с.

7. Храмцов П. Лабиринт Internet. – М.: ЭЛЕКТРОНИНФОРМ, 1996. — 256 с.

8. Мамаев М.А. Телекоммуникационные технологии: Сети TCP/IP: Учеб. пособие – Владивосток: Изд-во ВГУЭиС, 1999.

9. Postel J. User Datagram Protocol, 28 August 1980 – http://www.faqs.org/rfc/rfc768.txt

10.Internet Protocol. DARPA Internet Program Protocol Specification, September 1981 – http://www.faqs.org/rfc/rfc791.txt

11.Transmission Control Protocol. DARPA Internet Program Protocol Specification, September 1981 – http://www.faqs.org/rfc/rfc793.txt

Учебное издание

Еленев Дмитрий Валерьевич

КОМПЬЮТЕРНЫЕ СЕТИ

Учебное пособие

Редактор Н. С. К у п р и я н о в а
Компьютерная верстка Т. Е. П о л о в н е в а

Подписано в печать 21.10.2010. Формат 60x84 1/16
Бумага офсетная. Печать офсетная.
Печ. л. 5,0.
Тираж 100 экз. Заказ .

Самарский государственный
аэрокосмический университет,
443086, Самара, Московское шоссе, 34.

Издательство Самарского государственного
аэрокосмического университета
443086, Самара, Московское шоссе, 34.