

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

В.П. Комагоров

АРХИТЕКТУРА СЕТЕЙ И СИСТЕМ ТЕЛЕКОММУНИКАЦИЙ

*Допущено Учебно-методическим объединением вузов
по университетскому политехническому образованию
в качестве учебного пособия для магистров, обучающихся
по направлению «Информатика и вычислительная техника»*

Издательство
Томского политехнического университета
2012

УДК 621.39(075.8)

ББК 32.968я73

К63

Комагоров В.П.

К63 Архитектура сетей и систем телекоммуникаций: учебное пособие / В.П. Комагоров; Томский политехнический университет. – Томск: Изд-во Томского политехнического университета, 2012. – 151 с.

ISBN 978-5-4387-0054-8

Пособие содержит сведения о принципах построения и функционирования локальных, региональных, глобальных вычислительных сетей и мобильных телекоммуникаций. В конце каждого раздела приведены методические указания, что поможет лучшему усвоению ключевых моментов по конкретным темам.

Предназначено для подготовки магистров по специализации «Сети ЭВМ и телекоммуникации» направления 230100 «Информатика и вычислительная техника».

УДК 621.39(075.8)

ББК 32.968я73

Рецензенты

Доктор технических наук, профессор
заведующий кафедрой ТКС НИУ МИЭТ

В.В. Баринов

Доктор технических наук, профессор ТПУ

В.К. Погребной

Кандидат технических наук

директор ООО «Инком»

М.А. Сонькин

ISBN 978-5-4387-0054-8

© ФГБОУ ВПО НИ ТПУ, 2012

© Комагоров В.П., 2012

© Оформление. Издательство Томского
политехнического университета, 2012

ВВЕДЕНИЕ

Компьютерные сети играют важную роль в распределенной обработке, хранении и передаче информации. На их основе создаются современные цифровые системы связи. Самая известная из них глобальная сеть Internet, включающая в себя сотни миллионов компьютеров и соединяющая города, страны и материки.

Материал излагается таким образом, что вначале студенты знакомятся с общими принципами построения компьютерных сетей, а затем более детально изучают особенности каждой из них: локальной, региональной, глобальной. В заключение приводится описание современного состояния мобильных телекоммуникаций. Пособие содержит пять глав.

В первой главе излагаются общие принципы построения компьютерных сетей. Здесь приводится описание семиуровневой модели ISO/OSI, которое базируется на материале, изложенном в [1, 5, 7].

Вторая глава содержит описание принципов построения локальных вычислительных сетей (ЛВС). В ней рассматриваются три типовые ЛВС: Ethernet, ARCnet и Token Ring, в основе которых лежит стандарт IEEE 802. При изложении этой главы были использованы материалы, содержащиеся в [1, 8, 9].

Третья глава посвящена региональным вычислительным сетям, построенным по технологии FDDI и ATM. Основным источником для описания этих технологий явились материалы, изложенные в [2, 3].

В четвертой главе рассмотрены глобальные компьютерные сети, построенные на основе двух протоколов: X.25 и TCP/IP. Основная часть этой главы содержит описание принципов построения глобальной сети Internet. Эти материалы заимствованы из [4, 6].

Пятая глава посвящена описанию мобильных телекоммуникационных систем, построенных по беспроводной технологии Wi-Fi. Этот раздел содержит материалы по беспроводной локальной сети WLAN, сети средних и коротких расстояний Bluetooth и сети мобильной связи GSM. Эти материалы заимствованы из [10, 11, 12].

В конце каждой главы приведены методические указания, содержащие основные выводы по главе.

Глава 1

ОБЩИЕ ПРИНЦИПЫ ПОСТРОЕНИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ

1.1. Введение в компьютерные сети

Анализ мировых тенденций развития экономики свидетельствует о том, что ее состояние в значительной степени зависит от степени развития средств сбора, хранения, передачи и обработки информации в различных сферах человеческой деятельности.

Ключевую роль в этом вопросе призваны сыграть компьютерные сети, которые возникли как результат сотрудничества специалистов из двух областей – компьютерной техники и связи. Они являются конкретным воплощением общей тенденции к распределенной информации, которая проявляется в создании мультипроцессорных систем (серверов), распределенных баз данных, в использовании интеллектуальных терминалов на основе персональных компьютеров и мобильных средств связи.

Важной компонентой компьютерной сети является система передачи данных. Наиболее перспективными в этом отношении системами являются волоконно-оптические (ВОЛС), спутниковые системы связи (ССС) и мобильные телекоммуникации. Именно эти системы обеспечили возможность создания международной глобальной сети Internet, которая располагает мировыми, распределенными по материкам и странам информационными ресурсами, позволяет получать к ним удаленный доступ, обмениваться информацией в режиме электронной почты.

Таким образом, *компьютерная сеть представляет собой комплекс распределенной компьютерной техники (компьютеров, программируемых контроллеров, устройств ввода-вывода информации и т. д.), соединенной между собой системой передачи данных, содержащей коммуникационное оборудование и каналы связи.*

В зависимости от территориального расположения, *компьютерные сети подразделяются на локальные, региональные и глобальные.*

Локальная компьютерная сеть (LAN) – это комплекс распределенной в пределах отдельных зданий и сооружений компьютерной техники, соединенной высокоскоростными цифровыми каналами связи.

Характерной особенностью LAN является упрощенная топология, т. е. пространственное расположение компьютерной техники и каналов связи. Типовыми топологиями являются *шина* (рис. 1), *звезда* (рис. 2) и *кольцо* (рис. 3).



Рис. 1. Топология «шина»

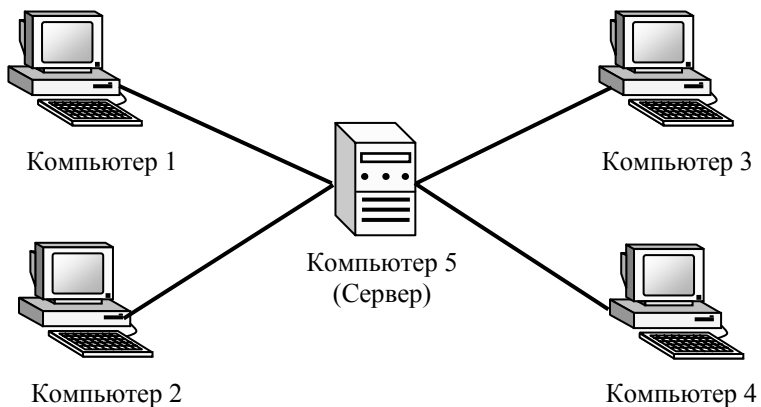


Рис. 2. Топология «звезда»

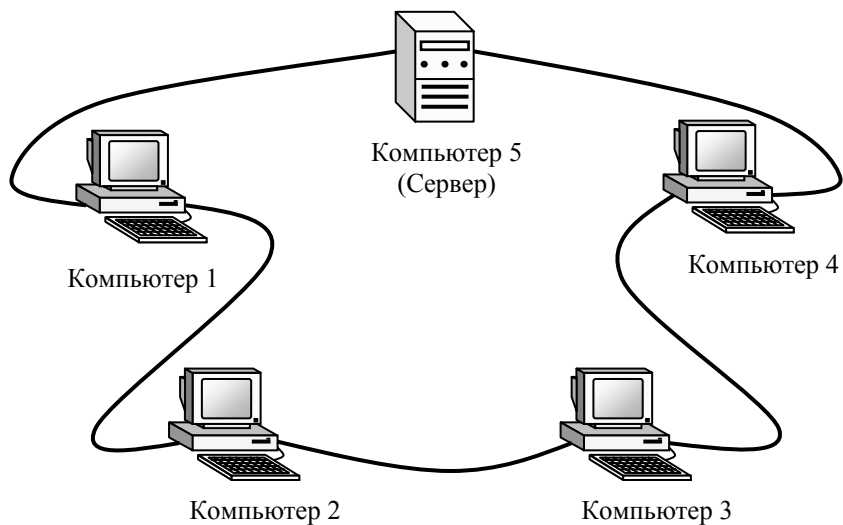


Рис. 3. Топология «кольцо»

Упрощенная топология LAN, а также малая протяженность (несколько тысяч метров) обеспечили им высокую скорость передачи данных (более одного миллиарда бит в секунду). В качестве каналов связи в LAN применяются витая пара (скрученные медные провода), ВОЛС и Wi-Fi – беспроводная технология соединения компьютеров в локальную сеть и подключения к Internet (Wireless Fidelity – высокая точность беспроводной передачи данных).

Кроме топологии, важной характеристикой LAN является технология передачи данных (метод доступа компьютера к каналу связи). В LAN в основном применяются два метода: множественный доступ с контролем несущей и обнаружением столкновений (CSMA/CD) и маркерный метод доступа.

При методе доступа CSMA/CD компьютер перед началом передачи слушает канал связи и определяет наличие несущей (физического сигнала, свидетельствующего о передаче данных другим компьютером). После исчезновения несущей компьютер начинает передавать данные и одновременно слушает канал для обнаружения столкновения несущих, если другой компьютер пытается также передать данные. Обнаружив столкновение, компьютер прекращает передачу и пытается возобновить ее через некоторый случайный промежуток времени.

В LAN с маркерным методом доступа правом передавать данные обладает только один компьютер, в котором находится маркер. Маркер представляет собой специальное сообщение (пакет), который постоянно циркулирует в сети от одного компьютера к другому. Такой метод доступа гарантирует, что любой компьютер рано или поздно получит маркер и выполнит передачу данных. При этом сеть содержит средства восстановления маркера в случае его пропажи.

Примером LAN, в которой реализован метод доступа CSMA/CD, является сеть Ethernet. На основе маркерного метода доступа построены сети ARCNet и Token Ring.

Региональные компьютерные сети (WAN) представляют собой объединение LAN предприятий и организаций, расположенных в пределах региона или области и связанных между собой разнообразными каналами передачи данных: кабельными, ВОЛС, радиоканалами, спутниковыми системами связи (ССС).

WAN могут иметь произвольную топологию. Для объединения LAN применяются специальные устройства: мосты, маршрутизаторы и шлюзы.

Мост – это устройство, соединяющее две сети, построенные по одной и той же технологии (например, Ethernet и ARCNet). Через мост передаются сообщения, которыми обмениваются компьютеры, расположенные в разных сетях.

Маршрутизатор представляет собой устройство для соединения LAN с разной технологией (например, Ethernet и Token Ring). Маршрутизатор, в отличие от моста, имеет свой собственный сетевой адрес и используется как промежуточный пункт назначения. Основное назначение маршрутизатора состоит в управлении маршрутами передаваемых сообщений.

Шлюз – это устройство, которое, кроме функций маршрутизации, выполняет преобразование данных из одного формата в другой либо специальных программ сетевого обмена (протоколов) из одного типа в другой.

Глобальные компьютерные сети (GAN) объединяют WAN, компьютерные сети стран, материков. Построение этих сетей выполняется строго в соответствии с международными стандартами. *Примером глобальной сети является сеть Internet*, которая соединила в себе национальные сети стран мира, содержит сотни миллионов компьютеров, обеспечивает удаленный доступ к мировым информационным ресурсам (в том числе, национальным библиотечным фондам), позволяет передавать и принимать сообщения в режиме электронной почты (E-mail) абонентам, находящимся на разных материках.

Важной особенностью сети Internet является ее способность хранить и передавать не только цифровые данные, но и речь, музыку, видеоизображение. Поэтому с дальнейшим развитием сети Internet (созданием более производительных маршрутизаторов и шлюзов, широким внедрением ВОЛС и ССС) она заменит существующие в настоящее время средства связи.

В процессе своего развития сеть Internet оказывает существенное влияние на современные способы построения LAN, которое проявляется в разработке Intranet-технологий. Основу Intranet-технологий составляют те же методы и средства (в первую очередь средства доступа к информационным ресурсам), которые применяются в сети Internet.

1.2. Многоуровневая архитектура компьютерной сети

Компьютерная сеть представляет собой сложную систему, предназначенную для распределенной обработки, хранения и передачи данных. На рис. 4 приведена ее конфигурация в самом общем виде. *Компьютерная сеть состоит из коммуникационной подсети и сетевых абонентов (компьютерной техники, подключенной к коммуникационной подсети и реализующей функции обработки, хранения информации и доступа в сеть).*

В состав коммуникационной подсети входят узлы коммутации (маршрутизаторы) и соединяющие их каналы связи. Сетевыми абонентами могут являться LAN, мощные многопроцессорные компьютеры (HOST), сетевые терминалы на базе персональных компьютеров. Под-

ключение абонентов к коммуникационной подсети осуществляется с помощью шлюзов, выполняющих преобразование форматов данных и сетевых протоколов.

На основании концепции открытых систем (OSI) Международный институт стандартов (ISO) разработал семиуровневую модель компьютерной сети, которая получила название модель ISO/OSI. В соответствии с этой моделью взаимодействие абонентов через коммуникационную подсеть происходит с помощью сетевых протоколов.

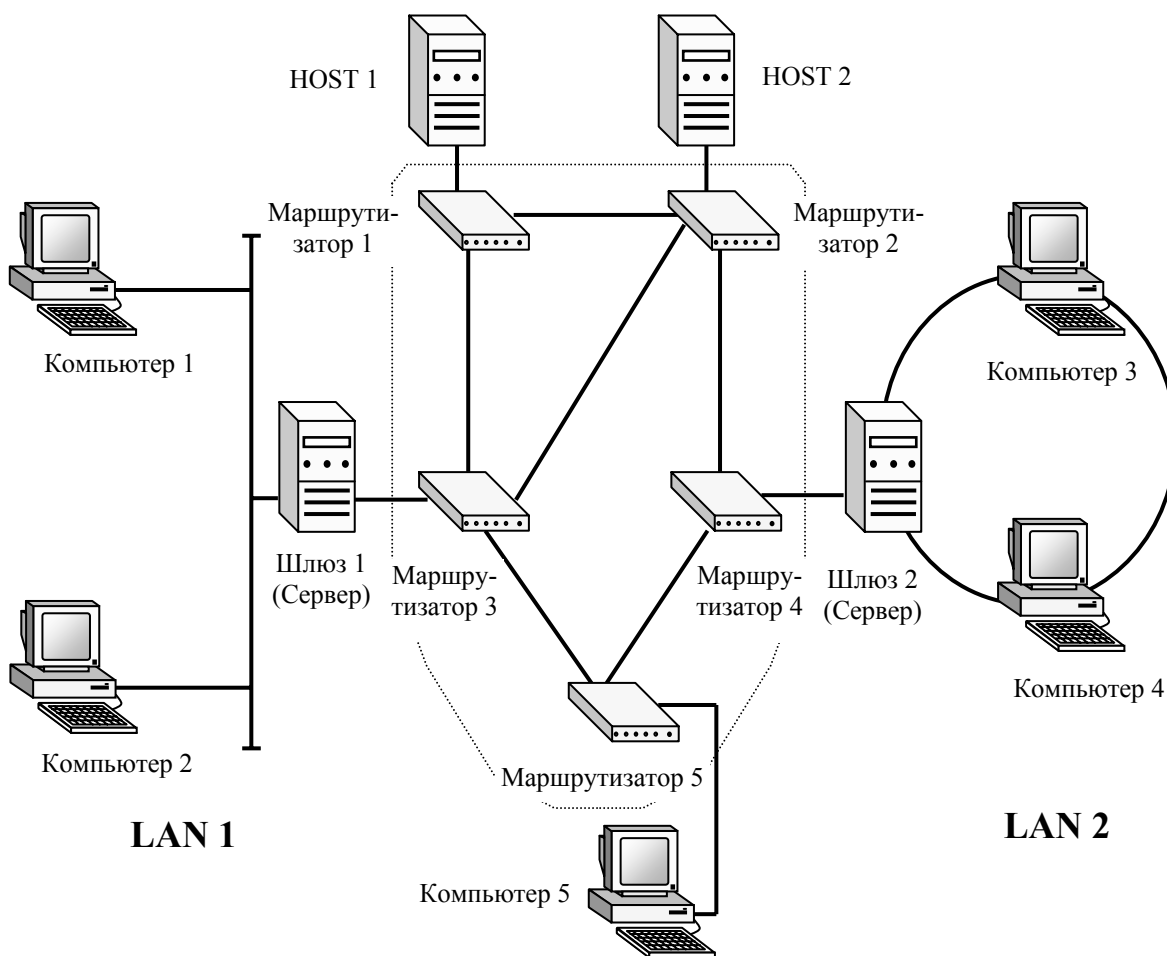


Рис. 4. Пример конфигурации компьютерной сети

Под сетевым протоколом понимается строго формализованная процедура (определенная последовательность правил) взаимодействия абонентов сети через коммуникационную подсеть. При этом между уровнями модели и сетевыми протоколами имеет место определенное соответствие. Функции протоколов каждого уровня поясняет табл. 1.

Функции протоколов сетевых уровней

Наименование уровня	Наименование протокола	Функции протокола
7. Прикладной уровень	Протокол прикладного уровня	Управление вычислительными процессами, доступом к внешним устройствам, административное управление сетью
6. Представительный уровень	Протокол представительного уровня	Доступ к файлам данных и командным файлам (локальным), преобразование данных в требуемый формат, подготовка эмуляторов программ (команд) к работе
5. Сеансовый уровень	Протокол сеансового уровня	Формирование каталога сетевых процессов, установление логического соединения с удаленными процессами, завершение сеанса связи
4. Транспортный уровень	Протокол транспортного уровня	Передача файлов данных и доступ к удаленным файлам, передача и удаленное управление командными файлами, фрагментация и сборка передаваемых сообщений
3. Сетевой уровень	Протокол сетевого уровня	Установление и закрытие логических соединений через коммуникационную подсеть, управление потоками данных и маршрутами движения сообщений (пакетов)
2. Канальный уровень	Протокол канального уровня	Управление передачей и приемом сообщений (кадров), контроль ошибок, формирование сообщений (кадров)
1. Физический уровень	Протокол физического уровня	Установление и разъединение физических соединений, управление сигнализацией и тактированием

1.2.1. Физический уровень

Физический уровень определяет аппаратный интерфейс между компьютером и каналом связи, характеристики канала связи и способ обмена данными. Протокол физического уровня управляет процессом обмена данными по физическому каналу связи между удаленными компьютерами. Основными характеристиками канала связи являются пропускная способность и достоверность передачи данных.

Пропускная способность канала оценивается предельным числом бит данных, передаваемых по каналу за единицу времени, и измеряется в бит/с, Кбит/с (килобит/с), Мбит/с (мегабит/с), Гбит/с (гигабит/с).

Достоверность передачи данных характеризуется вероятностью искажения передаваемого бита. Основная причина искажений – воздейст-

вие внешних помех на линию связи и наличие шумов в аппаратуре передачи данных. В зависимости от типа канала связи, достоверность изменяется в пределах 10^{-4} ... 10^{-8} .

Канал связи содержит две основные компоненты: линии связи и аппаратуру передачи данных.

Линии связи. Используются следующие типы линий связи: кабельные, радиорелейные, радиоканалы, волоконно-оптические линии связи (ВОЛС), спутниковые системы связи (ССС).

Кабельные линии связи состоят из телефонных пар, коаксиальных кабелей и скрученных проводов (витая пара). Пропускная способность телефонных пар не превышает несколько десятков Кбит/с. Коаксиальный кабель и витая пара применяются при построении LAN. Скорость передачи данных в LAN на основе коаксиального кабеля составляет 10 Мбит/с, на основе витой пары – от 100 Мбит/с до 1 Гбит/с.

Радиорелейные линии связи и радиоканалы применяются в тех случаях, когда прокладка кабельных соединений экономически нецелесообразна либо практически невозможна. Скорость передачи данных в этом случае не превышает нескольких десятков Мбит/с.

ВОЛС, по сравнению с другими линиями связи, имеет ряд преимуществ, к которым относятся:

- устойчивость к электромагнитным излучениям;
- высокая пропускная способность (десятки Гбит/с);
- возможность передачи данных на большие расстояния (до 40 км) без повторителей;
- безопасность данных;
- малый вес и диаметр волокна.

Оптоволокно представляет собой тонкую нить из стекла (или пластика), которая служит средой передачи. В отличие от проводника, по оптоволокну передается свет вместо электрического сигнала. Схема преобразования электрического сигнала в световой и наоборот представлена на рис. 5.

Передатчик преобразует электрический сигнал в световой с помощью источника, в качестве которого используется светодиод или лазерный диод. Способ преобразования задается драйвером.

Оптоволокно служит средой для передачи светового сигнала.

Приемник состоит из двух частей: детектора-преобразователя светового сигнала в электрический и выходной цепи, предназначенной для усиления или преобразования электрического сигнала.

Коннекторы (разъемы) соединяют волокно оптического кабеля с источником, детектором или другим волоконно-оптическим кабелем.

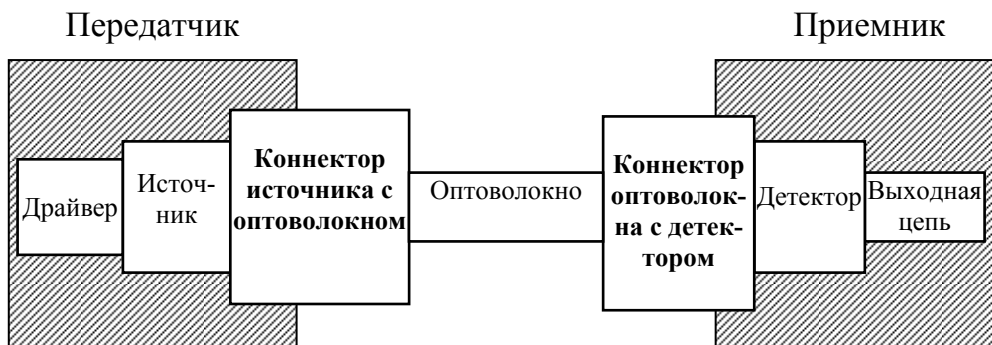


Рис. 5. Схема волоконно-оптического канала связи

Оптоволоконно включает в себя следующие элементы:

- световод, который изготавливается из стекла или пластика;
- специальное отражающее покрытие световода (например, серебро);
- многослойная оболочка для защиты от механических повреждений.

Существует два типа оптоволоконна: одномодовое и многомодовое.

Они различаются способом прохождения света.

В одномодовом волокне свет распространяется только прямо (рис. 6). Диаметр сечения световода такого волокна сравним с длиной волны. Сечение световода слишком мало (от 5 до 10 мкм), что исключает отклонение светового луча. Входной сигнал искажается минимально и несет минимальные потери. Одномодовое волокно удобно использовать при передаче сигнала на большие расстояния (до 40 км). Оно имеет бóльшую пропускную способность, чем многомодовое, но оно и дороже.

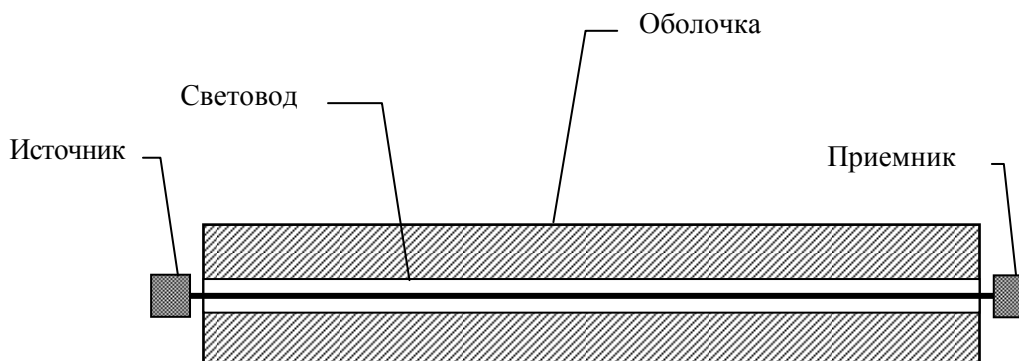


Рис. 6. Распространение света в одномодовом оптоволоконном световоде

Многомодовое волокно имеет меньшую пропускную способность и дальность передачи светового сигнала, но стоит дешевле, чем одномодовое волокно. Диаметр световода многомодового волокна значительно больше длины волны. Лучи света распространяются во все стороны и отражаются от стенок световода под разными углами, длина пути различных лучей за счет этого разная (рис. 7).

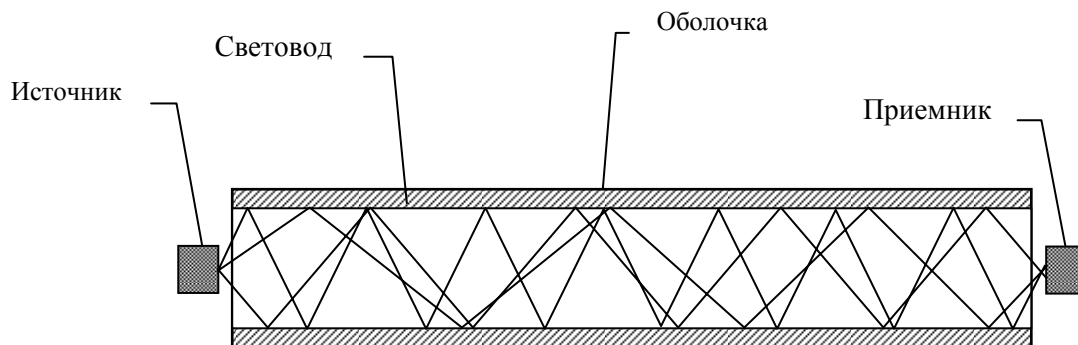


Рис. 7. Распространение света
в многомодовом оптоволоконном световоде

Таким образом, световой сигнал растягивается во времени, и возникает явление модальной дисперсии, которая ограничивает пропускную способность многомодового волокна и расстояние передачи (до 2 км). Диаметр световода многомодового волокна составляет от 50 до 85 мкм.

ССС являются наиболее эффективным средством связи компьютерных сетей, расположенных на значительном удалении друг от друга (свыше 500 км). В состав ССС входят спутники и наземное оборудование. Существуют два метода спутниковой связи: метод множественного доступа с частотным разделением (FDMA) и метод множественного доступа с временным разделением (TDMA).

FDMA предполагает одновременное использование многими абонентами выделенного участка спектра радиочастот. Применение этого метода сопряжено с определенными трудностями, так как необходимо спутниковое оборудование для одновременной обработки нескольких частот радиоканала. Кроме того, взаимная модуляция между несколькими несущими может привести к появлению искажений.

Существующая при частотном разделении проблема взаимной модуляции исключена в TDMA. В этом случае каждая наземная станция использует спутниковый передатчик в течение короткого промежутка времени, который определяется ее трафиком (поток данных). Синхронизация временных интервалов и передача данных в виде групп пакетов обеспечивают разделение единственного частотного канала между разными станциями.

Эти группы пакетов поступают на спутник, отделяемые друг от друга небольшими интервалами, называемыми временем переключения. В FDMA-системах для разделения каналов используют частоты переключений, которые выполняют те же функции, что и время переключения в TDMA, – исключение влияния соседних каналов друг на друга. Схему работы ССС по методу TDMA поясняет рис. 8.

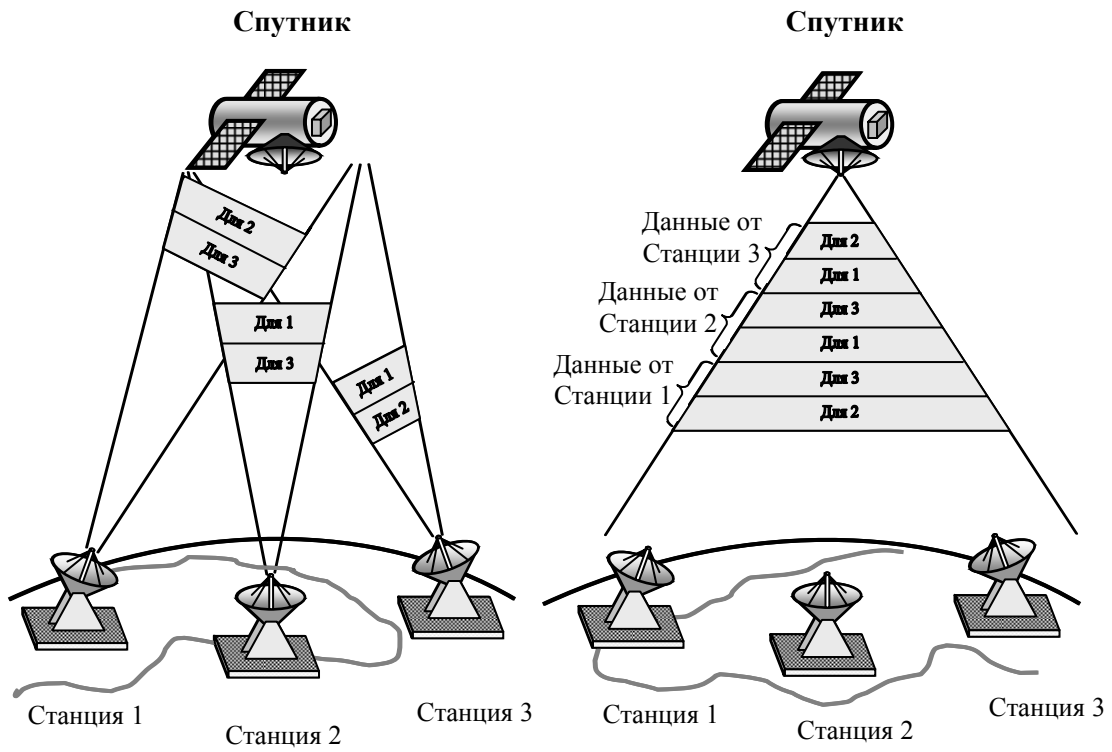
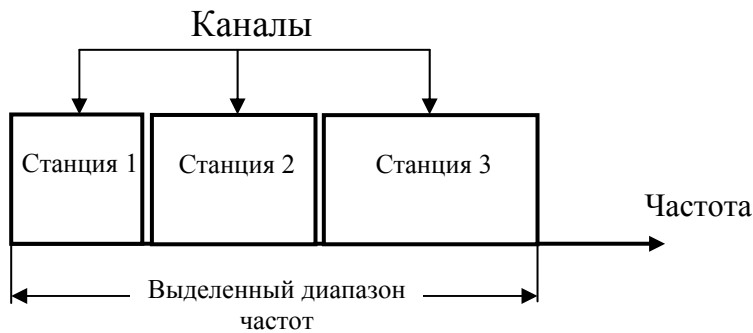
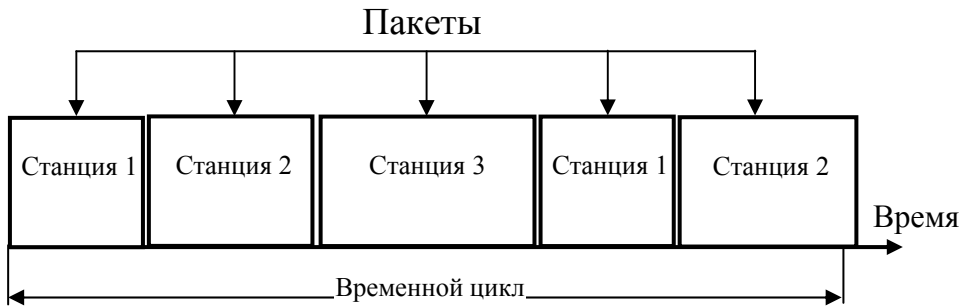


Рис. 8. Схема работы спутниковой системы связи по методу TDMA



FDMA – множественный доступ с частотным разделением



TDMA – множественный доступ с временным разделением

Рис. 9. Схемы разделения частот в FDMA и разделения времени в TDMA

Выходящие от станций группы пакетов двоичных данных адресованы некоторым другим станциям. При этом каждый пакет связан с определенным временным тактом. Часы наземных станций синхронизированы таким образом, что все станции используют по одному такту из общего цикла системы. Из-за малой длительности полного цикла пользователи не ощущают прерываний передачи. На спутнике частота сигнала меняется на выходную, и далее группы пакетов передаются наземным станциям, как и в случае FDMA. Станции получают все пакеты, проверяют их адреса и обрабатывают только те пакеты, которые адресованы непосредственно им.

Следует отметить, что в целом TDMA функционирует во временной области, как FDMA – в частотной. Сравнение работы этих двух методов поясняет рис. 9. В FDMA каждой станции выделяется некоторый участок полосы пропускания в зависимости от объема трафика этой станции. В TDMA каждой станции в соответствии с объемом ее трафика назначается временной интервал.

Аппаратура передачи данных. Состав аппаратуры передачи данных и тип ее физического интерфейса (стыка) с линией связи определяются типом компьютерной сети. Поэтому эти вопросы достаточно подробно рассмотрены в соответствующих разделах пособия, содержащих описание принципов построения и функционирования LAN, WAN и GAN.

1.2.2. Канальный уровень

Уровень управления каналом передачи данных устанавливает порядок взаимодействия между двумя соседними компьютерами (маршрутизаторами) по единственному каналу связи. Этот уровень имеет собственный протокол обмена. Структура соответствующего ему сообщения, которое называется кадром, приведена на рис. 10.

Начальный разделитель	Адрес назначения	Адрес отправления	Поле управления	Блок данных	Контрольная последовательность	Конечный разделитель
1	2	3	4	5	6	7

Рис. 10. Структура кадра данных протокола канального уровня

Начальный разделитель. Специальная кодовая последовательность, определяющая начало кадра в общем потоке данных.

Адрес назначения. Адрес компьютера (маршрутизатора), которому предназначен передаваемый кадр.

Адрес отправления. Адрес компьютера (маршрутизатора), который передал кадр.

Поле управления. Раздел кадра, содержащий характеристики процесса передачи данных.

Блок данных. Раздел кадра, содержащий передаваемые данные (программу) или их отдельную часть.

Контрольная последовательность. Кодовая последовательность, формируемая перед передачей кадра для разделов 2, 3, 4, 5 с использованием специальных математических преобразований и проверяемая при получении кадра.

Конечный разделитель. Специальная кодовая последовательность, определяющая конец кадра в общем потоке данных.

Протокол канального уровня выполняет следующие основные функции:

- формирование кадра заданного формата;
- передача и прием кадров;
- оптимизация процесса передачи кадров.

На рис. 10 представлена структура кадра данных в общем виде. Вместе с тем в компьютерных сетях существует значительное количество разнообразных протоколов канального уровня (HDLC, SDLC, BSC, SLIP, PPP и др.), каждый из которых имеет собственный формат кадра данных. Поэтому одной из основных функций протокола является формирование кадра заданного формата.

Процесс передачи и приема кадров осуществляется в следующей последовательности. Сформированный кадр отправляется в канал связи, и на таймере устанавливается тайм-аут. *Под тайм-аутом понимается время с момента отправки кадра в канал до момента получения кадра-подтверждения о правильности его приема.* Если в течение тайм-аута кадр-подтверждение не поступил, то переданный кадр считается потерянным либо принятым с ошибкой. В этом случае он передается повторно.

Принятый удаленным компьютером (маршрутизатором) кадр проходит этап обработки. При этом на удаленном компьютере (маршрутизаторе) должен быть установлен протокол канального уровня того же типа, что и на узле-передатчике. Вначале для разделов 2, 3, 4, 5 принятого кадра формируется контрольная последовательность и сравнивается с принятой контрольной последовательностью, которая содержится в разделе 6. Если они совпадают, то считается, что передача кадра прошла без ошибок, и он подлежит дальнейшей обработке. При этом формируется кадр-подтверждение и отправляется узлу-передатчику. В случае несовпадения контрольных последовательностей считается, что принят ошибочный кадр, и кадр-подтверждение не формируется.

При высоком качестве каналов связи целесообразно оптимизировать процесс передачи кадров. Оптимизация выполняется с помощью

настройки окна передачи данных. *Под окном передачи данных понимается количество переданных кадров на один кадр-подтверждение.* В современных протоколах канального уровня настройка окна передачи данных на качество канала связи выполняется автоматически.

1.2.3. Сетевой уровень

Этот уровень определяет общие аспекты создания и управления логическими соединениями и потоками данных и обеспечивает одновременное взаимодействие нескольких абонентов сети. Сетевому уровню соответствует сетевой протокол, реализующий следующие основные функции:

- коммутацию (соединение) абонентов компьютерной сети через коммуникационную подсеть;
- выбор и оптимизацию маршрутов передачи данных;
- управление потоками данных.

Процесс взаимодействия абонентов сети может осуществляться через коммуникационную подсеть с помощью коммутации каналов, сообщений и пакетов.

Реализация связи абонентов по *принципу коммутации каналов* осуществляется с помощью специальных устройств – коммутаторов. При этом устанавливаемый сквозной физический канал, проходящий через коммуникационную подсеть и соединяющий вступивших в связь абонентов, используется монопольно.

В случае второго способа связи (*коммутации сообщений*) сообщение последовательно через промежуточные коммуникационные узлы (маршрутизаторы) проходит путь от компьютера-источника к компьютеру-приемнику. Выбор маршрута следования сообщения осуществляется в каждом из промежуточных узлов (маршрутизаторов) и зависит от наличия свободного канала на пути следования к компьютеру-приемнику. Существенными недостатками метода коммутации сообщений являются значительные временные задержки в условиях интенсивного сетевого трафика (потока данных) и низкая эффективность использования ресурсов узлов коммутации (маршрутизаторов) и пропускных способностей каналов связи.

Коммутация пакетов позволяет в значительной степени избежать недостатков коммутации сообщений. Сущность этого метода заключается в разбиении передаваемого сообщения в компьютере-источнике на отдельные блоки (пакеты), размер которых определяется стандартным рядом: 64, 128, 256, 512, ..., 4096 байт. Затем пакеты перемещаются через коммуникационную подсеть независимо друг от друга в компью-

тер-приемник, где осуществляется сборка из принятых пакетов переданного сообщения.

Наибольшее распространение получили два метода коммутации пакетов: *датаграммный*, когда пакеты перемещаются через коммуникационную подсеть без предварительного определения пути их следования, и *виртуального* соединения, при котором перед передачей данных такой путь устанавливается и затем разрушается с окончанием передачи.

Следует отметить, что при передаче длинных сообщений коммутация каналов обеспечивает более высокую скорость передачи по сравнению с другими видами коммутации. Кроме того, коммутация каналов не требует наличия промежуточной памяти (буферов) в узлах коммутации.

При выборе стратегии маршрутизации, которая подразделяется на статическую и адаптивную, следует руководствоваться следующими соображениями.

Если технология сети не изменяется (из-за отказов, модификации, развития) и входные потоки данных стационарны, то выбирается статическая маршрутизация, которая характеризуется совокупностью фиксированных путей между всеми парами узлов. Трафик между каждой парой источник–адресат может быть распределен одновременно по нескольким путям во вполне определенных, фиксированных во времени, пропорциях. Однако в условиях реальной сети топология со временем изменяется, а входные данные пользователей имеют тенденцию к колебаниям во времени. Поэтому для минимизации задержек необходимо реализовать некоторую адаптивную стратегию маршрутизации, позволяющую реагировать на изменения состояния сети.

Выбор маршрутов движения сообщений через коммуникационную подсеть осуществляется на основе данных таблиц маршрутизации, которые находятся в узлах коммутации (рис. 11). Структура таблицы маршрутизации приведена на рис. 12.

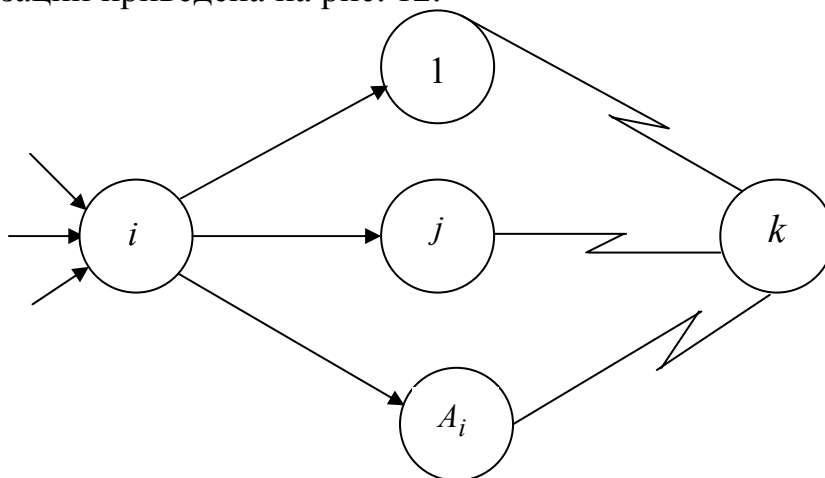


Рис. 11. Схема информационных потоков от узла i к узлу k

	1	2	•	j	•	A_i
1	$P^i(1,1)$	$P^i(1,2)$	•	$P^i(1,j)$	•	$P^i(1, A_i)$
•	•••	•••	•	•••	•	•••
k	$P^i(k,1)$	$P^i(k,2)$	•	$P^i(k,j)$	•	$P^i(k, A_i)$
•	•••	•••	•	•••	•	•••
N	$P^i(N,1)$	$P^i(N,2)$	•	$P^i(N,j)$	•	$P^i(N, A_i)$

Рис. 12. Таблица маршрутизации узла i

Таблица маршрутизации указывает, как, в зависимости от конечного адресата, должен быть распределен по выходным линиям трафик, поступающий в данный узел. Маршрутная таблица для узла i представляет собой некоторую матрицу $P^i(.,.)$ размерностью $N \times A_i$, где N – число узлов коммутации в сети, а A_i – число соседей узла i . Матрица $P^i(k, j)$ – это часть трафика, адресованного в узел k , который при поступлении в узел i направляется через соседний узел j . Тогда справедливо следующее выражение:

$$\sum_{j=1}^{A_i} P^i(k, j) = 1, A_i.$$

При *статической маршрутизации* содержимое таблиц маршрутизации не изменяется либо изменяется достаточно редко.

При *адаптивной стратегии* маршрутизации значения $P^i(k, j)$ будут изменяться во времени. Существуют следующие типы адаптивной стратегии.

Изолированная стратегия. Маршруты вычисляются каждым узлом независимо, на основе локальной информации (состояние очередей к выходным линиям, приоритет выходных линий и т. д.). Между узлами не производится обмена ни маршрутной информацией, ни информацией о состоянии узлов.

Распределенная стратегия. Маршруты вычисляются параллельно и согласовываются всеми узлами на основе неполной информации об их состоянии, которой они обмениваются.

Централизованная стратегия. Сетевой маршрутный центр (СМЦ) собирает глобальную информацию о состоянии сети, вычисляет маршруты минимальной задержки и корректирует или распределяет маршрутные таблицы (или маршрутные команды) по всем узлам.

Смешанная стратегия. Эта стратегия включает в себя свойства всех предыдущих стратегий или их комбинацию. Например, она может объединять изолированную и централизованную стратегии маршрутизации.

Управление потоком данных. При передаче данных между абонентами сети возникает состязание за сетевые ресурсы (каналы связи, буфера приема-передачи, узлы коммутации). Если состязание за эти ресурсы не контролируется, то возникают следующие проблемы: падение эффективности, несправедливое распределение ресурсов и перегрузки.

Пример неэффективного использования ресурсов приведен на рис. 13.

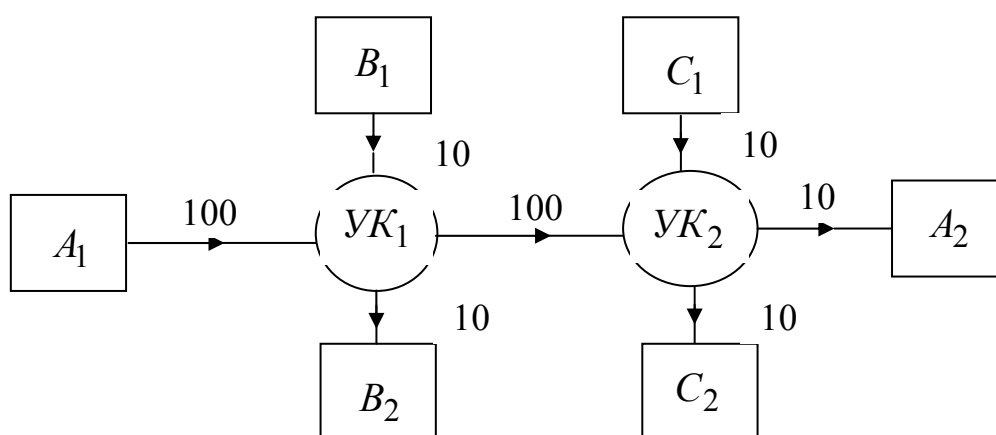


Рис. 13. Пример неэффективного распределения сетевых ресурсов

На рис. 13 представлена двухузловая сеть, состоящая из двух узлов коммутации UK_1, UK_2 и подключенных к нему компьютеров $A_1, A_2, B_1, B_2, C_1, C_2$. Цифрами указаны скорости передачи данных. Предположим, что первоначально от компьютера A_1 к компьютеру A_2 передача данных не ведется. Тогда общая производительность сети, равная 20 единицам, определяется передачей от компьютеров B_1 к B_2 и C_1 к C_2 . Допустим, что в некоторый момент времени открылась передача данных из компьютера A_1 к компьютеру A_2 . Из-за несогласованности скоростей передачи данных в линиях связи буфера приема-передачи в узлах коммутации быстро наполняются трафиком от компьютера A_1 . Следовательно, пакеты из B_1 и C_1 сбрасываются узлами коммутации (переполнение буферов), и производительность передачи по линиям связи B_1, B_2 и C_1, C_2 падает до нуля. Введение нового трафика вызывает уменьшение суммарной производительности сети с 20 до 10 единиц. Это падение эффективности вызвано неэффективным расходом буферной памяти трафиком A_1, A_2 (захват буферов).

Сеть считается перегруженной, если некоторое приращение внешнего трафика вызывает уменьшение ее производительности. В условиях перегрузки работа сети нежелательна по двум причинам: из-за падения эффективности и возникновения блокировок.

Блокировки представляют собой такое событие, при котором производительность сети или ее отдельных фрагментов падает до нуля. Блокировки подразделяются на два типа: прямые и косвенные.

Пример прямой блокировки приведен на рис. 14.

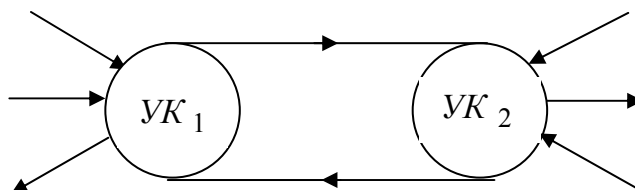


Рис. 14. Пример прямой блокировки передачи данных

Если узел UK_1 наполнен адресованными к узлу UK_2 пакетами, а узел UK_2 наполнен адресованными к узлу UK_1 пакетами, то по линии UK_1-UK_2 , не может пройти никакой трафик. Эту тупиковую ситуацию часто называют прямой блокировкой передачи с промежуточным накоплением.

Простым решением проблемы возникновения прямой блокировки является ограничение очереди к линии связи Q_{\max} . Если очередь в линию связи $i \geq Q_{\max}$ (где Q_{\max} меньше суммарного количества буферов узла), рассматриваемый узел объявляется перегруженным для входного трафика, направленного в линию i . Эта стратегия, называемая стратегией ограничения канальных очередей, исключает возможность возникновения прямых блокировок, поскольку пакеты узла UK_1 , направленные к узлу UK_2 , не могут занять весь буферный пул в узле UK_1 . При этом защита от перегрузок узлов UK_1, UK_2 выполняется протоколом управления каналом передачи данных, который осуществляет автоматический сброс пакетов на приемной стороне (если приемник перегружен) и последующую их повторную передачу после тайм-аута. Этот процесс продолжается до тех пор, пока перегрузка узла не исчезнет.

Существует другой вид блокировки, которая может возникнуть в пакетных сетях, – *косвенная блокировка*. Этот вид блокировки поясняет рис. 15.

Предположим, что создались неблагоприятные условия распределения трафика в сети кольцевой топологии, приведенной на рис. 15.

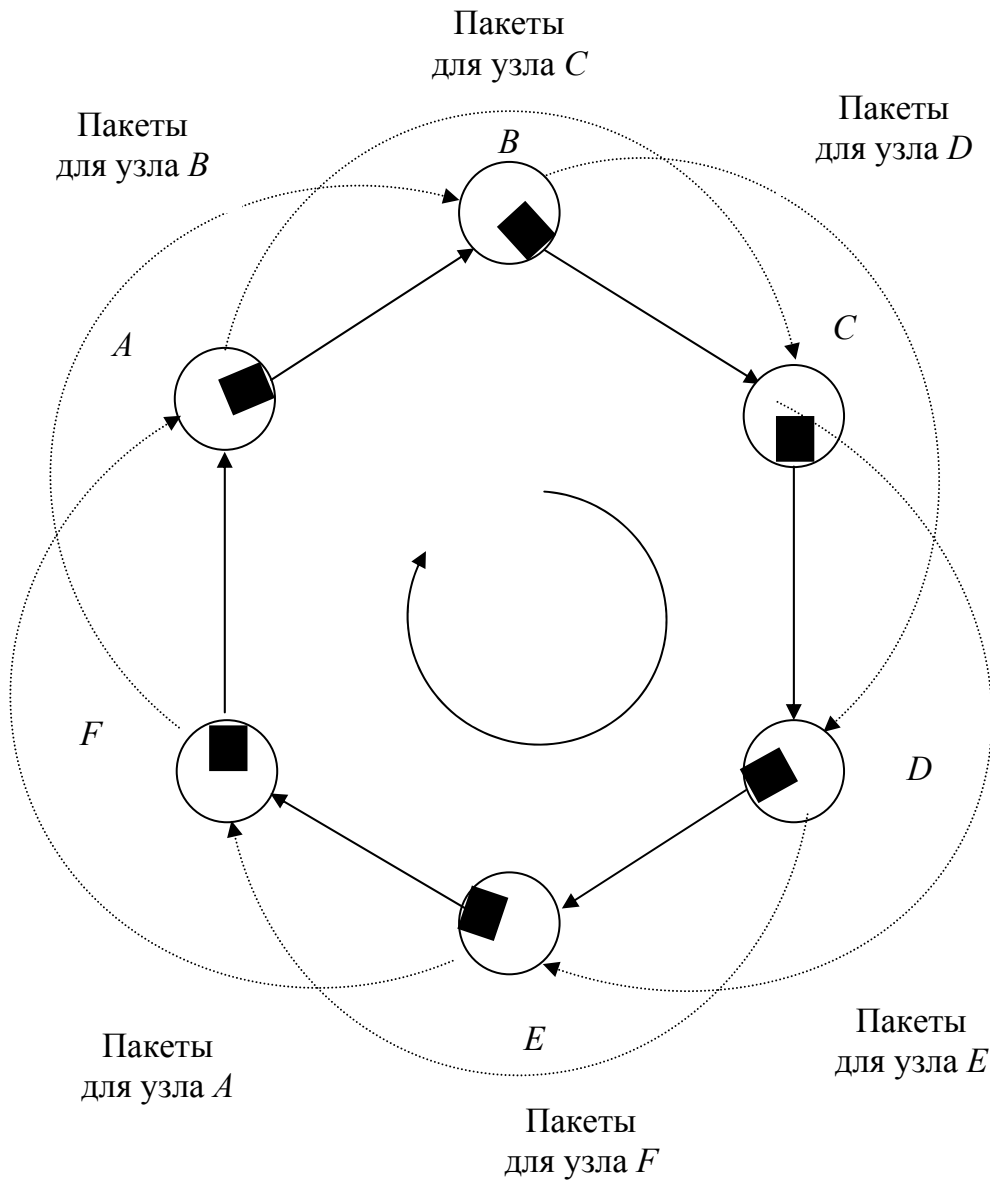


Рис. 15. Пример косвенной блокировки передачи

В результате этого произошло заполнение каждой очереди пакетов до уровня Q_{\max} , т. е. предела, определяемого стратегией ограничения канальных очередей. Кроме этого, предположим, что в каждом узле находятся пакеты, адресованные узлу, находящемуся через два или более транзитных участка (например, все пакеты, находящиеся в очереди к линии AB , адресованы узлу C). В этих условиях в сети не сможет передаваться никакой трафик, поскольку все очереди равны Q_{\max} . Таким образом, существует тупиковая ситуация, несмотря на то что сеть снабжена механизмом предотвращения прямых блокировок, т. е. стратегией ограничения канальных очередей. Такой вид блокировки называется косвенной блокировкой.

Для предотвращения косвенных блокировок применяется стратегия структурированного буферного пула. Согласно этой стратегии буферы узлов организованы в иерархическую структуру, которая приведена на рис. 16.



Рис. 16. Структурированный буферный пул

На нулевом уровне имеется пул неограниченных для использования буферов. От уровня 1 до уровня H_{\max} (где H_{\max} – максимальное число транзитных участков на любом пути в сети) буферы резервируются для пакетов конкретного класса. В частности, буферы уровня i резервируются для пакетов, которые преодолели i транзитных участков. Таким образом, в условиях большой нагрузки буферы постепенно заполняются от уровня 0 до H_{\max} . Когда на узле буферы уровня $\leq i$ заполнены, поступающие пакеты, прошедшие $\leq i$ транзитных участков, сбрасываются, что исключает прямую и косвенную блокировки.

Для создания структурированного буферного пула в каждом узле требуется H_{\max} буферов ($H_{\max} = N - 1$, где N – число узлов коммутации), а также поддержка его работы.

1.2.4. Транспортный уровень

Этот уровень оговаривает порядок передачи и доступа к удаленным файлам. Протокол транспортного уровня выполняет следующие функции:

- фрагментацию и сборку передаваемых файлов;
- передачу файлов данных и доступ к удаленным файлам;
- передачу и удаленное управление командными файлами.

1.2.5. Сеансовый уровень

Этот уровень устанавливает порядок взаимодействия двух удаленных процессов (программ). При выполнении протокола этого уровня осуществляется:

- формирование каталога сетевых процессов;
- установление логических связей с другими удаленными процессами;
- завершение сеанса взаимодействия удаленных процессов.

1.2.6. Представительный уровень

Уровень представления данных определяет порядок доступа к данным и программам, расположенным на местном (локальном) компьютере пользователя, подключенном к сети. Протокол этого уровня реализует следующие основные функции:

- доступ к файлам данных и командным файлам компьютера пользователя;
- преобразование данных в формат, необходимый для решения сетевой задачи;
- подготовку эмуляторов программ (команд) к работе.

1.2.7. Прикладной уровень

Протокол этого уровня определяет порядок использования информационных и вычислительных ресурсов компьютера пользователя. Под его управлением осуществляется:

- решение информационно-вычислительных задач;
- доступ и управление устройствами ввода-вывода;
- административное управление сетью.

Семиуровневая модель ISO/OSI была разработана в период с 1977 по 1984 год. К этому времени уже были созданы реальные компьютерные сети (в том числе сеть ARPANET – прототип сети INTERNET), архитектура которых отличается от модели ISO/OSI. Поэтому модель ISO/OSI не является стандартом, а служит в качестве рекомендаций для построения конкретных компьютерных сетей.

1.3. Организация взаимодействия абонентов компьютерной сети

Процесс передачи сообщений можно разбить на три этапа:

- установление логической связи между удаленными процессами (программами);
- передача сообщений (файлов данных и командных файлов);
- завершение сеанса связи.

На первом этапе устанавливается логический канал между системами и выполняется обмен сообщениями о конфигурациях операционных систем, их версиях для проверки совместимости и возможности переноса программ с одного компьютера на другой. Затем осуществляется передача идентификатора пользователя, его пароля и учетной информации. На основании этих данных пользователь получает разрешение доступа к ресурсам удаленной системы. Ему сообщаются характеристики устройств и файловой системы, атрибуты и порядок предоставления данных в затребованном файле.

Второй этап передачи данных включает в себя последовательную выборку записей по ключам из затребованного файла и формирование сообщений, содержащих текст записей. При этом передача данных продолжается до наступления одного из трех событий:

- при чтении очередной записи обнаружен конец файла;
- в запросе указан ключ несуществующей записи, или она не может быть прочитана;
- очередной запрос содержит признак окончания доступа.

Завершение сеанса связи (доступа к файлу) осуществляется следующим образом.

Если обнаружен конец файла, то пользователю отправляется сообщение с кодом «конец файла» и «доступ закончен». После получения ответа от пользователя вторичная система отсоединяется либо иницирует доступ к другому файлу.

Во втором случае пользователь, получив сообщение об ошибке или невозможности прочитать запись, может исправить ошибку и продолжить передачу или завершить сеанс связи.

Третий случай имеет место, когда инициатива завершения сеанса связи принадлежит пользователю сети (первичной системе).

Передача и прием данных в компьютерной сети выполняется под управлением сетевых протоколов. Каждому сетевому уровню соответствует свой собственный протокол. Схема взаимодействия протоколов компьютерной сети модели ISO/OSI представлена на рис. 17.



Рис. 17. Схема взаимодействия протоколов компьютерной сети модели ISO/OSI

Решение сетевой задачи начинается с работы протокола прикладного уровня. Он анализирует структуру задачи (программы) и определяет, содержит ли она команды обращения к удаленным компьютерам, содержащим файлы данных и программы, необходимые для решения данной задачи. Если таких команд в программе не содержится, то управление передается операционной системе и решается локальная задача. В противном случае задача объявляется сетевой и управление передается протоколу представительного уровня, который формирует каталог удаленных файлов и программ (каталог информационных входов) и передает управление протоколу сеансового уровня.

Может иметь место другой тип сетевой задачи, когда пользователь желает передать на удаленный компьютер командный файл (программу)

и осуществить его удаленный запуск либо передать данные по определенному регламенту. В этом случае протокол представительного уровня составляет отдельный каталог (каталог информационных выходов) и совершает переход к протоколу сеансового уровня.

Основной задачей протокола сеансового уровня является подготовка условий (среды) для решения сетевой задачи. Для этого необходимо, чтобы удаленные файлы и программы были приняты и размещены на компьютере пользователя (первый тип сетевой задачи) либо файлы пользователя подготовлены для передачи на удаленный компьютер (второй тип сетевой задачи). Протокол сеансового уровня на основе каталогов информационных входов и выходов формирует каталог сетевых процессов и для каждого из них устанавливает логическое соединение с удаленными системами изложенным ранее способом. Затем для каждого процесса осуществляется прием-передача данных. При этом протоколы всех уровней выполняются в последовательности, указанной стрелками на рис. 17: сверху вниз при передаче и снизу вверх при приеме.

Процесс преобразования данных выполняется следующим образом (рис. 18).

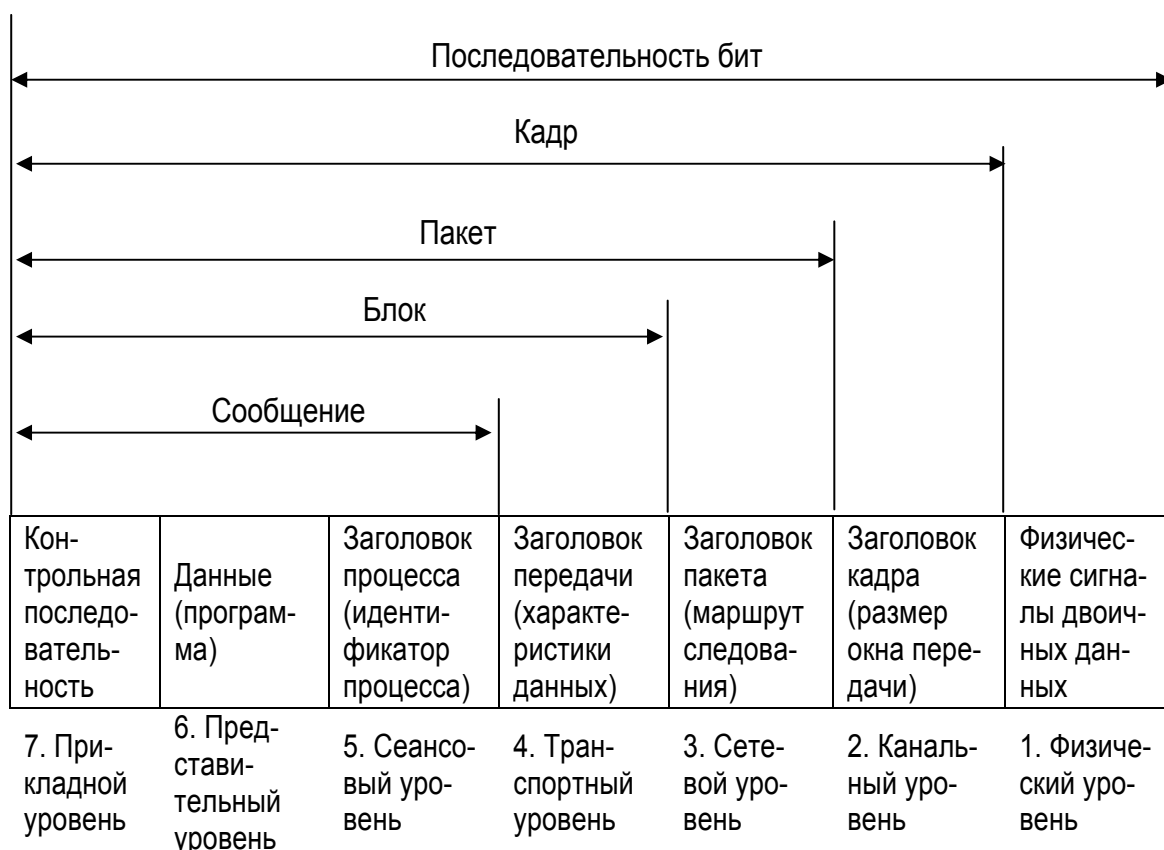


Рис. 18. Процесс преобразования передаваемых данных в компьютерной сети модели ISO/OSI

В общем случае передаваемое сообщение может быть достаточно большим. С точки зрения эффективности передачи имеет смысл разбивать длинные сообщения на фрагменты и передавать их независимо друг от друга через коммуникационную подсеть, а затем на удаленном компьютере осуществлять сборку из принятых фрагментов исходного сообщения. Эта функция осуществляется протоколом транспортного уровня. При этом каждый фрагмент (блок) сообщения имеет наряду с заголовком процесса заголовок передачи, включающий в себя характеристики передаваемого блока.

На следующем этапе передачи данных выполняется протокол сетевого уровня. Он формирует из блоков пакеты, в заголовках которых указываются адреса взаимодействующих абонентов (адреса компьютера пользователя и удаленного компьютера) при датаграммном способе передачи данных, и дополнительно указывается маршрут следования пакетов через коммуникационную подсеть, если применяется метод виртуальных соединений (каналов).

На канальном уровне к пакету добавляется заголовок кадра. Этот заголовок содержит сведения о числе переданных и принятых кадров и размере окна передачи. Кроме того, для него формируется контрольная последовательность и начальный и конечный разделители.

Перед отправлением кадра в канал связи он преобразуется в последовательность бит. Протокол физического уровня управляет синхронизацией и тактированием при передаче двоичных данных по физической линии.

Поступающая по физическому каналу последовательность бит претерпевает обратное преобразование, включая сборку из фрагментов (пакетов) принятого сообщения. Затем выполняется процесс приема-передачи следующего файла или программы.

После того как протокол сеансового уровня завершит все процессы приема-передачи удаленных файлов и программ, он передает управление протоколу представительного уровня, который осуществляет преобразование данных в требуемый формат и (при необходимости) загружает в оперативную память эмуляторы программ. Протокол прикладного уровня совместно с операционной системой управляет решением сетевой задачи.

Приведенная схема взаимодействия удаленных компьютеров через коммуникационную подсеть справедлива только для модели ISO/OSI. Сетевые модели и схемы функционирования конкретных LAN, WAN и GAN имеют ряд существенных отличий, которые достаточно подробно изложены в последующих разделах пособия.

Методические указания

Этот раздел пособия необходим для понимания общих принципов построения и функционирования компьютерной сети. Он содержит следующие ключевые моменты:

- компьютерные сети играют важную роль в информационной экономике, которая приходит на смену индустриальной;
- компьютерная сеть представляет собой два или более компьютеров, соединенных между собой и способных обмениваться сообщениями;
- компьютерные сети делятся на локальные (LAN), региональные (WAN) и глобальные (GAN);
- LAN располагается в пределах отдельных зданий и сооружений и имеет сетевую топологию типа шина, звезда, кольцо;
- WAN объединяет LAN в рамках отдельных регионов и областей с помощью специальных устройств типа мост, маршрутизатор и шлюз;
- GAN включает в себя WAN, национальные сети стран, материков. Самой мощной GAN является сеть Internet, содержащая сотни миллионов компьютеров;
- компьютерная сеть состоит из двух основных компонентов: коммуникационной подсети и сетевых абонентов;
- коммуникационная подсеть предназначена для обеспечения соединения сетевых абонентов между собой и содержит коммуникационные узлы (маршрутизаторы) и каналы связи;
- сетевые абоненты представляют собой LAN, мощные многопроцессорные HOST-компьютеры, персональные компьютеры, подключенные к коммуникационной подсети;
- взаимодействие абонентов компьютерной сети осуществляется с помощью сетевых протоколов;
- сетевой протокол представляет собой строго формализованную процедуру взаимодействия сетевых абонентов через коммуникационную подсеть;
- сетевая модель ISO/OSI содержит семь функциональных уровней, каждому из которых соответствует свой собственный сетевой протокол;
- физический уровень управляет передачей двоичных данных по каналам связи, состоящим из линий связи (систем связи) и аппаратуры передачи данных;
- канальный уровень формирует кадры данных и управляет их передачей между двумя соседними компьютерами (маршрутизаторами);

- сетевой уровень выполняет функции коммутации (соединения) сетевых абонентов, маршрутизации пакетов и управления потоками данных через коммуникационную подсеть;
- транспортный уровень осуществляет фрагментацию и сборку передаваемых сообщений, удаленный доступ к файлам данных, передачу и удаленный запуск командных файлов;
- сеансовый уровень формирует каталог сетевых процессов (приема-передачи данных) и управляет их выполнением;
- представительный уровень формирует каталог передаваемых (выходных) и удаленных (входных) файлов, а также осуществляет преобразование входных файлов в формат, необходимый для решения сетевой задачи;
- прикладной уровень совместно с операционной системой осуществляет решение сетевой задачи;
- процесс взаимодействия абонентов компьютерной сети заключается в последовательном выполнении протоколов сетевых уровней: сверху вниз при передаче и снизу вверх при приеме.

Глава 2

ЛОКАЛЬНЫЕ КОМПЬЮТЕРНЫЕ СЕТИ

2.1. Общие принципы построения локальных компьютерных сетей

Локальная компьютерная сеть (LAN) – это коммуникационная система, расположенная в пределах отдельного здания или другой ограниченной территории, поддерживающая один или несколько высокоскоростных цифровых каналов связи, предоставляемых подключенным к ней компьютерам в кратковременное монопольное использование.

LAN имеет следующие характеристики:

- общая протяженность LAN составляет несколько тысяч метров;
- скорость передачи данных изменяется в пределах от нескольких Мбит/с до нескольких Гбит/с;
- LAN позволяет осуществлять простое подключение новых компьютеров и отключение старых без нарушения работы сети;
- для устройств коллективного доступа (например, серверов) в LAN обеспечен равноправный доступ для всех компьютеров;
- вероятность передачи пакета, содержащего необнаруженную ошибку, составляет $10^{-14} \dots 10^{-16}$.

Комитетом по стандартизации LAN IEEE (Institute of Electrical and Electronic Engineers) был разработан проект стандарта LAN, который получил название стандарт 802. Как и модель ISO/OSI, модель LAN стандарта IEEE 802 содержит основные рекомендации, которыми следует руководствоваться при построении конкретных LAN.

При разработке стандарта IEEE 802 за основу была принята модель ISO/OSI. Комитет по LAN выполнил дальнейшую декомпозицию уровней 1 и 2. Основные отличия моделей ISO/OSI и IEEE 802 представлены на рис. 19.

В модели IEEE 802 канальный уровень делится на два подуровня: управление логическим каналом LLC (Logical Link Control) и управление доступом к передающей среде MAC (Medium Access Control). В функции LLC входит передача кадров между станциями, включая исправление ошибок. LLC не зависит от алгоритмов доступа к среде. MAC реализует алгоритм доступа к среде и задает адресацию станций. Кроме того, модель IEEE 802, в отличие от семиуровневой модели ISO/OSI, характеризуется наличием средств для широковещательных передач.

7. Прикладной уровень	7. Прикладной уровень
6. Представительный уровень	6. Представительный уровень
5. Сеансовый уровень	5. Сеансовый уровень
4. Транспортный уровень	4. Транспортный уровень
3. Сетевой уровень	3. Сетевой уровень
2. Канальный уровень	2.2. Управление логическим каналом (LLC)
	2.1. Управление доступом к среде (MAC)
	1.3. Передача физических сигналов (PS)
	1.2. Интерфейс с устройством доступа (AUI)
1. Физический уровень	1.1. Средства подключения к физической среде (PMA)
	0. Физическая среда

Модель ISO/OSI
Модель IEEE 802

Рис. 19. Модель ISO/OSI компьютерной сети общего назначения и модель IEEE 802 локальной компьютерной сети

Физический уровень делится на три подуровня: передача физических сигналов PS (Physical Signalling), интерфейс с устройством доступа AUI (Access-Unit Interface) и подключение к физической среде PMA (Physical Medium Attachment).

PS выделяется с целью облегчения схемной интеграции с канальным уровнем. PMA согласует сигналы из PS с требованиями передающей среды, обеспечивая тем самым возможность использования определенного PS с несколькими различными типами передающей среды. AUI представляет собой кабель и позволяет размещать PS (и подключенный компьютер) на некотором расстоянии от передающей среды.

В модели IEEE 802 введен нулевой уровень, определяющий физическую среду передачи данных.

Определим характеристики LAN в рамках модели IEEE 802.

2.1.1. Физическая среда передачи данных

В LAN применяются различные типы линий связи: коаксиальный кабель, витая пара, ВОЛС, инфракрасные и радиоканалы. Основные характеристики перечисленных линий связи (за исключением инфракрасных каналов) приведены в разделе 1.2.1. Инфракрасные каналы находят ограниченное применение, так как имеют малую дальность передачи. Описание современной беспроводной технологии соединения компьютеров в локальную сеть и подключения их к Internet (Wi-Fi) приведено в заключительной (пятой) главе пособия.

2.1.2. Физический уровень

Линия связи определяет тип устройства (РМА), с помощью которого компьютер подключается к физической среде для обмена сигналами с удаленными компьютерами. Общая структура РМА определяется топологией LAN и принципами передачи сигналов.

В связи с тем, что устройства, реализующие РМА, иногда устанавливаются в фальшпотолках и других труднодоступных местах, их делают предельно простыми. Из этих соображений кодирование и декодирование сигнала включено в подуровень передачи физических сигналов PS. Электронные схемы реализации этого подуровня, как правило, размещаются в компьютере (станции). Модули РМА и PS соединяются интерфейсным кабелем АUI, длина которого может достигать 50 метров.

Кодирование физических сигналов в LAN осуществляется в основном двумя способами: манчестерского кодирования и дифференциального манчестерского кодирования (рис. 20).

И при манчестерском, и при дифференциальном манчестерском кодировании смена уровня сигнала производится один раз для каждого бита в середине интервала времени, отведенного для его передачи. При манчестерском кодировании всегда происходит смена уровня вверх для 1 и вниз для 0. При дифференциальном манчестерском кодировании перепад для 0 имеет то же направление, что и в предыдущем битовом интервале, а для 1 – обратное. Благодаря большой частоте перепадов уровня упрощается синхронизация, а также допускается пропуск некоторых перепадов, используемых как сигналы управления.

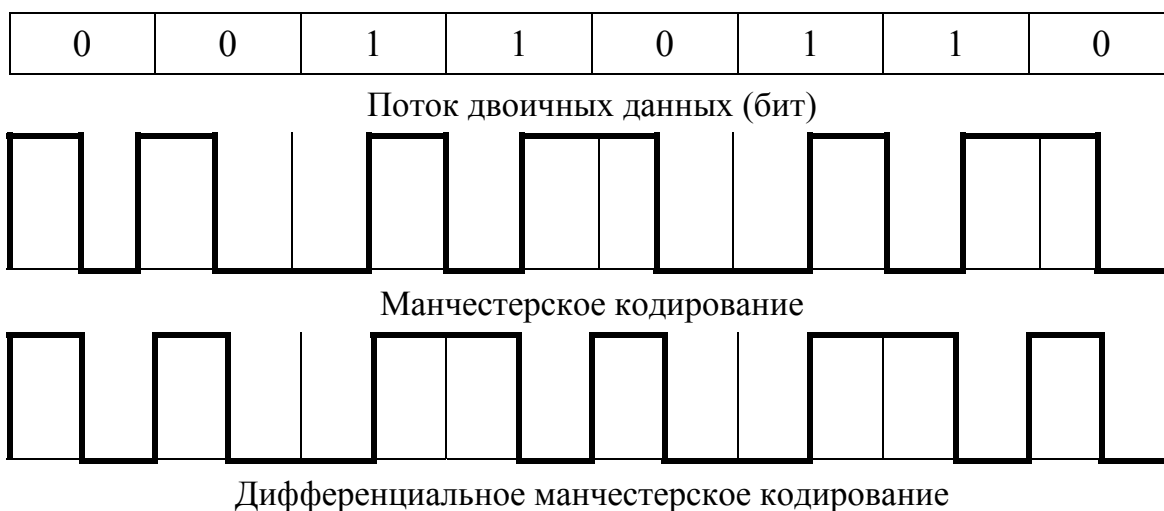


Рис. 20. Методы кодирования двоичных сигналов в локальной компьютерной сети

2.1.3. Канальный уровень

В зависимости от способа передачи данных сети LAN бывают следующих типов:

- с доступом к каналу связи в режиме соперничества (множественным доступом);
- с передачей маркера (пакета, дающего право на передачу данных);
- с опросом;
- со вставкой регистра;
- с резервированием времени передачи;
- широкополосные.

В большинстве LAN в любой момент времени только один компьютер (станция) передает данные, все остальные работают на прием.

В настоящее время наибольшее распространение получили LAN, имеющие топологию типа шина, звезда и кольцо с множественным доступом и передачей маркера. Поэтому в пособии основное внимание уделяется принципам построения этих типов LAN.

Канальный уровень модели IEEE 802 делится на два подуровня: управление логическим каналом LLC и управление доступом к среде MAC (рис. 21).

Управление логическим каналом	Подуровень LLC IEEE 802.2	Подуровень LLC IEEE 802.2	Подуровень LLC IEEE 802.2
Управление доступом к среде	Подуровень MAC IEEE 802.3 Множественный доступ с контролем несущей и обнаружением столкновений (CSMA/CD)	Подуровень MAC IEEE 802.4 Передача маркера	Подуровень MAC IEEE 802.5 Передача маркера
Физический уровень	Шина, звезда	Шина, звезда	Кольцо

Рис. 21. Структура канального уровня модели IEEE 802

Подуровень LLC не зависит от типа сетевой топологии и конкретного метода доступа. Этому подуровню соответствует стандарт IEEE 802.2. Структура блока данных подуровня LLC представлена на рис. 22. Она включает в себя следующие основные разделы.

Адрес назначения. Адрес удаленного процесса (программы), с которым взаимодействует данный процесс (программа).

Адрес отправления. Адрес процесса (программы) отправителя сообщения.

Поле управления. Содержит порядковые номера переданных и принятых пакетов (кадров).

Информационное поле. Содержит передаваемую информацию.

Адрес назначения	Адрес отправления	Поле управления	Информационное поле
1	2	3	4

Рис. 22. Структура блока данных подуровня LLC

Подуровень MAC определяет тип сетевой топологии и метод доступа к каналу передачи данных. Он содержит три основных стандарта LAN:

1. *Стандарт IEEE 802.3.* Определяет стандарт на LAN шинной или звездообразной топологии, в которой применяется множественный доступ с контролем несущей и обнаружением столкновений (CSMA/CD). Практической реализацией этого стандарта является LAN Ethernet.

2. *Стандарт IEEE 802.4.* Определяет стандарт на LAN шинной или звездообразной топологии, в которой применяется маркерный метод доступа. Практической реализацией этого стандарта является LAN ARCnet.

3. *Стандарт IEEE 802.5.* Определяет стандарт на LAN кольцеобразной топологии, в которой применяется маркерный метод доступа. Практической реализацией этого стандарта является LAN Token Ring.

Для каждого перечисленного стандарта кадр данных подуровня MAC имеет свою структуру. Она приведена в разделах пособия, содержащих описание конкретных LAN, построенных на основе модели IEEE 802.

Разбиение канального уровня на два подуровня LLC и MAC дает ряд преимуществ в организации построения и функционирования LAN.

Протокол подуровня LLC является универсальным для любой конфигурации LAN с любым методом доступа. Он реализуется программно и легко может быть установлен на компьютере, подключенном к сети.

Протокол подуровня MAC определяет конфигурацию LAN и метод доступа к каналу передачи данных. Он реализуется аппаратно в виде отдельного блока либо электронной платы (сетевого контроллера), размещаемой непосредственно в корпусе компьютера (станции).

2.1.4. Верхние уровни модели IEEE 802

К верхним уровням модели IEEE 802 относятся сетевой, транспортный, сеансовый, представительный и прикладной (см. рис. 19). Эти уровни соответствуют модели ISO/OSI и не зависят от конфигурации LAN и методов доступа к каналу передачи данных. Сетевое программное обес-

печение, реализующее протоколы верхних уровней, является универсальным и может применяться как в LAN различных типов, так и WAN и GAN. Однако LAN, по сравнению с WAN и GAN, имеет простую топологию (шина, звезда и кольцо) и простой способ взаимодействия удаленных станций: в любой момент времени только одна станция передает данные, все остальные работают на прием. Поэтому в LAN для взаимодействия удаленных станций достаточно функций протокола канального уровня, так как нет необходимости решать сложные задачи выбора и оптимизации маршрутов передачи данных через коммуникационную подсеть и управления трафиком (поток данных). В WAN и GAN эти функции выполняет протокол сетевого уровня.

С учетом этих обстоятельств в разделы пособия по применению модели IEEE 802 для построения конкретных LAN включены только вопросы реализации канального уровня. Описание протоколов сетевого и других верхних уровней содержится в разделах пособия по методам построения WAN и GAN.

2.2. Локальная компьютерная сеть Ethernet

Одной из самых распространенных LAN является сеть Ethernet, разработанная фирмой Xerox совместно с фирмами DEC и Intel в 1980 году. В основе LAN Ethernet лежит стандарт IEEE 802.3, спецификации которого содержат описание сети шинной топологии с множественным доступом, контролем несущей (физического сигнала передачи данных) и обнаружением столкновений (CSMA/CD). В дальнейшем, с развитием передающей среды и аппаратных средств, она нашла применение в двух конфигурациях: шинной и звездообразной. На момент создания LAN Ethernet скорость передачи данных составляла 10 Мбит/с. Реализация стандарта IEEE 802.3 в рамках сети Ethernet выполнена следующим образом.

2.2.1. Физическая среда передачи данных

В качестве среды передачи данных в LAN Ethernet используются коаксиальный кабель, витая пара и ВОЛС.

Коаксиальный кабель, как правило, применяется для построения LAN Ethernet шинной топологии. Он имеет волновое сопротивление 50 Ом, обычно прокладывается в желобах или фальшпотолках и состоит из участков, не превышающих по длине 500 м. Одна LAN Ethernet может включать любое число участков, соединенных повторителями, при условии, что между двумя какими-либо станциями существует только один соединяющий их путь и этот путь содержит не более 1500 м коаксиального кабеля. Для минимизации отражения, которое может быть

воспринято как конфликт, каждый участок снабжается терминатором и согласуется по волновому сопротивлению с остальным кабелем. Высокая скорость передачи данных диктует необходимость минимизации потерь, обусловленных отражением в кабеле. Эти ограничения должны соблюдаться при выборе участков для подключения станций. Интервалы между ними должны составлять не менее 2,5 м. Кроме того, для функционирования системы обнаружения конфликтов экранирующая оплетка кабеля не должна быть заземлена.

Витая пара (UTP-cables) представляет собой кабель, состоящий из пар скрученных медных проводов и применяемый, как правило, для построения LAN Ethernet звездообразной топологии. Наибольшее распространение получили неэкранированные кабели категории 5, содержащие 4 скрученные с различными шагами пары проводов. По этим кабелям можно передавать данные со скоростью от 10 Мбит/с до 1,8 Гбит/с. Длина каждой цепи, проходящей от центрального коммутатора до конечной станции и включающей в себя промежуточные концентраторы, может составлять до 185 м.

Основные характеристики ВОЛС были приведены ранее, в разделе 1.2.1 настоящего пособия.

2.2.2. Физический уровень

Конфигурации LAN Ethernet приведены на рис. 23.

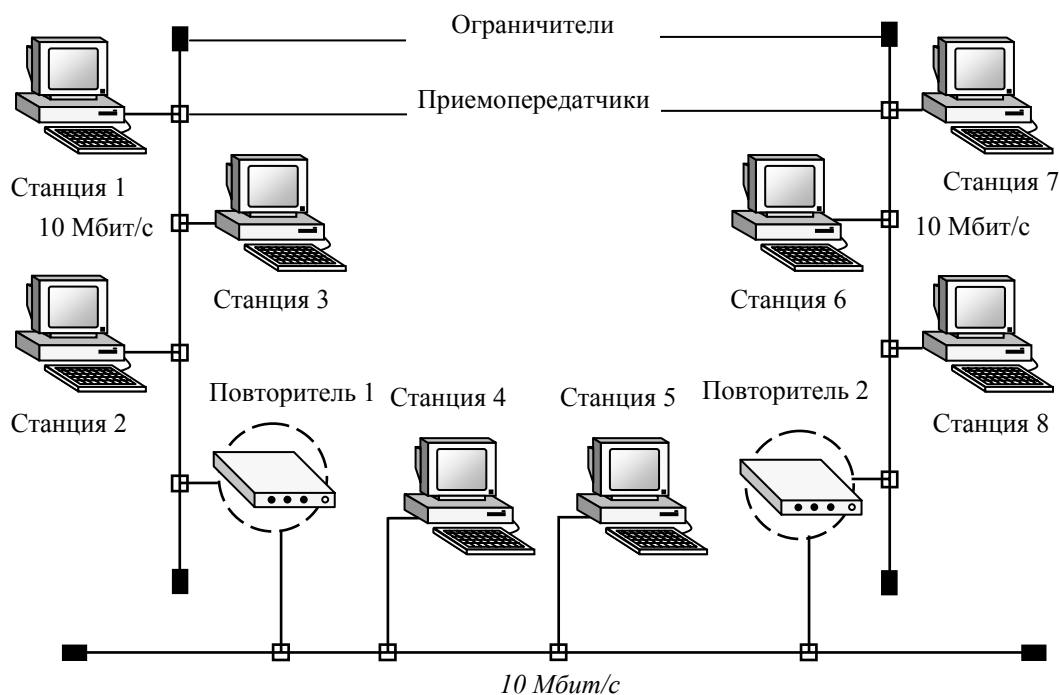
Для построения шинной топологии применяются коаксиальный кабель и устройства: повторители и приемопередатчики.

Повторитель LAN Ethernet опознает несущую (физический сигнал передачи данных) и конфликты в одном участке кабеля и регенерирует соответствующее состояние сети и поток данных на другом участке. При этом в LAN Ethernet может включаться через повторители один кабель с двухточечным соединением (без подключения станций) длиной не более 1000 м. Одна LAN может содержать до 1024 единиц компьютерной техники (компьютеров и устройств ввода-вывода).

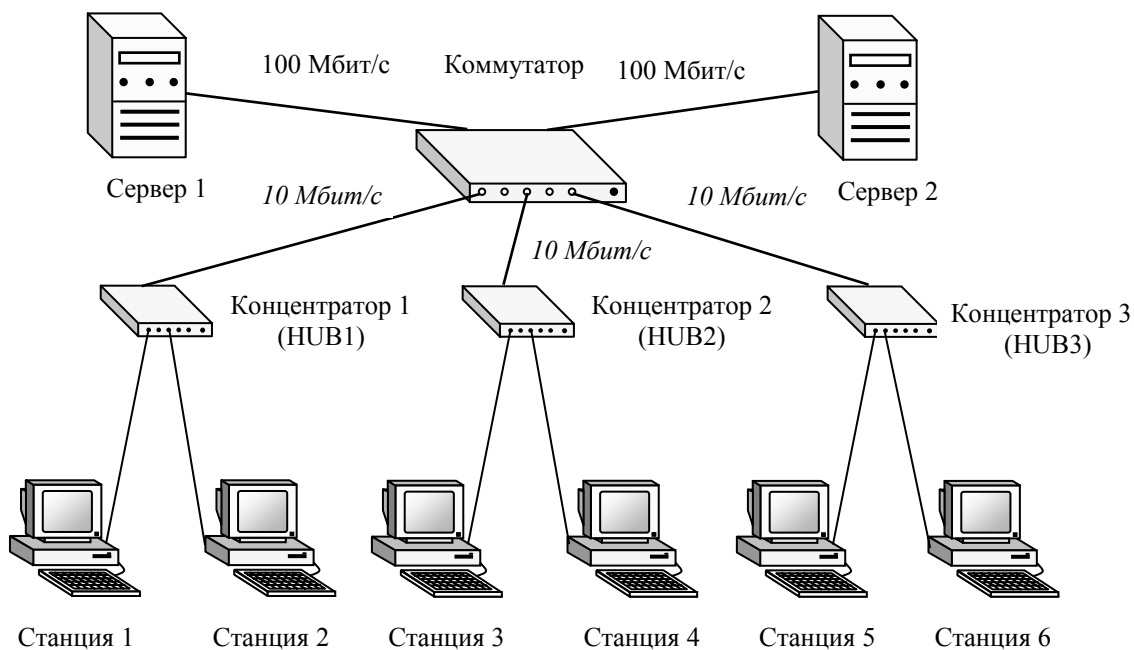
Приемопередатчик (подуровень РМА модели IEEE 802) предназначен для согласования параметров сигнала с характеристиками коаксиального кабеля, для гальванической развязки интерфейсного кабеля с кабелем шины и обнаружения конфликтов. С сетевым контроллером (электронной платой, устанавливаемой в корпусе станции) приемопередатчик соединяется интерфейсным кабелем (подуровень АUI) длиной до 50 м. Кабель состоит из 4 витых пар: передача данных, прием данных, обнаружение конфликтов и питание.

Приведенная схема подключения станций имеет место в том случае, когда в качестве передающей среды применяется так называемый толстый коаксиальный кабель. Если для передачи данных применяется

«тонкий» кабель (RG 58/U), то приемопередатчик размещается непосредственно в сетевом контроллере и для подключения станции к кабелю применяется тройниковый разъем (BNC).



Шинная топология LAN



Звездообразная топология LAN

Рис. 23. Виды конфигураций локальной сети Ethernet

Подуровень передачи физических сигналов PS модели IEEE 802 в LAN Ethernet реализуется электронными схемами сетевого контроллера, которые осуществляют преобразование данных из двоичного кода в манчестерский и обратно, а также создание и удаление *преамбул (специальная кодовая последовательность бит, обеспечивающая предварительную синхронизацию процесса приема-передачи кадра данных)*.

LAN Ethernet звездообразной топологии строятся в основном с использованием витой пары, ВОЛС и устройств: концентраторов и коммутаторов. Отдельные сетевые фрагменты могут быть выполнены на основе коаксиального кабеля.

Концентратор (HUB) представляет собой интеллектуальное устройство, которое осуществляет контроль ошибок, восстановление сегментации и автосегментацию, разрешение конфликтов, возникающих в случае одновременной передачи данных станциями, подключенными к концентратору. Для обеспечения их подключения концентратор содержит порты (стыки BNC для коаксиального кабеля, RJ-45 для витой пары, FL для ВОЛС). Число портов может быть равно 8, 16, 24, 48.

Коммутатор (SWITCHING) – это устройство, конструктивно выполненное в виде сетевого концентратора и действующее как высокоскоростной многопортовый мост. Он имеет встроенный механизм коммутации, который позволяет осуществить сегментирование локальной сети и разрешать конфликты путем выделения полосы пропускания конечным станциям в сети. Коммутаторы применяются как для сегментирования LAN, так и для прямого подключения станций. Тем самым создаются бесконфликтные домены на 10/100 Мбит/с.

Максимальная протяженность LAN Ethernet определяется интервалом времени, необходимым для обнаружения конфликта между двумя одновременно передающими станциями. В наиболее неблагоприятной ситуации станция на одном конце сети начнет передачу как раз в момент приема кадра от станции, находящейся на другом ее конце. Время, затрачиваемое на прохождение кадра через сеть и затем на передачу сигнала конфликта обратно на передающую станцию, составляет так называемую круговую задержку сети. В наихудшем случае круговая задержка равна 45 мкс, что соответствует 450 бит информации при скорости передачи 10 Мбит/с.

Для обеспечения нормального функционирования LAN с доступом в режиме соперничества все станции должны одинаково опознавать состояние конфликта. С этой целью в LAN Ethernet определена минимальная длина кадра данных, при которой любая передающая станция в са-

мых неблагоприятных условиях получит сигнал конфликта до окончания передачи кадра. Такой минимальный по длине кадр составляет 72 байта, или 576 бит.

Это ограничение относится ко всем LAN с доступом в режиме соперничества независимо от конкретной реализации. Его можно ослабить путем уменьшения либо скорости передачи, либо протяженности сети. Например, снижение скорости передачи вдвое сократит минимальную длину кадра в два раза.

2.2.3. Канальный уровень

В соответствии с моделью IEEE 802 канальный уровень LAN делится на два подуровня: управление логическим каналом LLC и управление доступом к среде MAC.

Подуровень LLC является универсальным для всех типов LAN, в том числе для сети Ethernet. Он выполняет функции интерфейса с верхними уровнями модели IEEE 802 и устанавливает логический канал связи между процессом (программой) на данной станции и процессом (программой) на удаленной станции. Структура блока (пакета) данных подуровня LLC приведена в разделе 2.1.3.

Подуровень MAC осуществляет формирование кадров данных, распознавание кадров, предназначенных для конкретной станции, обнаружение ошибок, управление доступом к среде. Структура кадра данных подуровня MAC приведена на рис. 24.

Преамбула	Начальный разделитель	Адрес назначения	Адрес отправления	Блок (пакет) данных LLC	Вставка	Контрольная последовательность	Конечный разделитель
1	2	3	4	5	6	7	8

Рис. 24. Структура кадра данных подуровня MAC

Преамбула. Специальная кодовая последовательность бит (11111110), обеспечивающая предварительную синхронизацию процесса приема-передачи данных.

Начальный разделитель. Специальная кодовая последовательность бит (01111110), предназначенная для выделения начала кадра в общем потоке данных.

Адрес назначения. Адрес станции-получателя передаваемого кадра.

Адрес отправления. Адрес станции-отправителя кадра данных.

Блок (пакет) данных LLC. Блок данных, поступающий с верхнего подуровня LLC (для LLC верхним уровнем является сетевой, формирующий пакеты данных).

Вставка. Дополнительная (как правило, малозначительная) информация, вставляемая в кадр в том случае, если его длина меньше необходимой для обнаружения столкновений.

Контрольная последовательность. Проверочная кодовая последовательность бит, формируемая путем специальных математических преобразований разделов 3, 4, 5, 6 и используемая для проверки правильности принятых кадров.

Конечный разделитель. Специальная кодовая последовательность бит (01111110), предназначенная для выделения конца кадра в общем потоке данных.

2.2.4. Передача данных в локальной сети Ethernet

Передача данных в сети Ethernet выполняется с помощью протоколов верхних уровней и подуровня LLC, которые не зависят от типа LAN и представляют собой универсальное сетевое программное обеспечение (например, сетевой пакет программ NetWare фирмы NOVELL), и протоколов подуровня MAC и физического уровня, реализованных аппаратно в виде сетевого контроллера (электронной платы), вставляемого в корпус станции. Интерфейс между универсальным сетевым программным обеспечением и сетевым контроллером конкретной LAN обеспечивается программой-драйвером.

Ранее уже указывалась целесообразность изложения материала о работе протоколов верхних уровней модели IEEE 802 в разделах по WAN и GAN, поэтому в настоящем разделе приведено описание работы протоколов только канального и физического уровней сети Ethernet.

Подключение и работа в сети Ethernet выполняются с помощью сетевого контроллера, функциональная структура которого приведена на рис. 25.

Функциональные блоки контроллера имеют следующее назначение.

Блокирование данных. Формирует кадр данных, структура которого приведена на рис. 24.

Деблокирование данных. Производит обработку принятого кадра, выделяет блок данных LLC и передает его верхнему уровню (подуровню LLC).

Управление доступом к среде. Передает кадр в физический уровень и принимает кадр из физического уровня, обеспечивает обработку и устранение столкновений.

Кодирование данных. Формирует преамбулу и кодирует двоичные данные в самосинхронизирующийся манчестерский код.

Декодирование данных. Распознавание и удаление преамбулы, преобразование данных из манчестерского кода в двоичный код.

Доступ к среде. Вводит физический сигнал в канал связи на передающей стороне и получает сигнал на принимающей стороне, контролирует наличие несущей (сигнала передачи данных) в канале связи как на передающей, так и на принимающей стороне (это означает, что канал связи занят), обнаруживает столкновения в канале связи на передающей стороне (сообщает, что произошло наложение сигналов).

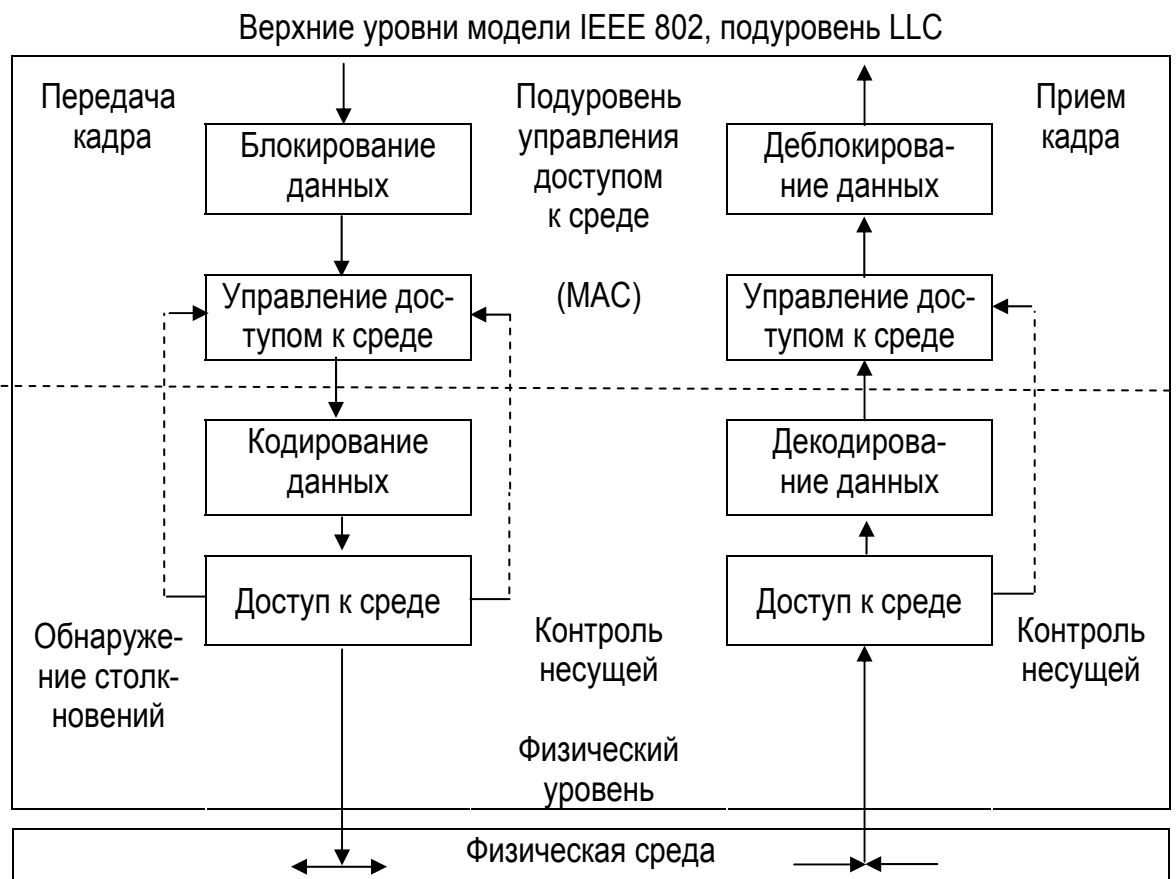


Рис. 25. Функциональная структура контроллера локальной сети Ethernet

Процесс передачи данных в LAN Ethernet происходит следующим образом.

Блок данных LLC поступает на вход блока, который формирует кадр MAC. Он добавляет к блоку LLC начальный и конечный разделители, адреса передающей и принимающей станций, формирует контрольную последовательность. После этого кадр MAC передается блоку управления доступом к среде, который помещает кадр в буфер и хранит его до тех пор, пока не освободится канал связи. Канал считается свободным, когда произведен сброс сигнала контроля несущей по сигналу блока доступа к среде. После небольшой задержки (9,6 мкс), необходи-

мой для полного освобождения канала, кадр передается физическому уровню.

На физическом уровне блок кодирования данных формирует преамбулу и выполняет преобразование двоичных данных в манчестерский код. Затем физические сигналы через блок доступа к среде (приемопередатчик) поступают в канал связи.

Кадр MAC передается всем станциям, подключенным к каналу связи. Принимающая станция через блок доступа к среде контролирует преамбулу, синхронизируется с сигналом передачи данных и устанавливает сигнал контроля несущей. Затем принятый сигнал поступает на блок декодирования, который удаляет преамбулу, преобразует манчестерский код в двоичную последовательность бит и передает кадр блоку управления доступом к среде.

Блок управления доступом к среде хранит принятый кадр в буфере до тех пор, пока не будет произведен сброс сигнала контроля несущей. Сброс этого сигнала означает, что приняты все биты. Из буфера кадр поступает на деблокирование. При деблокировании кадра производится контроль ошибок, которые могли возникнуть в процессе передачи (формируется контрольная последовательность для принятого кадра и сравнивается с принятой). Если ошибок не обнаружено, производится проверка адресов, чтобы определить правильность адресации кадра данной станции. Если адрес правильный, то выделяется блок (пакет) данных LLC и передается верхнему уровню. В противном случае кадр отбрасывается.

Особое место при передаче данных в локальной сети Ethernet занимает явление столкновений (коллизий). Оно может происходить тогда, когда несколько станций одновременно попытаются захватить канал и начать передачу данных. В этом случае возникает наложение и искажение сигналов, в результате чего их правильный прием станциями невозможен.

Коллизии характеризуются двумя параметрами: круговой задержкой и окном коллизий. Под круговой задержкой понимается время, затрачиваемое на прохождение кадра через сеть и на передачу сигнала конфликта обратно на передающую станцию. Для LAN Ethernet круговая задержка равна 45 мкс, что соответствует времени передачи 450 бит при скорости передачи 10 Мбит/с. Окно коллизий представляет собой интервал времени, необходимый для распространения сигнала конфликта по каналу и обнаружения его всеми станциями.

Для обработки коллизии блок управления доступом к среде выполняет две функции. Во-первых, усиливает эффект коллизии путем передачи специальной последовательности битов, называемой затормозкой. Цель

затора состоит в том, чтобы сделать коллизию настолько продолжительной, чтобы ее смогли заметить все другие передающие станции, которые вовлечены в конфликт. В различных реализациях LAN Ethernet затор состоит по меньшей мере из 32 бит, но не более 48 бит. Это гарантирует, что продолжительность коллизии будет достаточно большой, чтобы ее обнаружили все передающие станции в сети. Ограничение сверху длины затора необходимо для того, чтобы станции ошибочно не приняли его за действительный кадр. Любой кадр, содержащий менее 64 байт (октетов), считается фрагментом испорченного коллизией кадра и игнорируется любой принимающей станцией сети.

Блок управления доступом к среде передающей станции после отправки затора выполняет вторую функцию. Он генерирует случайное число, которое определяет длительность задержки до следующей попытки передачи. Время задержки всегда кратно 51,2 мкс (этот интервал, называемый тактом, несколько длиннее времени круговой задержки). В результате любая станция, выбросившая наименьшее случайное число, получает возможность осуществить свою передачу без конфликтов. Станции, случайные числа которых оказались хотя бы на единицу больше, обнаружат несущую менее чем через 51,2 мкс и задержат передачу. Если наименьшее случайное число выбросили две или более станции, то процедура повторяется с увеличенным диапазоном возможных чисел.

В течение первых 10 попыток диапазон генерируемых случайных чисел экспоненциально возрастает от $0 \dots 1$ до $0 \dots 1023$ (т. е. максимальная задержка равна 65 мс), а для 5 последующих попыток остается на том же уровне. Если 16 попытка заканчивается неудачей, канальный уровень отказывается от передачи кадра и оповещает об этом верхний уровень. Возникновение такой катастрофической ситуации маловероятно при нормальном функционировании сети и обычно является признаком разрыва в канале связи или каких-либо нарушений его электрических характеристик.

В принимающей станции или станциях биты, образованные в результате коллизии, декодируются физическим уровнем. Принятые фрагменты кадров, вовлеченных в коллизию, опознаются блоком управления доступом к среде как действительные. Блок определяет, что коллизионный фрагмент меньше, чем самый короткий действительный кадр (64 байта), и игнорирует принятый фрагмент. Таким образом, затор используется с той целью, чтобы гарантировать, что все передающие станции заметят коллизию, а передача фрагментарного кадра гарантирует, что любая принимающая станция проигнорирует эту передачу.

Работа сети Ethernet характеризуется рядом параметров, к числу которых относится вероятность захвата канала и эффективность.

Первый параметр определяется по выражению

$$P = \left(1 - \frac{1}{Q}\right)^{Q-1},$$

где P – вероятность того, что ровно одна станция попытается передать кадр в течение такта и захватит канал; Q – число станций, пытающихся захватить канал для передачи кадра данных.

Эффективность LAN Ethernet определяется следующим образом. Общее время работы сети Ethernet делится между интервалами передачи и интервалами конкуренции. Для передачи кадра данных требуется L/C секунд, где L – длина кадра в битах, C – скорость передачи данных в бит/с. Среднее время T , необходимое на захват канала, равно

$$T = W \cdot B,$$

где W – среднее число тактов, прошедших в интервале конкуренции, пока станция не захватит канал для передачи кадра данных; B – длительность такта, или время до обнаружения конфликта после начала передачи кадра.

Среднее число тактов W рассчитывается таким образом:

$$W = \frac{1 - P}{P}.$$

С учетом введенных показателей эффективность E работы локальной сети Ethernet определяется следующим образом:

$$E = \frac{L/C}{L/C + T}. \quad (1)$$

Как следует из выражения (1), эффективность сети Ethernet изменяется в пределах от 0 до 1. Результаты исследований показали, что с увеличением Q эффективность сети Ethernet может понизиться до 35...40 %.

2.2.5. Перспективы развития локальной сети Ethernet

Развитие сети Ethernet происходит в основном в направлении повышения скорости передачи данных с 10 до 100 Мбит/с. Примером этого может служить разработка стандарта 100Base-T, названного Fast Ethernet.

Стандарт 100Base-T оставляет неизменным подуровень MAC сети Ethernet, а также протоколы более высоких уровней, что позволяет ис-

пользовать прежнее программное обеспечение и средства управления сетями Ethernet. Для поддержки передачи данных со скоростью 100 Мбит/с произведена модификация физического уровня. Одна из этих модификаций получила обозначение 100Base-X. Буква «X» означает возможность использования разных сред передачи: двух неэкранированных витых пар категории 5, двух экранированных витых пар или многомодового оптоволоконного кабеля. Поддержка традиционной технологии Ethernet обеспечила возможность построения сетей, содержащих сегменты, работающие со скоростями 10 и 100 Мбит/с одновременно.

Другим перспективным направлением является разработка стандарта IEEE 802.3z на построение LAN Gigabit Ethernet. В июне 1998 года был ратифицирован стандарт IEEE 802.3z DF для Gigabit Ethernet по оптическому кабелю. Для других сред разработки продолжаются.

Технология Gigabit Ethernet, как и Fast Ethernet, следует методу множественного доступа с контролем несущей и обнаружением коллизий (CSMA/CD). Метод расчета домена коллизий изменен в связи с увеличением скорости передачи данных. Чтобы сохранить диаметр домена коллизий Gigabit Ethernet равным 200 м, минимальный размер передаваемого кадра Gigabit Ethernet увеличен с 64 до 512 байт.

Разработанный стандарт IEEE 802.3z DF определяет две спецификации: 1000BaseLX и 1000BaseSX. В соответствии со спецификацией 1000BaseLX одномодовые оптические соединения способны обеспечивать передачу данных на расстояние до 5000 м, а в соответствии со спецификацией 1000BaseSX многомодовые оптические соединения могут поддерживать передачу на расстоянии до 550 м.

Основной областью применения Gigabit Ethernet является создание высокопроизводительных магистралей между серверами. Коммутаторы Gigabit Ethernet могут использоваться и в рабочих группах, где приложениям требуется высокая скорость передачи данных.

2.3. Локальная компьютерная сеть ARCNet

LAN ARCNet относится к классу сетей с передачей маркера. Маркером называется специфическая комбинация битов, передаваемая от станции к станции в определенной последовательности. Станция может осуществлять передачу данных только после поступления к ней маркера и должна передавать его дальше в течение короткого интервала времени. Сеть ARCNet была создана в 1982 году фирмой Datapoint. Она функционировала по принципу передачи маркера в физической звезде. Позднее маркерный метод доступа был распространен на сети шинной и кольцевой топологий.

2.3.1. Физическая среда передачи данных

В качестве передающей среды в LAN ARCNet используется коаксиальный кабель и витая пара.

2.3.2. Физический уровень

LAN ARCNet может иметь звездообразную и шинную топологию. Максимальная протяженность сети составляет 6,5 км. Скорость передачи данных в LAN ARCNet равна 2,5 Мбит/с.

2.3.3. Канальный уровень

Построение LAN ARCNet шинной топологии выполняется с учетом спецификаций стандарта IEEE 802.4. В соответствии с этим стандартом подуровень LLC для LAN ARCNet остается без изменений. Для подуровня MAC определена следующая структура кадра данных (рис. 26).

Начальный разделитель	Управление кадром	Адрес назначения	Адрес отправления	Блок (пакет) данных LLC	Контрольная последовательность	Конечный разделитель
1	2	3	4	5	6	7

Рис. 26. Структура кадра данных подуровня MAC стандарта IEEE 802.4

Структура этого кадра в основном совпадает со структурой кадра данных подуровня MAC стандарта IEEE 802.3 (LAN Ethernet). Исключение составляет второй раздел «Управление кадром», который отсутствует в LAN Ethernet. Для сетей с маркерным методом доступа этот раздел играет ключевую роль, так как именно он определяет тип передаваемого кадра.

Рассмотрим основные типы кадров подуровня MAC стандарта IEEE 802.4.

Маркер. При получении маркера станция может передавать кадры данных в течение интервала времени, не превышающего предельного для сети значения. Маркер имеет следующую структуру (рис. 27).

Начальный разделитель	00000000	Адрес назначения	Адрес отправления	Контрольная последовательность	Конечный разделитель
1	2	3	4	5	6

Рис. 27. Структура кадра «маркер»

Данные. Кадры данных посылаются в порядке приоритетности. Существует четыре вида передач: синхронная, срочная асинхронная, обычная асинхронная и передача без ограничений по времени. Такая система передачи позволяет одновременно передавать по одной шине трафик различных видов обслуживания (начиная с синхронного и заканчивая без ограничений по времени). Структура кадра данных приведена на рис. 28. Во втором столбце rrr обозначают биты приоритета.

Начальный разделитель	11000rrr	Адрес назначения	Адрес отправления	Блок (пакет) данных LLC	Контрольная последовательность	Конечный разделитель
1	2	3	4	5	6	7

Рис. 28. Структура кадра «данные»

Установка следующей станции. Маркер передается по логическому кольцу в порядке очередности, определяемой адресами станций в направлении их убывания (возрастания). Достигнув станции с наименьшим адресом, он вновь поступает на станцию с наибольшим адресом. Станция может передавать данные только при наличии маркера и после завершения передачи отсылает маркер следующей станции. Располагающая маркером станция может отключиться от кольца, пошлав в предшествующую станцию команду на соединение с последующей станцией, начиная с очередного цикла. Это осуществляется с помощью кадра «установка следующей станции» (рис. 29).

Начальный разделитель	00001000	Адрес назначения	Адрес отправления	Новый адрес следующей станции	Контрольная последовательность	Конечный разделитель
1	2	3	4	5	6	7

Рис. 29. Структура кадра «установка следующей станции»

Поиск следующей станции. Использование логического кольца обуславливает необходимость реализации некоторых управляющих функций, а именно:

- перестройки кольца;
- изменения параметров управляющих алгоритмов (например, максимального интервала времени, в течение которого станция может удерживать маркер);
- приема запросов на подключение к кольцу от неактивных станций.

Выполнение этих функций возлагается на одну или несколько станций, каждая из них может осуществлять управление при поступлении маркера.

Первые две из указанных функций реализуются посылкой соответствующих командных кадров, причем перестройка кольца осуществляется с помощью кадра (команды) «установка следующей станции». Реализация третьей функции связана с серьезной проблемой: станция не может начать передачу, не получив маркера, но станция, отключенная от кольца, не получит его никогда.

Для выхода из создавшегося тупика при подключении к кольцу новых станций применяют процедуру «управляемое соперничество». Расширенный вариант этой же процедуры выполняется при инициализации сети после отказов. Каждая станция кольца запускает процедуру «управляемое соперничество» через N поступлений маркера (число N устанавливается при инициализации сети). В начале процедуры управляющая станция передает кадр «поиск следующей станции» (рис. 30) с одним или двумя пустыми окнами для записи требований на подключение (np – число окон; два окна нужны в том случае, когда управляющая станция имеет наименьший адрес). Размер окна равен двум максимальным задержкам распространения сигнала по шине. Станции, желающие подключиться к кольцу, передают в соответствующем окне кадры «установка следующей станции».

Начальный разделитель	000000 np	Адрес назначения	Адрес отправления	Контрольная последовательность	Конечный разделитель	Окно 1	Окно 2
1	2	3	4	5	6	7	8

Рис. 30. Структура кадра «поиск следующей станции»

Разрешение спора. Если управляющая станция примет один ответ, то ответившая станция будет подключена к кольцу. Если не будет получено ни одного ответа, цикл управления завершается. При регистрации конфликта посылается кадр «разрешение спора» (рис. 31), сопровождаемый четырьмя окнами для записи требований на подключение к кольцу. Каждая станция, запрашивающая подключение, выбирает одно окно в соответствии с первыми двумя битами собственного адреса и передает кадр «установка следующей станции». При обнаружении в окне конфликта требование аннулируется.

Начальный разделитель	00000100	Адрес назначения	Адрес отправления	Контрольная последовательность	Конечный разделитель	Окно 1	Окно 2	Окно 3	Окно 4
1	2	3	4	5	6	7	8	9	10

Рис. 31. Структура кадра «разрешение спора»

В случае конфликта повторно передается кадр «разрешение спора», однако при этом ответы формируются в соответствии с третьим и четвертым разрядами адресов. Процедура выполняется до тех пор, пока либо управляющая станция не получит верный кадр «установка следующей станции», либо не завершится обработка всех требований, либо не будет превышено максимальное число повторений.

2.3.4. Передача данных в локальной сети ARCNet

Каждый узел в сети ARCNet идентифицируется собственным адресом (MID). В сети типа шины с передачей маркера каждому узлу известен идентификатор следующего узла в логическом кольце (NID). Обычно следующая станция имеет больший адрес. На рис. 32 приведена схема логического кольца сети ARCNet.

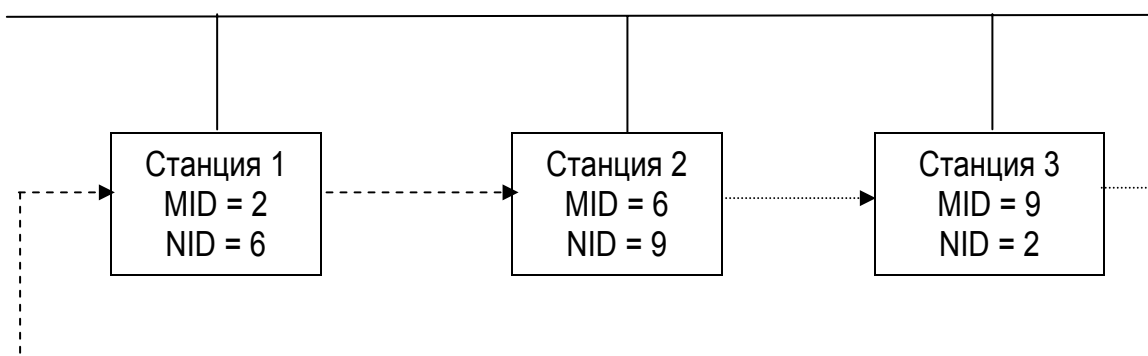


Рис. 32. Схема логического кольца LAN ARCNet

Во время нормальной работы, когда не выполняется ни восстановление маркера, ни реконфигурация кольца, каждая станция (кроме передающей) находится в состоянии прослушивания канала. Если заголовок входящего кадра содержит адрес данной станции, то она переходит в состояние приема и обрабатывает принятый кадр. Если принятый кадр содержит блок (пакет) данных LLC, то он передается верхнему уровню, а станция возвращается в состояние прослушивания канала. Если принятый кадр является маркером, то это означает, что станция получает право передачи кадра. В этом случае, если имеется пакет данных, поступивший с верхнего уровня, осуществляется его передача.

После завершения передачи пакета выполняется передача маркера. При отсутствии пакета передается маркер и станция переходит в состояние прослушивания канала.

Кроме передачи маркера, в LAN ARCNet должны решаться проблемы потери маркера и реконфигурации кольца.

Потеря маркера обнаруживается по продолжительному молчанию шины. Установив, что маркер потерян, станции начнут соперничать, как в рассмотренной выше ситуации при управлении маркером. Процесс восстановления маркера начинается со станции с бóльшим (меньшим) адресом среди функционирующих.

Реконфигурация логического кольца выполняется ранее изложенным методом с использованием процедуры «управляемое соперничество».

2.3.5. Перспективы развития локальной сети ARCNet

Сети шинной топологии с маркерным методом доступа нашли широкое применение для построения систем управления производственными процессами. В такой системе, в отличие от систем, построенных на базе сети Ethernet, каждой промышленной установке гарантирован доступ к каналу передачи данных в требуемые интервалы времени, необходимые для организации непрерывного технологического процесса.

Развитие LAN ARCNet происходит в направлении замены коаксиального кабеля на витую пару и ВОЛС, повышения скорости передачи данных и протяженности сети, создания более производительных концентраторов и коммутаторов.

2.4. Локальная компьютерная сеть Token Ring

LAN Token Ring представляет собой однонаправленное физическое кольцо с передачей маркера. Она была разработана фирмой IBM в 1986 году. В ее основе лежит стандарт IEEE 802.5.

2.4.1. Физическая среда передачи данных

В качестве среды передачи данных в сети Token Ring применяются коаксиальный кабель, витая пара и ВОЛС. Скорость передачи данных равна 4 Мбит/с, для широкополосной реализации – 16 Мбит/с.

2.4.2. Физический уровень

В физическом кольце сигналы усиливаются сетевыми контроллерами станций, и, следовательно, максимальная длина физического кольца практически не ограничивается вследствие ослабления сигнала в среде передачи данных. В LAN Token Ring максимальное расстояние

между соседними станциями составляет 2 км. Однако следует учитывать, что повреждение отдельного узла или кабельного сегмента физического кольца приводит к разрушению пути следования сигналов, и вся сеть выходит из строя. В связи с этим LAN Token Ring может иметь смешанную звездно-кольцевую топологию. Это решение требует использования концентраторов, которые автоматически переключаются для обхода поврежденных узлов.

2.4.3. Канальный уровень

Подуровень MAC стандарта IEEE 802.5 предусматривает использование трех типов кадров.

Маркер. Структура маркера (рис. 33) состоит из трех типов байтов: начальный разделитель, поле управления доступом и конечный разделитель. Назначение двух разделителей – указание начала и конца маркера. Поле управления доступом содержит восемь битов. Три бита *PPP* используются для индикатора приоритета, три бита *RRR* – для индикатора резервирования приоритета, бит *T* – бит маркера, бит *M* – мониторный бит. Когда бит маркера установлен в 0, это означает, что передаваемый кадр является маркером, если в 1 – передаваемый кадр является информационным. Мониторный бит предназначен для управления доступом. Он позволяет специально выделенной мониторинговой станции контролировать кольцо с целью обнаружения и исправления ошибок, а также восстановления маркера в случае его потери.

Маркер аварийного прерывания (рис. 34) состоит из начального и конечного разделителя. Он может быть послан в любой момент времени для того, чтобы отменить предыдущую передачу.

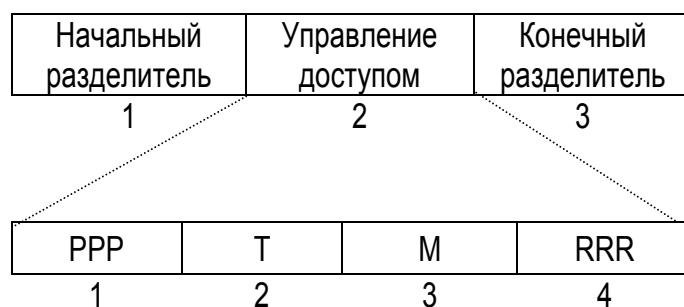


Рис. 33. Структура маркера стандарта IEEE 802.5

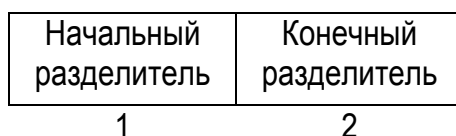


Рис. 34. Структура маркера аварийного прерывания стандарта IEEE 802.5

Информационный кадр. Структура информационного кадра приведена на рис. 35. Кроме начального разделителя, поля управления доступом и конечного разделителя стандарт IEEE 802.5 предусматривает дополнительные поля. Поле управления кадром определяет тип кадра (данные подуровня MAC или LLC) и может использоваться для установления приоритетов между двумя логическими блоками LLC. Адресные поля идентифицируют передающую и принимающую станции. Информационное поле содержит блок (пакет) данных LLC или данные подуровня MAC. Поле контрольной последовательности используется для контроля ошибок в принятом кадре. Поле состояния кадра включает в себя два бита: бит приема и бит соответствия. В исходном состоянии эти биты равны 0. В бит приема записывается 1, если принимающая станция опознала свой адрес и скопировала информационный кадр. Бит соответствия принимает значение, равное 1, если в принятых данных содержатся ошибки.

Начальный разделитель	Управление доступом	Управление кадром	Адрес назначения	Адрес отправления	Блок (пакет) данных LLC	Контрольная последовательность	Конечный разделитель	Состояние кадра
1	2	3	4	5	6	7	8	9

Рис. 35. Структура информационного кадра стандарта IEEE 802.5

2.4.4. Передача данных в локальной сети Token Ring

В маркерном кольце (приоритетном) для обеспечения доступа к сети на основе приоритетов используется маркер. Этот подход в настоящее время широко используется фирмами-изготовителями сетевого оборудования, которое базируется на стандарте IEEE 802.5. У него много общего с обычной LAN с передачей маркера. Например, маркер передается по кольцу и содержит индикатор, указывающий, занято или свободно кольцо. Маркер циркулирует непрерывно по кольцу, проходя через каждую станцию. Если станция желает передать данные и маркер свободен, она захватывает кольцо, превращая маркер в индикатор начала информационного кадра, добавляя данные и управляющие поля и посылая кадр по кольцу к следующей станции.

Каждая станция в кольце анализирует принятый маркер. Если оказывается, что маркер занят, принимающая станция должна регенерировать его и передать следующей станции. Копирование данных требуется только в том случае, если данные должны быть переданы прикладной

системе конечного пользователя, связанной с этой конкретной станцией. После того как кадр возвращается на исходную станцию, которая произвела его передачу, маркер снова восстанавливается в исходном виде (инициализируется) и передается в кольцо.

В LAN стандарта IEEE 802.5 каждой станции может быть установлен приоритет и доступ к кольцу для передачи данных будет происходить в соответствии с установленным приоритетом. Это достигается путем размещения в маркере индикаторов приоритета.

Рассмотрим принцип функционирования LAN Token Ring на примере схемы, представленной на рис. 36.

На этой схеме к маркерному кольцу подсоединены пять станций. Каждая станция имеет приоритет, равный P . Через R и T обозначены приемный и передающий регистры сетевых контроллеров. Как следует из схемы, станция A обладает самым низким приоритетом, равным 1, станции B и D имеют приоритет 2, станции C и E – приоритет 3.

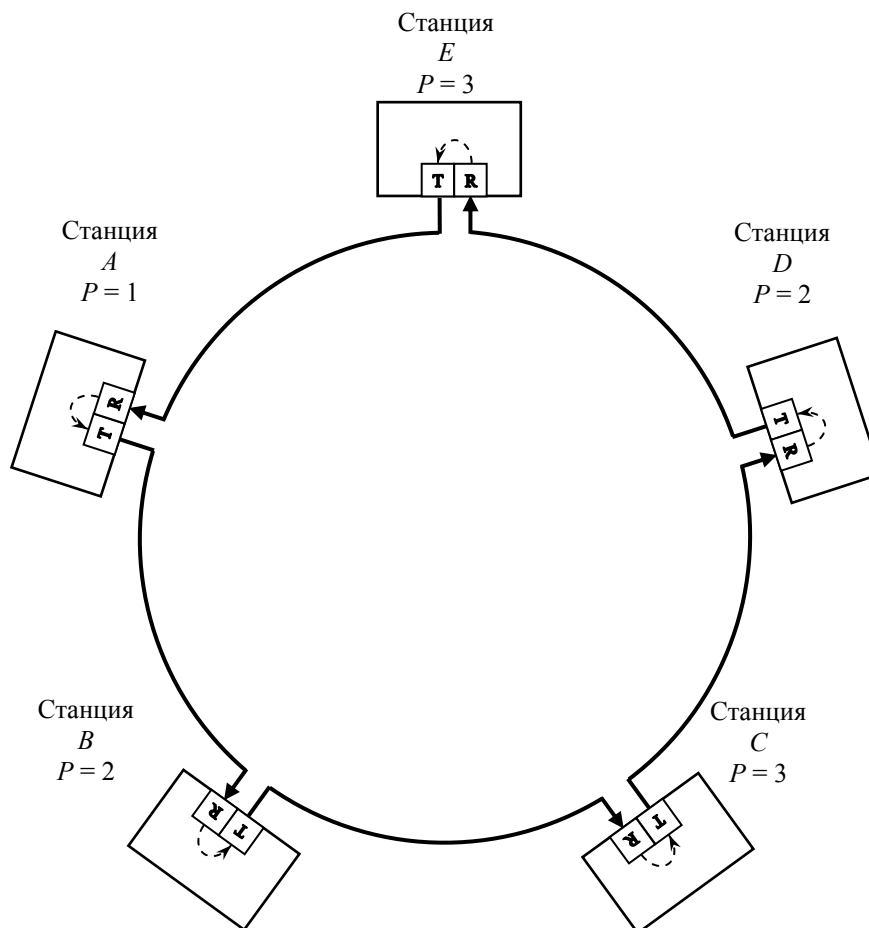


Рис. 36. Схема кольцевой LAN Token Ring

Предположим, что станция A уже захватила кольцо и передает кадры данных. В маркере имеется бит T , который установлен в 1 для инди-

кации того, что маркер занят. Следующая последовательность событий иллюстрирует один из подходов к приоритетной передаче маркера.

- Станция *B* получает кадр. У нее есть данные для передачи, поэтому она записывает свой приоритет, равный 2, в поле резервирования в маркере (поле *RRR*). Далее она передает маркер станции *C*.

- Станция *C* также определяет, что кольцо занято. У нее есть данные для передачи. Она помещает $P = 3$ в поле резервирования *RRR* вместо $P = 2$, записанного станцией *B*. Затем станция *C* передает кадр станции *D*.

- Станция *D* должна уступить, так как она не может поместить свой приоритет $P = 2$ в поле резервирования *RRR*, потому что там находится $P = 3$. Следовательно, она передает кадр станции *E*, которая анализирует поле резервирования *RRR*. Убедившись, что в этом поле записано $P = 3$, она ничего не предпринимает, поскольку ее приоритет $P = 3$.

- Станция *A* получает кадр. Она проверяет биты приема и соответствия. Если бит приема равен 1, значит станция, которой был адресован информационный кадр, выполнила его копирование. Если бит соответствия равен 0, значит передача прошла без ошибок. Тогда станция освобождает кольцо, восстанавливая маркер путем присвоения $T = 0, P = 0$, и передает его станции *B*. В противном случае выполняется повторная передача.

- Станции *B* не разрешено использовать маркер, потому что поле резервирования приоритета *RRR* в маркере имеет значение $P = 3$, что на единицу больше приоритета станции *B*.

- Станции *C* разрешается захватить маркер, так как ее приоритет $P = 3$ не меньше поля резервирования приоритета *RRR* в маркере. Она записывает свой приоритет в поле приоритетов *PPP* и освобождает поле резервирования *RRR*, записывая в него 0. Затем она формирует информационный кадр и посылает его станции *D*.

- Станция *D* записывает свой приоритет $P = 2$ в поле резервирования *RRR* и передает кадр станции *E*.

- Станция *C* замещает приоритет станции *E* своим приоритетом $P = 3$ и передает кадр станции *A*.

- Станция *A*, поскольку ее приоритет $P = 1$, не меняет значение поля резервирования *RRR*.

- Станция *B* также не меняет значение поля резервирования *RRR*, так как ее приоритет $P = 2$.

- Станция *C* получает обратно свой информационный кадр и должна освободить кольцо. Она делает это и передает маркер станции *D*.

- Станции *D* не разрешается захватить кольцо, поскольку ее приоритет $P = 2$ меньше значения поля резервирования в маркере, равного $P = 3$. Она передает маркер станции *E*.

- Станция *E* захватывает кольцо, поскольку ее приоритет $P = 3$ не меньше значения поля резервирования *RRR* маркера.

Как следует из приведенной схемы функционирования LAN Token Ring, маркер передается по кольцу от станции к станции. Если станция получает адресованный ей кадр, она копирует его и передает следующей станции. Когда занятый маркер обращается по кольцу, станции претендуют на его использование во время следующей передачи по кольцу. В данной конкретной ситуации, если у всех станций есть данные для передачи, маркером фактически обмениваются две станции – *C* и *E*, так как они имеют наивысший приоритет. В большинстве случаев станции, имеющие наибольший приоритет, не будут вести передачу данных при каждом обороте маркера. Следовательно, кольцевая конфигурация с приоритетами дает возможность станциям с низким приоритетом захватить кольцо в случае неактивности станций с более высоким приоритетом.

2.4.5. Перспективы развития локальной сети Token Ring

Эта сеть, по сравнению с LAN Ethernet, имеет существенное преимущество, которое проявляется в том, что она позволяет создавать кольцевые конфигурации протяженностью 50 и более км. Она имеет низкую скорость передачи данных (4 Мбит/с) и не обладает высокой надежностью вследствие кольцевой топологии. С целью ликвидации этих недостатков была разработана двунаправленная высоконадежная кольцевая сеть FDDI, имеющая скорость передачи данных 100 Мбит/с и предназначенная для построения региональных (WAN) сетей.

Методические указания

В этом разделе пособия рассматривались вопросы построения локальных компьютерных сетей (LAN). При изучении этого раздела необходимо усвоить следующее:

- LAN представляет собой коммуникационную систему, расположенную в пределах отдельного здания или сооружения и содержащую компьютеры, соединенные между собой высокоскоростными цифровыми каналами связи;
- модель LAN определяется спецификациями стандарта IEEE 802;

- в модели IEEE 802, в отличие от модели ISO/OSI, канальный уровень делится на два подуровня: управление логическим каналом LLC и управление доступом к передающей среде MAC;
- в качестве передающей среды в LAN применяются коаксиальный кабель, витая пара и ВОЛС;
- для кодирования физических сигналов в LAN применяется манчестерское и дифференциальное манчестерское кодирование;
- в качестве базовых конфигураций LAN применяются шина, звезда и кольцо;
- тип конфигурации LAN и метод доступа к среде передачи данных определяются спецификациями подуровня MAC: для LAN шинной (звездообразной) топологии с множественным доступом, контролем несущей и обнаружением столкновений (CSMA/CD) – спецификациями стандарта IEEE 802.3, для LAN шинной (звездообразной) топологии с передачей маркера – спецификациями стандарта IEEE 802.4, для кольцевой LAN с передачей маркера – спецификациями стандарта IEEE 802.5;
- блок данных подуровня LLC является универсальным для всех типов LAN;
- верхние уровни модели IEEE 802 соответствуют модели ISO/OSI;
- широко известная LAN Ethernet построена на основе спецификаций стандарта IEEE 802.3;
- LAN Ethernet имеет максимальную протяженность 2,5 км и скорость передачи данных 10 Мбит/с;
- эффективность работы LAN Ethernet зависит от количества станций, пытающихся одновременно захватить канал для передачи данных, и изменяется в пределах от 0 до 1;
- развитие LAN Ethernet происходит в направлении повышения скорости передачи данных с 10 до 100 Мбит/с (LAN Fast Ethernet) и 1000 Мбит/с (LAN Gigabit Ethernet);
- LAN ARCNet построена на основе спецификаций стандарта IEEE 802.4;
- LAN ARCNet имеет максимальную протяженность 6,5 км и скорость передачи данных 2,5 Мбит/с;
- правом передавать данные в LAN ARCNet обладает станция, владеющая маркером;
- передача маркера в LAN ARCNet происходит по логическому кольцу;
- LAN ARCNet применяют в основном для построения систем управления производством;

- LAN Token Ring построена на основе спецификаций стандарта IEEE 802.5;
- LAN Token Ring может иметь протяженность несколько десятков километров (расстояние между двумя соседними станциями до 2 км) и скорость передачи данных 4 Мбит/с;
- передача маркера в LAN Token Ring выполняется в соответствии с приоритетами, которые назначаются станциям;
- дальнейшим развитием LAN Token Ring является высоконадежная двунаправленная WAN FDDI, имеющая скорость передачи данных 100 Мбит/с.

Глава 3

РЕГИОНАЛЬНЫЕ КОМПЬЮТЕРНЫЕ СЕТИ

3.1. Общие принципы построения региональных компьютерных сетей

Региональные компьютерные сети (WAN) представляют собой LAN отдельных предприятий и организаций (или мощные компьютеры), расположенные в пределах города или региона и связанные между собой высокоскоростными магистральными каналами связи. К числу недостатков рассмотренных ранее LAN можно отнести их малую протяженность (для LAN Ethernet она составляет не более 2,5 км, для Fast Ethernet и Gigabit Ethernet не более 250 метров), а также недостаточную скорость передачи данных (скорость передачи данных в LAN Token Ring равна 4/16 Мбит/с) и низкую надежность. В соответствии с этим для построения WAN необходимо было разработать новые спецификации и стандарты, позволяющие избежать перечисленных недостатков LAN.

К числу основных требований, которым должны соответствовать создаваемые WAN, следует отнести:

- высокую пропускную способность каналов связи и высокую производительность коммуникационного оборудования, обеспечивающих скорость передачи данных от 100 до 1000 Мбит/с;
- возможность одновременной передачи голоса, видео и данных по одному каналу связи;
- экономичность и доступность по цене, сопоставимой с ценами оборудования Fast Ethernet и Gigabit Ethernet;
- хорошую совместимость канального и коммуникационного оборудования различных производителей;
- поддержку инфраструктуры существующих LAN предприятий;
- масштабируемость и возможность создания виртуальных сетей.

Перечисленным требованиям в значительной степени удовлетворяют две технологии построения WAN: *FDDI-технология построения двунаправленной кольцевой сети на оптическом волокне со скоростью передачи данных 100 Мбит/с и ATM-технология коммутации ячеек (Cell) для передачи данных, речи и изображения. Следующие разделы пособия посвящены этим двум технологиям.*

3.2. Региональная компьютерная сеть FDDI

Технология FDDI использует два типа передающей среды (оптическое волокно и витую пару) и позволяет строить сети со скоростью передачи данных 100 Мбит/с. Стандарт FDDI, разработанный комитетом X3T9.5 ANSI, позволил обеспечить совместимость устройств разных производителей. Пример применения технологии FDDI для построения WAN приведен на рис. 37.

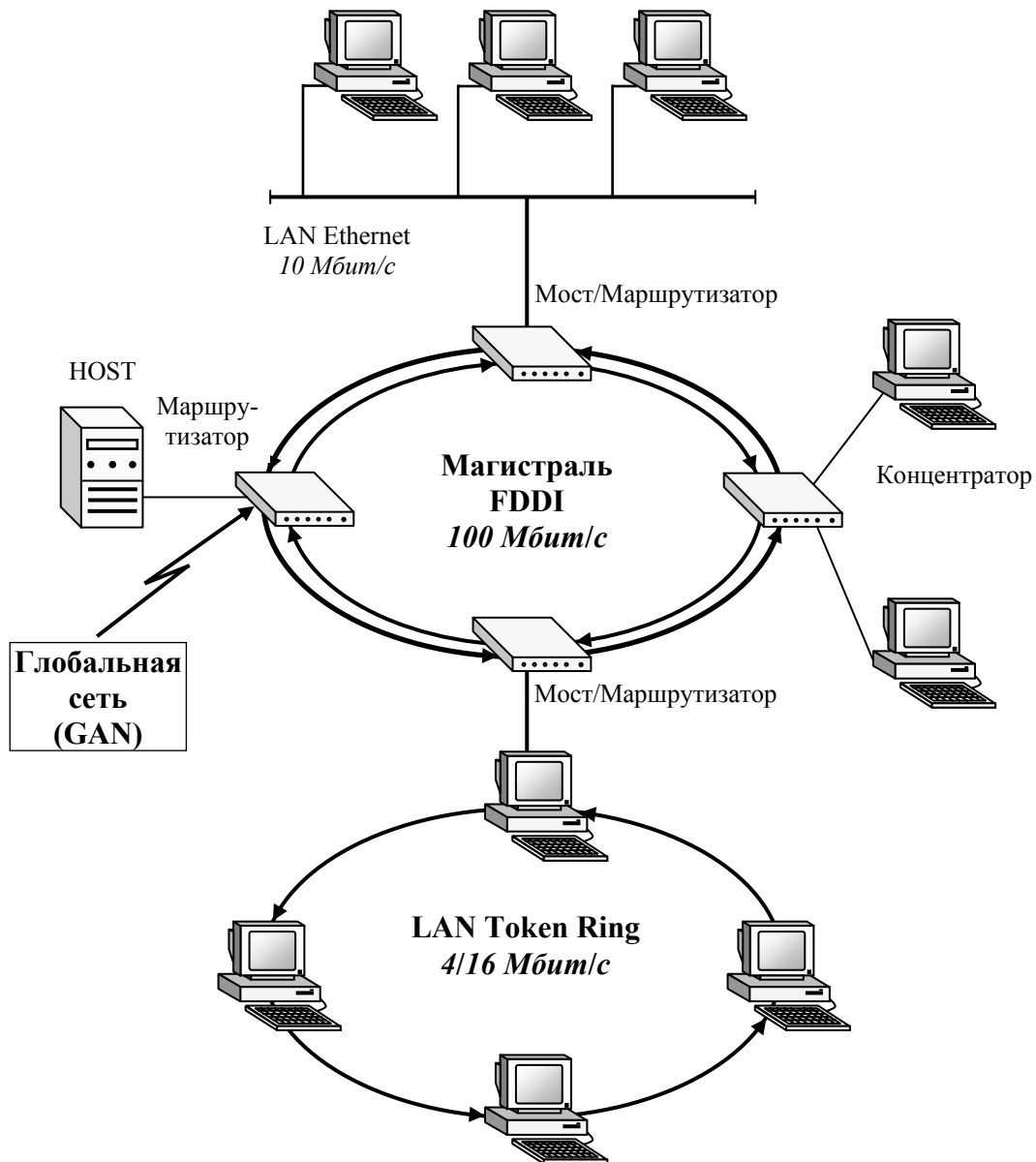


Рис. 37. Применение технологии FDDI для построения WAN

Отказоустойчивость сети FDDI обеспечивается применением двух колец передачи данных. В нормальном состоянии данные передаются только по основному кольцу. При одиночном физическом разрыве основного кольца (обрыв кабеля, выход из строя рабочей станции) станции по обе стороны места разрыва обнаруживают неисправность и автоматически переключают поток данных на резервное кольцо в направлении, противоположном направлению передачи по основному кольцу. Тем самым сохраняется непрерывность логического кольца передачи данных.

В стандарте FDDI определены также методы восстановления после серьезного нарушения целостности кольца (две станции с одним адресом и др.), требующего вмешательства администратора сети. Станция, обнаружившая нарушение, начинает передавать специальные сигнальные кадры (Beacon) до тех пор, пока не получит кадр того же типа от предыдущей станции. В итоге только одна станция остается в состоянии посылки сигнальных кадров. Это означает, что нарушение целостности кольца произошло непосредственно перед данной станцией. Знание места аварии позволяет администратору сети предпринять действия по восстановлению кольца.

3.2.1. Физическая среда передачи данных

В качестве среды передачи данных для FDDI можно использовать:

- оптоволоконный кабель с коннекторами типа MIC (Media Interface Connector), регламентируется стандартом физического уровня PMD;
- экранированную витую пару (STP IBM Type 1) с коннекторами типа DB-9, регламентируется стандартом SDDI;
- неэкранированную витую пару категории 5 (UTP Level 5) с коннекторами RJ-45, регламентируется стандартом CDDI.

Применение оптоволоконного кабеля дает сети FDDI ряд преимуществ:

- Большое расстояние между узлами. Стандарт FDDI требует, чтобы станции находились на расстоянии до 2 км друг от друга, а общая длина кольца достигала 100 км при числе станций до 500. Применение специального тонкого оптоволоконного (single-mode fiber) и лазерных передатчиков позволяет увеличить расстояние между станциями до 50 км.
- Нечувствительность к электромагнитным помехам, вызываемым электродвигателями и другими излучающими приборами.
- Большая степень безопасности. Благодаря тому, что оптоволоконный кабель практически не излучает в радиодиапазоне, передаваемую по нему информацию трудно перехватить удаленными приборами.

Это свойство имеет большое значение при построении правительственных, банковских сетей, предъявляющих повышенные требования к защите данных.

Развертывание сети FDDI на витой паре обойдется дешевле, чем оптоволоконный вариант (как по цене оборудования, так и стоимости монтажа). В случае использования медного кабеля (сеть CDDI) расстояние между станциями будет ограничено 100 метрами.

3.2.2. Физический уровень

Стандарт FDDI, определяемый комитетом X3T9.5 ANSI, имеет следующие основные компоненты, соответствующие физическому уровню:

- Physical Medium Dependent (PMD) – подуровень физического уровня, определяющий подключение к физической среде (в модели IEEE 802 подуровень PMA). Стандарт PMD регламентирует характеристики оптоволоконного кабеля для передачи данных, типы коннекторов, мощность передатчиков и т. д.

- Physical (PHY) – подуровень физического уровня (в модели IEEE 802 подуровень PS), определяющий способы кодирования и декодирования данных, схему синхронизации и набор управляющих символов. В стандарте FDDI используется схема кодирования 4/5 бит на тактовой частоте 125 МГц с инвертированием сигнала без возврата к нулю (NRZI).

Логической топологией FDDI является кольцо, физической – кольцо деревьев. *По варианту подключения к кольцу устройства FDDI делятся на подключаемые одновременно к основному и резервному кольцам (dual attachment) или только к одному кольцу, обычно основному (single attachment). По типу узла устройства FDDI делятся на концентраторы и конечные станции.*

Основные типы устройств FDDI:

- Dual Attachment Concentrator (DAC) – концентратор с двойным подключением к магистральной сети, участвует в процессе восстановления кольца при нарушении его целостности.

- Single Attachment Concentrator (SAC) – концентратор с одиночным подключением, никогда не подключается к магистральному кольцу, а всегда каскадно – к другому концентратору в сети.

- Null Attachment Concentrator (NAC) – не подключается к магистральному кольцу, а использует FDDI в качестве внутренней магистрали (backplane), часто используемая конфигурация, особенно для комбинированных концентраторов FDDI и Ethernet.

- Dual Attachment Station (DAS) – станция с двойным подключением к магистральному кольцу или концентратору, может участвовать в процессе восстановления кольца.

- Single Attachment Station (SAS) – станция с одиночным подключением только через концентратор.

В узлах с двойным подключением могут использоваться переключатели оптического обхода (Optical Bypass Switch), которые позволяют передавать данные через станцию даже в случае ее выключения.

3.2.3. Канальный уровень

Канальный уровень сети FDDI точно так же, как и в модели IEEE 802, делится на два подуровня: LLC и MAC. Функции и структура кадра подуровня LLC сети FDDI соответствуют стандарту IEEE 802.2. Основными функциями подуровня MAC являются: управление маркером (token), формирование кадров, адресация, обнаружение ошибок и восстановление кольца, а также распределение полосы пропускания между узлами. Структура маркера и информационного кадра сети FDDI соответствуют стандарту IEEE 802.5 (LAN Token Ring).

3.2.4. Передача данных в региональной сети FDDI

Высокая пропускная способность сети FDDI обеспечивается как за счет скорости передачи данных (100 Мбит/с), так и за счет того, что в сети FDDI, в отличие от LAN Ethernet, используется детерминированный метод доступа, требующий захвата маркера для передачи данных и, таким образом, исключаящий конфликты. Кроме того, по сравнению со стандартом IEEE 802.5 (LAN Token Ring), также основанном на использовании маркера, в *сети FDDI применяется более эффективный метод передачи данных, называемый ранним освобождением маркера – ETR (Early Token Release)*. В сети Token Ring данные передаются только с маркером, а в сети FDDI станция, передавшая данные в течение отведенного ей времени, освобождает маркер, не дожидаясь завершения цикла его обращения. Освободившийся маркер может захватить следующая станция и передать свои данные. Тем самым в сети FDDI в каждый момент времени может циркулировать много пакетов данных, переданных разными станциями.

Рассмотрим более подробно процесс функционирования сети FDDI. Каждая машина в сети FDDI участвует в процессе инициализации кольца. Всякий раз, когда устройство добавляется в кольцо или покидает его, когда обнаруживается потеря маркера, и в ряде других случаев начинается процесс, называемый Claim Token. В результате этого процесса стан-

ции достигают соглашения о параметрах функционирования сети и начинают передачу маркера и данных от узла к узлу по кольцу. Право формирования маркера получает станция с наименьшим временем TTRT (Target Token Rotation Time) – желаемым временем обращения маркера. Это время устанавливается производителем и может изменяться администратором сети для отдельных станций. Чем меньше время TTRT, тем быстрее маркер обращается по кольцу и тем чаще станции могут передавать данные. Но если выбрано малое значение TTRT, то станция не сможет передавать много кадров при захвате маркера.

Операция передачи данных в сети FDDI состоит из пяти шагов:

- захват маркера станцией-отправителем;
- передача данных станцией-отправителем;
- получение кадра другими станциями и возвращение его в кольцо;
- считывание кадра станцией-получателем и возвращение его в кольцо;
- удаление кадра из кольца станцией-отправителем.

В стандарте FDDI определены два режима передачи данных: синхронный и асинхронный (с приоритетами). В синхронном режиме станция при каждом захвате маркера может передавать данные в течение определенного времени вне зависимости от того, прибыл ли маркер вовремя или с опозданием. Этот режим обычно используется для приложений, чувствительных к временным задержкам (мультимедиа и др.).

После захвата маркера станция начинает передавать данные до тех пор, пока не будут переданы все данные или пока не будет превышено время захвата маркера ТНТ (Token Holding Time). В режиме синхронной передачи данных значение ТНТ фиксировано, в случае асинхронного режима зависит от того, прибыл ли маркер раньше, вовремя или с опозданием относительно минимального среди всех станций времени TTRT, определяемого в результате процесса Claim Token. Если передача завершается до истечения времени ТНТ, маркер будет немедленно возвращен в кольцо. Если ТНТ истекло до завершения передачи данных, то для передачи оставшихся данных станция должна ждать следующего захвата маркера.

Каждая станция в сети FDDI по очереди принимает кадр и сравнивает адрес назначения с собственным адресом. Если адреса не совпадают, то станция регенерирует кадр и посылает его следующему узлу. Если адреса совпадают, станция помещает кадр в приемный буфер, проверяет на наличие ошибок, делает отметку о приеме данных (или об ошибке) и возвращает кадр в кольцо. Станция-отправитель определяет, успешно ли доставлен кадр, и если да, то удаляет его из сети, если нет – регенерирует его (повторяет передачу ранее отправленного кадра).

3.3. Региональная компьютерная сеть АТМ

Модель пакетной коммутации ISO/OSI была разработана в то время, когда цифровая дистанционная передача осуществлялась с большим, в сравнении с современными системами связи, количеством ошибок. В результате схемы пакетной коммутации предполагают значительные накладные расходы для компенсации ошибок. Эти накладные расходы включают дополнительные биты в каждом из пакетов, а также дополнительную обработку на конечных станциях и в промежуточных узлах коммутации.

Подобный уровень накладных расходов не является необходимым в современных высокоскоростных системах дальней связи. Уровень ошибок довольно мал, а в конечных системах логика верхних уровней сети по отношению к уровню пакетной коммутации (например, транспортный по отношению к сетевому) может легко отследить ошибки передачи.

Основопологающий принцип технологии АТМ – предоставление пропускной способности по требованию. Она разрабатывалась с учетом преимуществ высокоскоростной передачи данных и низкого уровня ошибок современных сетевых средств. Первые сети пакетной коммутации были рассчитаны на скорость передачи к конечному пользователю в 64 Кбит/с, в то время как сети АТМ ориентировались на скорость в несколько Гбит/с. Достичь таких высоких скоростей передачи помогло исключение накладных расходов на управление потоком и контроль ошибок.

Другим существенным фактором, способствующим снижению накладных расходов в технологии АТМ, является метод управления вызовами. В модели ISO/OSI пакеты управления вызовами, используемые для установления и разрыва виртуальных каналов, передаются по тому же самому виртуальному каналу, что и пакеты данных.

В АТМ передача сигналов контроля вызова осуществляется по логическому соединению, отличному от используемого для передачи пользовательских данных. В пользовательском интерфейсе один канал управления соединением служит для управления всеми коммутируемыми соединениями передачи данных, поэтому промежуточным коммутирующим узлам нет необходимости поддерживать таблицы состояний маршрутов или обрабатывать управляющие вызовами сообщения для каждого соединения в отдельности.

Наиболее очевидно преимущество АТМ над моделью ISO/OSI в области управления потоками и контроля ошибок. Модель ISO/OSI использует трехуровневую архитектуру: сетевой, канальный и физиче-

ский уровни. На сетевом уровне происходит мультиплексирование нескольких виртуальных каналов в интерфейсе пользователя; формирование пакетов, содержащих номер виртуального канала, используемого для маршрутизации и коммутации потока данных по сети; управление потоком и контроль ошибок на всем пути следования пакетов от отправителя до получателя. На канальном уровне осуществляется контроль ошибок в коммутационных узлах сети: каждому узлу присваивается порядковый номер, после проведения контроля одновременно с передачей данных на следующий узел предыдущему передается подтверждение правильности приема. В случае приема ошибочного кадра передача повторяется.

В качестве пакета данных в сетях АТМ используется ячейка (Cell), имеющая фиксированную длину 53 байта. Каждая ячейка содержит номер логического соединения, используемого для маршрутизации и коммутации потока данных. Порядковые номера ячеек для управления потоком и контроля ошибок отсутствуют. Контроль за правильностью передачи данных от отправителя получателю должен осуществляться на более высоком уровне.

В сетях АТМ логические соединения называются виртуальными каналами (virtual channel) и устанавливаются по сети между двумя конечными пользователями для двустороннего обмена ячейками с переменной скоростью. Виртуальные каналы используются также для обмена между сетью и пользователем (контрольные сигналы) и между сетью и сетью (управление и маршрутизация в сети).

В сетях АТМ принята концепция виртуального пути. Виртуальный путь – это совокупность виртуальных каналов с одними и теми же адресами. Таким образом, все передаваемые ячейки по виртуальным каналам одного и того же виртуального пути также объединяются вместе (мультиплексируются). При этом необходимо отметить, что в сетях АТМ мультиплексирование ячеек осуществляется на втором (канальном) уровне.

Принятие концепции виртуальных путей имеет важное значение для организации эффективной передачи данных:

- Упрощается архитектура сети. Сетевые транспортные функции могут быть разделены на относящиеся к индивидуальным логическим соединениям (виртуальным каналам) и группе логических соединений (виртуальным путям).

- Увеличивается производительность и надежность сети. Сеть имеет меньшее число взаимодействующих объектов.

- Сокращается время на обработку и установление соединения. Основная часть работы производится при установке виртуального пути. Добавление новых виртуальных каналов к имеющемуся виртуальному пути требует минимальных затрат.

3.3.1. Общие принципы технологии ATM

Технология ATM (Asynchronous Transfer Mode) использует асинхронный режим передачи данных и базируется на технологии коммутации ячеек (Cell) и стандарте IEEE 802.6. Главная особенность технологии ATM в дополнение к высокому диапазону скоростей (от 155 Мбит/с до 2,5 Гбит/с) – ее способность к управлению трафиком мультисреды (multimedia), изменяющемуся от передачи данных и графики до речи и изображений. Режим асинхронной передачи ATM коммутирует ячейки с фиксированной длиной 53 байта между узлом-отправителем и узлом-получателем как в LAN, так и WAN. Для реализации ATM необходимы два главных компонента: коммутаторы и концентраторы ATM для LAN, серверов и высокопроизводительных рабочих станций. Наибольшее применение технология ATM находит для передачи больших файлов по магистральным каналам со скоростью от 155 до 622 Мбит/с. Многие специалисты в области компьютерных сетей считают, что в двадцать первом веке технология ATM станет основной.

В настоящее время сетевые компоненты по технологии ATM производятся многими известными фирмами: IBM, Bellcore, Cisco, 3Com, Bay Networks, Cabletron и др. При этом разработки этих фирм базируются на двух существующих стандартах технологии ATM: американском стандарте SONET (Synchronous Optical Network) и европейском стандарте синхронной цифровой иерархии SDH (Synchronous Digital Hierarchy). Эти стандарты определяют два уровня (физический и канальный) и включают в себя:

- стандартный мультиплексный формат с произвольным числом сигналов на 51,84 Мбит/с в качестве строительных блоков для построения общих потоков данных;
- стандарт на оптический сигнал для соединительного оборудования различных производителей;
- разнообразные режимы работы и администрирования как часть стандарта;
- стандартный синхронный мультиплексный формат для передачи низкоуровневых цифровых сигналов;
- стандарт на гибкую архитектуру с возможностью включения будущих приложений (например, широкополосной сети с интеграцией услуг ISDN).

Приведем краткую характеристику уровней стандарта SONET.

3.3.2. Физический уровень

Спецификация SONET определяет иерархию стандартных скоростей передачи цифровых данных. Нижний уровень STS-1 (Synchronous Transport Signal уровня 1) определен в 51,84 Мбит/с. Несколько сигналов STS-1 могут быть объединены в сигнал STS-N. Сигнал создается посредством чередования байтов и сигналов STS-1, которые синхронизируются друг с другом. Спецификация устанавливает наивысшую скорость передачи STS-48 в 2,5 Гбит/с.

3.3.3. Канальный уровень

Основным строительным блоком в SONET служит кадр STS-1. Он состоит из 810 октетов и передается каждые 125 мкс при общей скорости передачи данных в 51,84 Мбит/с. Административную и управляющую информацию несут 27 октетов кадра. Весь остаток кадра занимает полезная информация, в том числе 9 служебных октетов на задание пути, не обязательно с первой доступной позиции кадра. Служебные октеты кадра содержат указатель на начало октетов пути.

В традиционных сетях с коммутацией каналов подавляющая часть мультиплексоров и каналов телефонных компаний требует разуплотнения и повторного уплотнения всего сигнала для получения доступа к адресуемому узлу информации. Например, мультиплексор *B* получает данные по единственному каналу связи со скоростью 51,84 Мбит/с от мультиплексора *A* и передает данные мультиплексору *C*. В полученном сигнале один канал на 64 Кбит/с адресуется узлу *B*. Весь остальной сигнал будет передан узлу *C* и затем дальше по сети.

Для извлечения этого одного канала в 64 Кбит/с мультиплексор *B* должен разуплотнить каждый бит сигнала на 51,84 Мбит/с, извлечь данные и затем уплотнить каждый бит.

SONET предлагает стандартизованную возможность удаления и вставки не только для каналов на 64 Кбит/с, но и более высокоскоростных. При таком подходе используется набор указателей на местоположение каналов внутри полезной информации и самой полезной информации внутри кадра. Таким образом, можно получить доступ к информации, вставить и извлечь ее посредством простого изменения указателей.

Информация об указателях находится в октетах пути, описывающих мультиплексную структуру каналов и полезной информации. Указатель в служебных октетах кадра выполняет аналогичную функцию для всей полезной информации.

SONET выступает в роли магистрального носителя трафика АТМ. При этом поток ячеек АТМ передается как полезная информация син-

хронного трафика SONET. На передачу ячеек может быть отведен как целый кадр, так и его часть.

3.3.4. Передача данных в региональной сети ATM

Процесс передачи данных в сети ATM рассмотрим на примере схемы, приведенной на рис. 38. Она включает в себя следующие основные компоненты: коммутаторы, концентраторы и конечные системы (LAN, серверы и рабочие станции).

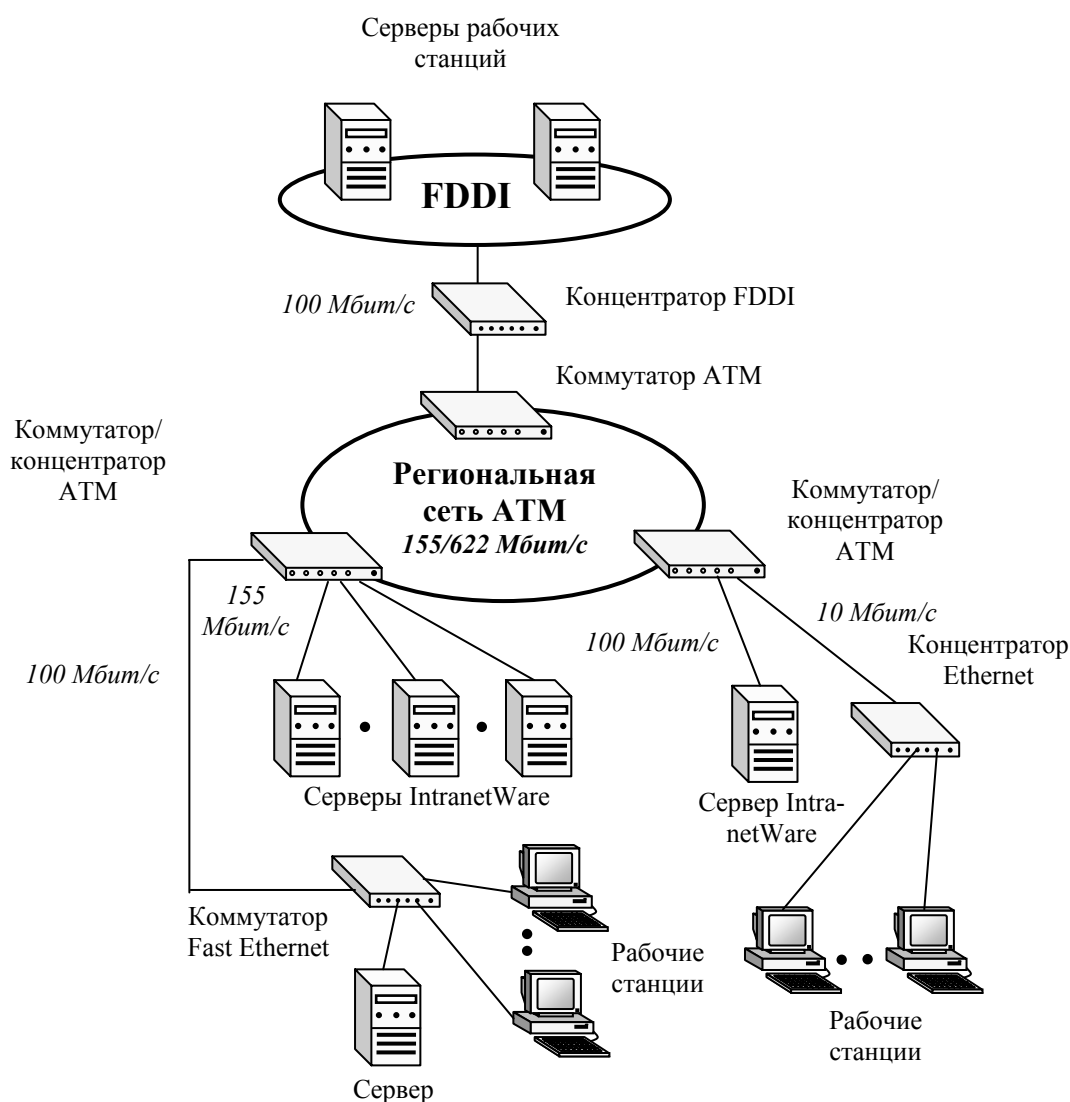


Рис. 38. Схема региональной сети ATM

Концентратор ATM – это устройство, предназначенное для объединения нескольких конечных систем и подключения их к сети ATM

через коммутатор. Он обычно состоит из нескольких монтируемых в стойку модулей, каждый из которых имеет порты с заданными скоростью и протоколами. В концентраторе АТМ каждая конечная система имеет выделенный прямой канал связи с концентратором, а также необходимое аппаратное и программное обеспечение для интерфейса с конкретным типом локальной сети.

Коммутатор АТМ – это устройство, предназначенное для установления виртуальных каналов и коммутации ячеек, передаваемых от источника к потребителю через коммуникационную подсеть сети АТМ. Он имеет несколько входных и выходных линий, число которых, как правило, совпадает, так как соединения являются двусторонними. Коммутаторы АТМ являются синхронными (хотя сам протокол является асинхронным) в том смысле, что во время одного цикла одна ячейка берется с каждой входной линии (если она, конечно, есть), проводится через внутреннюю коммутационную структуру и подается на нужную выходную линию.

Коммутаторы могут производить и конвейерную обработку, т. е. обработка поступившей ячейки происходит за несколько циклов, прежде чем она появляется на выходной линии. Ячейки поступают нерегулярно, поэтому начало каждого цикла определяется главным тактовым генератором. Ячейка подвергается обработке, т. е. коммутации, в том случае, если она полностью поступила к началу очередного цикла, иначе она ждет очередного цикла. Если ячейки прибывают со скоростью 155 Мбит/с, то длительность цикла составляет 2,7 мкс, при скорости 622 Мбит/с цикл длится 700 нс.

Коммутатор АТМ должен отвечать двум основным требованиям: во-первых, количество потерянных ячеек должно быть минимальным, во-вторых, ячейки, принадлежащие к одному и тому же виртуальному каналу, ни при каких обстоятельствах не могут менять порядок следования. Первое требование в цифровом выражении составляет одну ячейку из 10^{12} , т. е. крупный коммутатор может терять не более 1–2 ячеек в час. Второе условие налагает очень жесткие ограничения на схему коммутатора, таково требование стандарта АТМ.

Рассмотрим принципы функционирования одного из коммутаторов (рис. 39), который получил название коммутатор с выбыванием ячеек.

Одна из основных проблем при разработке принципиальной схемы коммутатора АТМ состоит в том, как поступить, если несколько прибывших одновременно, точнее к началу одного такта, ячеек предназначаются для одной и той же линии. Простейшее решение заключается в передаче одной ячейки и отбрасывании всех остальных. Это решение характеризуется низкой эффективностью.

Более эффективна организация очереди для каждой входной линии. Если две или более ячейки нужно передать на одну и ту же выходную ли-

нию, то одна ячейка, например, взятая случайным образом, коммутируется, а другая ждет следующего цикла. Но здесь может возникнуть другая проблема: ожидающая своей очереди ячейка блокирует все поступившие следом за ней на ту же линию ячейки, которые, возможно, направляются на другие выходные линии и могли бы быть обработаны. Этот эффект называется блокированием первого в очереди. Кроме того, при большом числе входных линий конфликт может быть обнаружен только тогда, когда ячейки прибывают на выходную линию. Иногда эта проблема решается путем отправки лишних ячеек назад по обратной шине в очередь на входной линии. При этом может возникнуть потенциальная опасность изменения порядка следования ячеек.

Входные линии

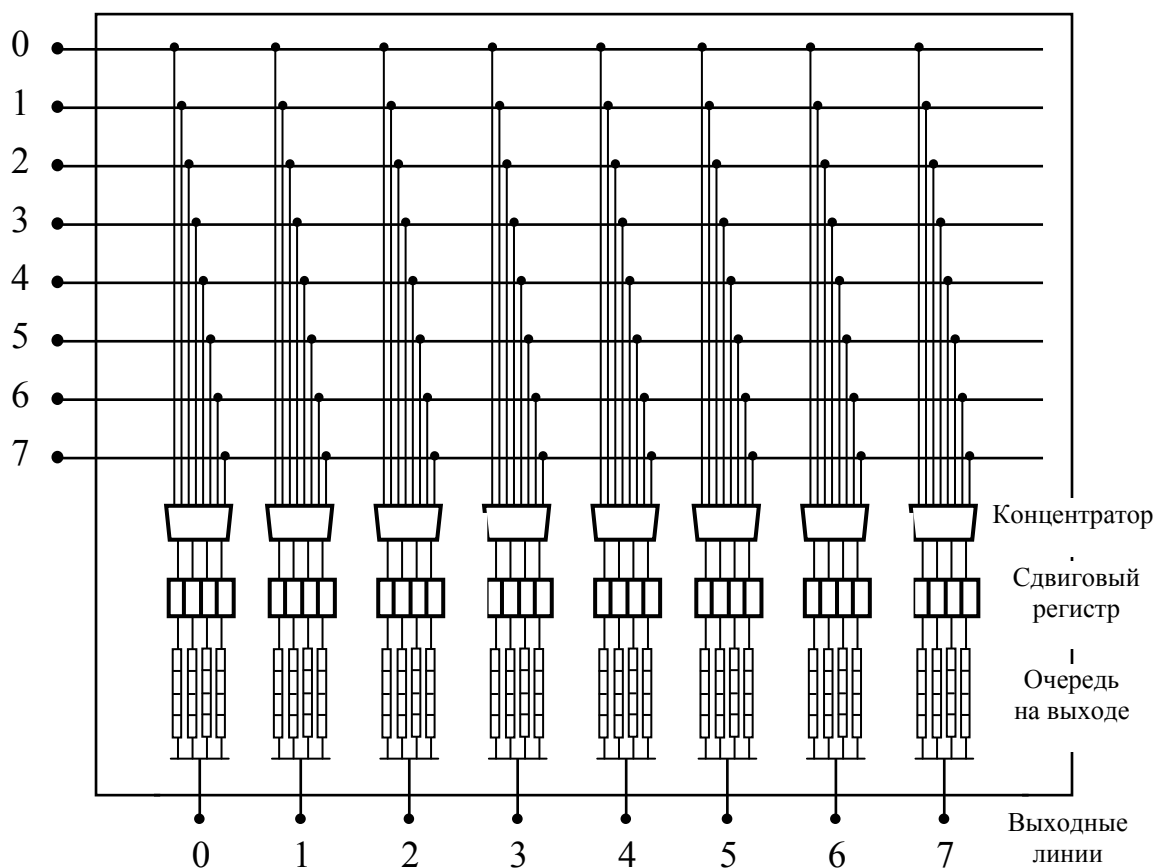


Рис. 39. Схема коммутатора ATM с выбыванием ячеек

Альтернативная схема состоит в организации очереди на выходной линии. В этом случае обе ячейки коммутируются, но при этом одна из них передается на выходную линию, а другая становится к ней в очередь. Каждая входная линия коммутатора подключена к шине, на кото-

рую поступают ячейки. Наличие всего одного задающего устройства значительно упрощает коммутацию и синхронизацию.

Функциональные схемы коммутатора анализируют заголовок каждой поступившей ячейки для определения информации о виртуальном канале, сопоставляют ее с таблицей маршрутов и активизируют соответствующий коммутирующий элемент. Ячейка передается по шине до активного коммутирующего элемента, где она поворачивает в направлении выходной линии. Кроме того, одна ячейка может быть направлена на несколько выходных линий посредством активизации нескольких коммутирующих элементов на широковещательной шине.

Простейший способ разрешения конфликтов состоит в помещении всех ячеек в буфер. Если коммутатор имеет 1024 входные линии, то в худшем случае потребуется 1024 буфера. На практике ситуация, когда все поступившие ячейки направляются на одну и ту же выходную линию, маловероятна, поэтому разработчики коммутаторов ограничиваются числом буферов N . В случае такого маловероятного события, как прибытие больше чем N ячеек, устройство, называемое концентратором, выбирает N ячеек, а остальные отбрасывает. Концентратор – это интеллектуальная схема для организации отбора ячеек.

Желательно, чтобы все выбранные ячейки поместились в одну выходную очередь (если она переполнена, все ячейки отбрасываются). Однако помещение всех ячеек в одну очередь за выделенное время невозможно. Поэтому выходная очередь представляет собой несколько очередей. Прошедшие концентратор ячейки попадают в сдвиговый регистр, который распределяет их равномерным образом между N выходными очередями. Последовательность отправки ячеек из той или иной очереди отслеживается при помощи маркера.

Существенным недостатком коммутатора с выбыванием является наличие большого числа коммутирующих элементов, которое равно квадрату числа линий. При числе линий 1024 число коммутирующих элементов будет более миллиона. В связи с этим существуют другие способы построения коммутаторов. Из-за ограничения объема они в настоящем пособии не рассматриваются.

Методические указания

В процессе изучения этого раздела пособия необходимо уяснить следующие моменты:

- региональные компьютерные сети (WAN) представляют собой LAN, связанные между собой высокоскоростными цифровыми магистральными каналами связи;

- WAN строятся на основе двух технологий: FDDI и ATM;
- технология FDDI ориентирована на построение двунаправленных кольцевых WAN на оптическом волокне;
- сети FDDI обладают повышенной отказоустойчивостью, которая обеспечивается применением двух колец передачи данных: основного и резервного;
- скорость передачи данных в сети FDDI составляет 100 Мбит/с, общая длина – до 100 км при числе станций до 500;
- структура кадров данных сети FDDI соответствует стандарту IEEE 802.5 (LAN Token Ring); в сети FDDI, в отличие от LAN Token Ring, в каждый момент времени может циркулировать множество пакетов данных, переданных различными станциями;
- в качестве пакетов данных в технологии ATM используются ячейки, имеющие фиксированную длину 53 байта;
- в основе технологии ATM лежат коммутация ячеек (Cell) и мультиплексирование виртуальных каналов, передающих данные, речь и изображение;
- максимальная скорость передачи данных в сетях ATM составляет 622 Мбит/с;
- в сетях ATM отсутствует управление потоком и контроль ошибок в промежуточных узлах коммутации;
- в сетях ATM мультиплексирование виртуальных каналов и соответствующих им ячеек происходит не на сетевом уровне, как в модели ISO/OSI, а на канальном уровне;
- в сетях ATM выделение полезной информации (демультиплексирование виртуальных каналов) происходит с помощью системы указателей, содержащихся в передаваемом кадре;
- для построения сетей ATM используются два типа устройств: концентраторы и коммутаторы;
- концентратор ATM – это устройство, предназначенное для объединения нескольких конечных систем (LAN и серверов) и подключения к коммутатору;
- коммутатор ATM – это устройство, предназначенное для установления виртуальных каналов и коммутации ячеек, передаваемых через коммуникационную подсеть;
- в связи с отсутствием в сетях ATM управления потоком и контроля ошибок коммутаторы ATM должны исключать возможность потери ячеек в процессе их коммутации.

Глава 4

ГЛОБАЛЬНЫЕ КОМПЬЮТЕРНЫЕ СЕТИ

4.1. Общие принципы построения глобальных компьютерных сетей

Глобальные компьютерные сети (GAN) объединяют WAN, компьютерные сети стран, материков. Построение этих сетей выполняется строго в соответствии с международными стандартами. Примером глобальной сети является сеть INTERNET, которая соединила в себе национальные сети стран мира, содержит сотни миллионов компьютеров, обеспечивает удаленный доступ к мировым информационным ресурсам (в том числе национальным библиотечным фондам), позволяет передавать и принимать сообщения в режиме электронной почты (E-mail) абонентам, находящимся на разных материках.

В зависимости от способа передачи данных GAN подразделяются на два больших класса: сети X.25 и сети TCP/IP. Принадлежность GAN к одному из этих двух классов определяется типом используемого для передачи данных сетевого протокола. В сетях X.25 для передачи данных через коммуникационную подсеть применяется протокол сетевого уровня X.25, реализующий метод виртуальных соединений. Сети TCP/IP строятся на датаграммном способе передачи данных, когда маршрут передаваемых сообщений (датаграмм) заранее не определен и зависит от степени загрузки каналов связи и узлов коммуникации. Эти сети используют для передачи данных семейство протоколов транспортного (TCP) и сетевого (IP) уровней.

В связи с тем, что все GAN содержат общие принципы организации физического уровня, представляется целесообразным вначале рассмотреть эти принципы, а затем особенности построений сетей X.25 и TCP/IP. Физический уровень GAN в значительной степени определяется требованиями, которые содержатся в моделях ISO/OSI и IEEE 802. В качестве каналов связи в GAN используются телефонные кабели, радиорелейные линии связи, волоконно-оптические магистральные каналы, ССС (основные характеристики этих каналов связи были рассмотрены ранее, в разделе 1.1).

Одной из основных составляющих физического уровня GAN является аппаратура передачи данных, с помощью которой осуществляется подключение абонента к коммуникационной подсети и преобразование физических сигналов. Если подключение абонента выполняется через LAN, то

для этого необходим сетевой контроллер, содержащий приемопередатчик и преобразователь двоичного цифрового сигнала в манчестерский код. Описание этих устройств было приведено ранее, в разделе 2.1.

Особенность физического уровня GAN состоит в применении специальных устройств-модемов для подключения удаленных сетевых абонентов к коммуникационной подсети по телефонным каналам связи. Слово модем является сокращением от слов «модулятор», «демодулятор». *Модем* – это устройство, преобразующее двоичные цифровые сигналы, поступающие с компьютера, в частотно-модулированные сигналы, которые необходимо передавать на большие расстояния (десятки и сотни километров) по телефонным каналам связи. При приеме модем осуществляет обратное преобразование модулированных сигналов в двоичный цифровой код, который обрабатывается принимающим компьютером.

Существуют три основных способа модуляции двоичных цифровых сигналов: амплитудная, фазовая и частотная. Схемы модуляции приведены на рис. 40.

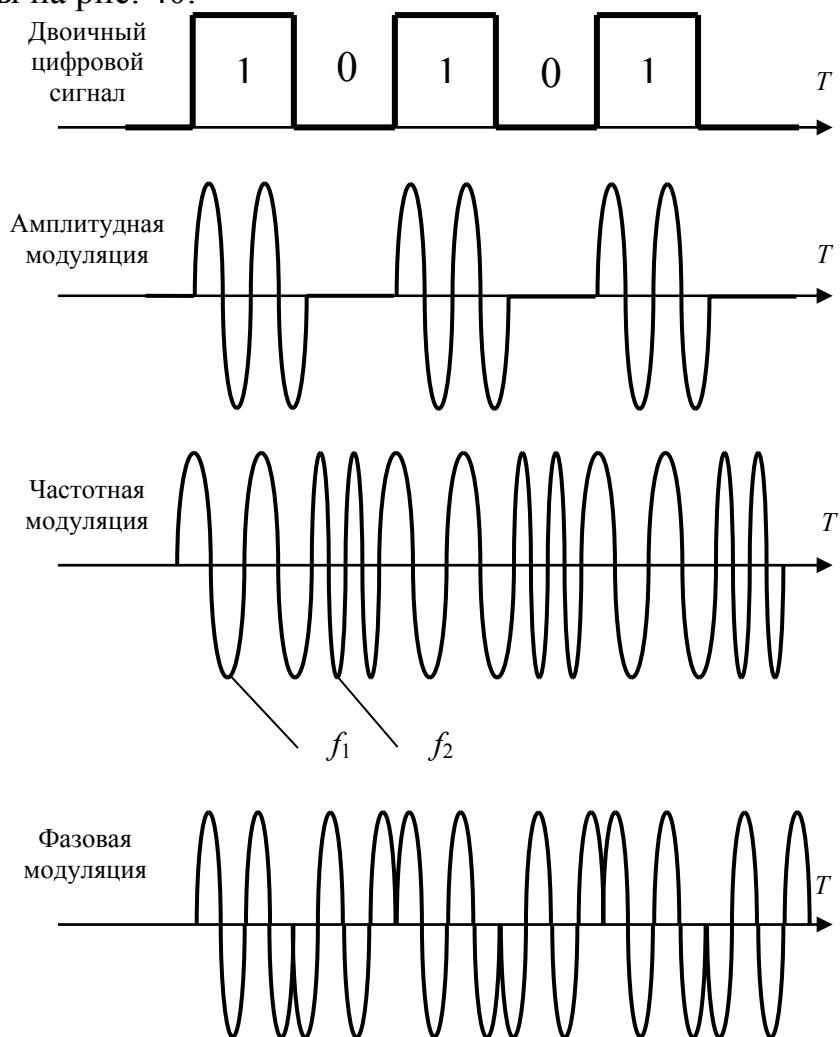


Рис. 40. Схемы модуляции двоичных цифровых сигналов

При амплитудной модуляции производится модуляция амплитуды несущей частоты двоичного сигнала.

При частотной модуляции значения 0 и 1 двоичного сигнала передаются сигналами с различной частотой: f_1 и f_2 .

При фазовой модуляции значениям сигналов 0 и 1 соответствуют сигналы частоты f_1 с разной фазой.

Существуют дискретные способы модуляции, применяемые для преобразования аналоговых сигналов, например речевых, в цифровые. Для этих целей широко используются амплитудно-импульсная, кодово-импульсная и времяимпульсная модуляция. Устройства на их основе применяются для построения сетей с интеграцией услуг ISDN и ATM (одновременная передача речи, данных и видеоизображения). Схема соединения компьютеров через телефонную сеть представлена на рис. 41.

Чтобы модемы могли обмениваться друг с другом информацией, необходимо, чтобы они использовали одинаковые способы преобразования цифровых данных в аналоговые и обратно. Другими словами, модемы должны применять одинаковые способы модуляции и демодуляции сигналов.



Рис. 41. Схема соединения компьютеров через телефонную сеть

Для разработки стандартов передачи данных был создан специальный Международный консультативный комитет по телеграфии и телефонии (*International Consultative Committee for Telegraphy and Telephony – CCITT*). Он разработал рекомендации, определяющие способы модуляции и демодуляции сигналов, алгоритм соединения модемов, протоколы коррекции ошибок, протоколы сжатия передаваемой информации и т. д. *Рекомендации CCITT для модемов пронумерованы и имеют в своем обозначении префикс V*. Наиболее распространенные рекомендации CCITT приведены в табл. 2.

Кроме скорости передачи информации, определяющей производительность модема в соответствии с рекомендацией CCITT, существуют еще две важные характеристики: режим передачи данных (дуплексный и полудуплексный) и способ передачи данных (асинхронный или синхронный).

Дуплексный режим работы модема позволяет одновременно передавать данные в двух направлениях. В дуплексном режиме работают модемы, соответствующие рекомендациям CCITT V.21, V.22, V.22 bis и V.32.

Полудуплексный режим (как и дуплексный) позволяет передавать данные в обоих направлениях, но в разные моменты времени. Таким образом, при полудуплексном режиме работы модема и одинаковой скорости передачи, данных будет передано в два раза меньше, чем при дуплексном режиме.

Таблица 2

Рекомендации CCITT для различных типов модемов

№ п/п	Рекомендация	Скорость передачи, бит/с
1	V.21	300
2	V.22	600, 1200
3	V.22 bis	1200, 2400
4	V.23	1200
5	V.32	4800, 9600
6	V.32 bis	7200, 12000, 14400
7	V.34	28800

При передаче данных по зашумленным телефонным линиям всегда существует большая вероятность того, что данные, переданные одним модемом, будут приняты другим модемом в искаженном виде. Некоторые передаваемые байты могут изменить свое значение или даже просто исчезнуть. Могут быть приняты данные, которые не были переданы удаленным модемом, т. е. принимающий модем может распознать принятый шум на линии как данные.

Для того чтобы пользователь имел гарантию, что его данные переданы без ошибок, используются протоколы коррекции ошибок.

Общая форма передачи данных по протоколам с коррекцией ошибок заключается в следующем: модем передает данные отдельными кадрами, размер которых определяется качеством связи. Каждый кадр снабжается заголовком, в котором указывается контрольная сумма кадра. Принимающий модем самостоятельно подсчитывает контрольную сумму каждого кадра и сравнивает ее с контрольной суммой из заголовка принятого кадра. Если эти две контрольные суммы совпали, считается, что кадр принят без ошибок. В противном случае принимающий модем отправляет передающему модему запрос на повторную передачу этого кадра. Передача сбойного кадра продолжается до тех пор, пока он не будет принят правильно.

Протоколы коррекции ошибок могут быть реализованы не только на аппаратном, но и на программном уровне. Аппаратный уровень реализации более эффективен. Наиболее распространены следующие протоколы коррекции, реализованные на аппаратном уровне: от MNP1 до MNP10 и V.42.

Современные модемы для ускорения передачи данных используют специальные протоколы, позволяющие производить сжатие передаваемой информации. Передающий модем сжимает данные, они в сжатом виде проходят через телефонный канал и принимаются удаленным модемом. Принимающий модем восстанавливает данные и передает их компьютеру.

Среди протоколов компрессии, реализованных на аппаратном уровне, наибольшее распространение получили протоколы MNP5 и MNP7, а также протокол, разработанный CCITT-V.42 bis. Протоколы MNP (Microcom Network Protocols) – серия аппаратных протоколов коррекции ошибок и сжатия передаваемой информации, разработанная и выпущенная фирмой Microcom, включает в себя 10 протоколов:

- *MNP1* и *MNP2* являются первыми версиями протоколов коррекции ошибок и имеют ограниченное распространение вследствие низкой эффективности.

- *MNP3* – *протокол* коррекции ошибок, поддерживающий синхронный дуплексный метод передачи данных между модемами.

- *MNP4* – *протокол*, поддерживающий синхронный дуплексный метод передачи информации. Обеспечивает большую эффективность, чем протоколы MNP2 и MNP3. Протокол MNP4 может менять размер передаваемых кадров данных при изменении числа ошибок на линии. При увеличении числа ошибок размер кадров уменьшается, увеличивая вероятность успешного прохождения отдельных кадров.

- *MNP5* – *протокол*, использующий простой метод сжатия передаваемой информации. Символы, часто встречающиеся в передаваемом кадре, кодируются цепочками битов меньшей длины, чем редко встречающиеся символы. Дополнительно кодируются длинные цепочки одинаковых символов. Обычно при этом текстовые файлы сжимаются до 35 % своей исходной длины. Следует заметить, что при передаче уже сжатых данных, например, архиватором ARJ дополнительного увеличения эффективности за счет сжатия данных модемом не происходит.

- *MNP6* – *протокол*, который дополняет протокол MNP4 автоматическим переключением между дуплексным и полудуплексным методом передачи в зависимости от типа передаваемой информации. Протокол MNP6 также обеспечивает совместимость с протоколом V.29 (полудуплексный протокол, используемый в факс-модемах).

- *MNP7* – *протокол*, который по сравнению с протоколом MNP5, использует более эффективный метод сжатия данных.

- *MNP9* – протокол, который использует рекомендации V.32 и соответствующий метод работы, обеспечивающий совместимость с низкоскоростными модемами.

- *MNP10* – протокол, предназначенный для обеспечения связи на сильно зашумленных линиях, таких как линии сотовой связи, междугородные линии, сельские линии. Стабильность связи достигается за счет многократного повторения попытки установить связь, изменяя размеры кадра данных и скорости передачи в соответствии с уровнем помех на линии.

Все протоколы MNP совместимы между собой снизу вверх. При установлении связи происходит установка наивысшего возможного уровня MNP-протокола. Если один из связывающихся модемов не поддерживает протокол MNP, то MNP-модем работает без него.

- *Рекомендация CCITT V.42*. Вскоре после разработки фирмой Micromcom протоколов коррекции ошибок MNP CCITT приступил к созданию стандарта V.42. Модемы, соответствующие рекомендации V.42, более устойчивы и обеспечивают бóльшую производительность, чем модемы с поддержкой протоколов MNP. Рекомендация V.42 включает в себя протоколы MNP3, MNP4, чтобы обеспечить совместимость со старыми модемами, и новый протокол коррекции ошибок LAMP (Link Access Procedure for Modems). Протокол LAMP включается только в том случае, если модем соединился с другим модемом, поддерживающим рекомендацию V.42.

- *Рекомендация CCITT V.42 bis*. Протокол V.42 bis использует метод компрессии, при котором определяется частота появления отдельных символьных строк и происходит их замена на последовательности символов меньшей длины (токены). Этот алгоритм компрессии носит название Lempel-Ziv.

За счет применения алгоритмов Lempel-Ziv модемы, реализующие V.42 bis, сильнее сжимают данные, чем модемы, поддерживающие MNP5.

Модем может работать в двух основных режимах: командном и обмена данными. В режиме обмена данными он может принимать и передавать данные между компьютером и удаленным модемом. При этом компьютер принимает и передает данные от модема через асинхронный порт (COM-порт), к которому подключен модем.

В командном режиме управляющие команды передаются от компьютера модему также через COM-порт. В командном режиме можно изменить характеристики обмена данными, условия связи, заставить модем набирать номер удаленного модема, принять от него вызов.

После выпуска американской фирмой Hayes модемов серии Smart-modem система команд, использованная в ней, стала стандартом,

которого придерживаются остальные разработчики модемов. Система команд, примененная в этих модемах, носит название Hayes-команд, или AT-команд. Со временем выпуска первых AT-совместимых модемов набор их команд дополнился и стал называться расширенным набором AT-команд.

4.2. Принципы построения сетей X.25

Сети X.25 соответствует модели ISO/OSI и называются пакетными сетями. Особенности их построения заключаются в организации верхних уровней: канального, сетевого и транспортного.

4.2.1. Канальный уровень

На канальном уровне передача данных осуществляется с помощью протокола HDLC (High – Level Data Link Control), разработанного в 1979 году. Структура кадра данных этого протокола приведена на рис. 42. Она включает в себя следующие элементы.

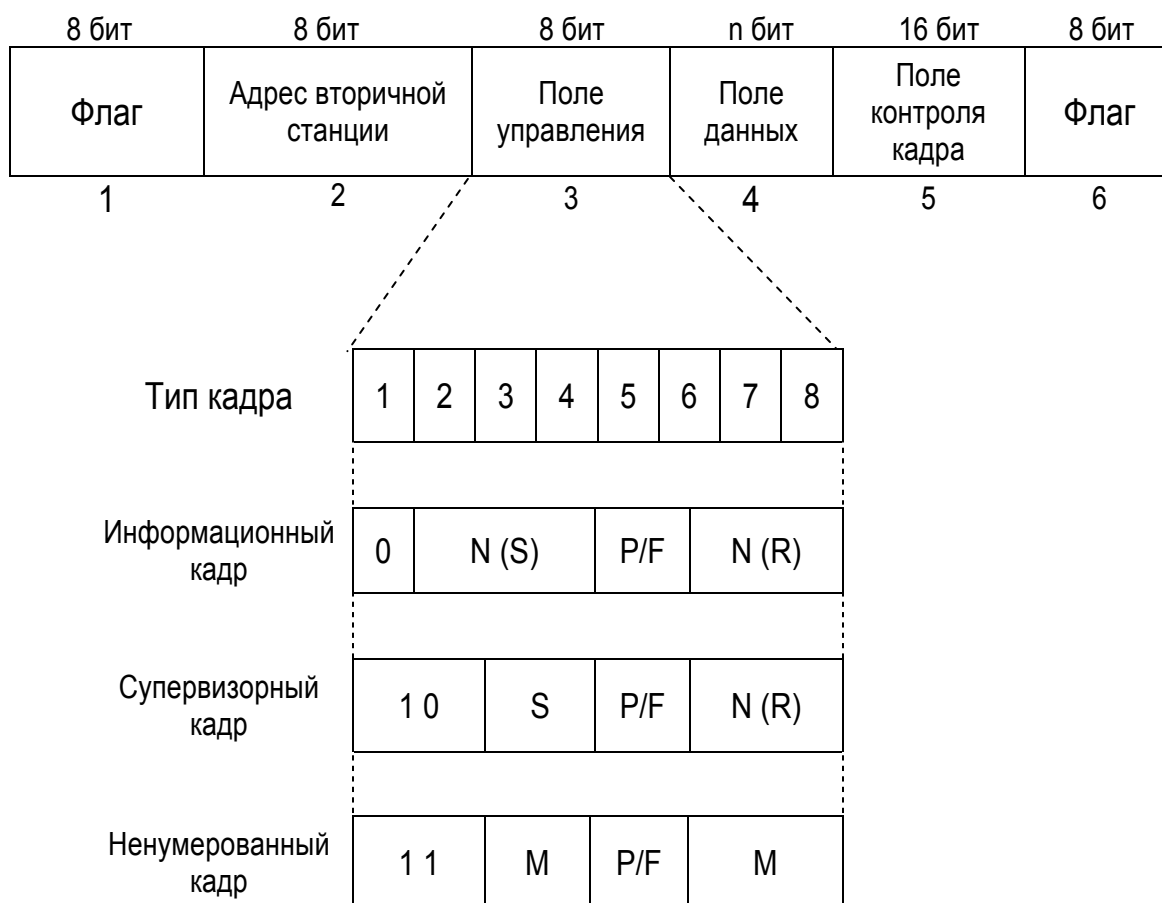


Рис. 42. Структура кадра HDLC

Флаги. Предназначены для выделения начала и конца кадра, имеют двоичный код 01111110.

Адрес вторичной станции. В протоколе HDLC существует одна главная (первичная) станция и несколько подчиненных (вторичных) станций. Первичная станция несет ответственность за инициирование всех переносов данных, а также инициацию канала и управление им.

Станции в HDLC могут передавать и принимать *кадры* нескольких типов, которые *делятся на команды и ответы*. *Команды* передаются от первичной станции ко вторичной. *Ответы* представляют собой реакцию на команду и передаются в обратном направлении. В HDLC только вторичные станции идентифицируются с помощью адреса. Адрес, входящий в состав кадра, является адресом вторичной станции, участвующей в соответствующем обмене. Первичная станция передает команду с адресом той вторичной станции, которой предназначена эта команда. Вторичная станция передает ответы, содержащие ее адрес и предназначенные первичной станции данные.

Поле управления. Передаваемые кадры делятся на три типа: информационные – значение 0 в бите 1; супервизорные определяются значениями битов 1–4; нумерованные определяются значениями битов 1–4 и 6–8.

В байте управления информационного кадра указываются номера $N(S)=0..7$ и $N(R)=0..7$ передаваемого и принимаемого кадра, в супервизорных кадрах указывается только номер $N(R)$ принимаемого кадра. Бит 5 поля управления называется битом запроса в командах и битом окончания в ответах. Когда станция получает команду с битом запроса $P=1$, она обязуется сформировать ответ с битом окончания $F=1$.

Информационные кадры служат для передачи пакетов, представленных в поле данных. Супервизорные кадры используются для восстановления кадров, потерянных из-за искажения информации в канале, а также для управления потоками кадров. Нумерованные кадры предназначены для установления соединений и разъединений, завершения соответствующих режимов передачи пакетов и для передачи информации о результатах выполнения этих действий.

Поле данных. Содержит передаваемый пакет данных.

Поле контроля кадра. При передаче данных формируется 16-разрядный циклический код (CRC) для позиций 2, 3 и 4, который включается в кадр. При приеме кадра вновь вычисляется контрольный циклический код. Если контрольные циклические коды совпадают, то принятый кадр считается корректным. В противном случае фиксируется искажение принятого кадра. При искажении флагов, разделяющих последовательно передаваемые кадры, два кадра сливаются в один иска-

женный кадр. Процедура формирования циклических кодов при передаче и приеме гарантирует обнаружение искажения этого типа.

Протокол HDLC обеспечивает несколько способов восстановления информационных кадров. Основным способом – использование тайм-аута. Когда супервизорные кадры подтверждают прием информационных кадров, таймер перезапускается на величину тайм-аута. Номер $N(R)$, полученный вторичной станцией, подтверждает прием всех кадров с номерами, меньшими $N(R)$. Если тайм-аут закончился, то вторичная станция начинает повторную передачу кадров, прием которых не подтвержден. Для повышения эффективности использования канала предусмотрена посылка отрицательных квитанций: супервизорных кадров «Отказ» и «Селективный отказ». Если принятый кадр искажен из-за ошибки, обнаруженной с помощью циклического суммирования, первичная станция, не дожидаясь окончания тайм-аута, посылает отрицательную квитанцию «Отказ», содержащую номер ожидаемого кадра $N(R)$, и ждет поступления информационного кадра с этим номером. При этом все поступающие кадры с большими номерами игнорируются принимающей станцией. Эффективность использования канала еще более повышается за счет селективной отбраковки. В этом случае станция, ожидающая кадр $N(R)$ и получившая кадр $N(R)+1$, принимает его и последующие кадры, извещая передающую станцию супервизорным кадром «Селективный отказ» о потере кадра $N(R)$. В ответ на команду «Селективный отказ» передающая станция повторно передает потерянный кадр. Отрицательные квитанции «Отказ» и «Селективный отказ» не исключают необходимость в тайм-ауте, поскольку квитанции могут быть потеряны в канале.

Для разъединения связи между станциями используется нумерованный кадр с командой «Разъединить», подтверждаемый ответом «Подтверждение».

4.2.2. Сетевой уровень

Рекомендации X.25 определяют два основных вида обслуживания в сети коммутации пакетов: постоянные виртуальные каналы и коммутируемые виртуальные соединения. Для обеспечения одновременной работы многих постоянных виртуальных каналов и виртуальных соединений используются логические каналы. Каждому виртуальному соединению присваивается групповой номер логического канала (ГНЛК) и номер логического канала (НЛК). Коммутируемому виртуальному соединению ГНЛК и НЛК присваиваются в фазе установления соединения, а постоянным виртуальным каналам ГНЛК и НЛК присваиваются по соглашению с администрацией сети во время постановки на обслуживание.

Формат пакета X.25 приведен на рис. 43.

4 бита	4 бита	8 бит	8 бит	n бит
Идентификатор общего формата	ГНЛК	НЛК	Тип пакета	Данные или управляющая информация
1	2	3	4	5

Рис. 43. Формат пакета X.25

Идентификатор общего формата. Код, определяющий общий формат пакета.

Групповой номер логического канала (ГНЛК). Код, определяющий групповой номер логического канала. Максимальное число групп равно 15.

Номер логического канала (НЛК). Код, определяющий номер логического канала. Максимальное число каналов равно 255.

Идентификатор типа пакета. Пакеты делятся на следующие типы: установление соединения и разъединения, данные и прерывание, управление потоком и сброс, рестарт.

Данные или управляющая информация. Этот раздел содержит передаваемые данные или управляющую информацию, которой обмениваются взаимодействующие абоненты.

4.2.3. Передача данных в глобальной сети X.25

Процесс взаимодействия абонентов сети по протоколу X.25 происходит следующим образом.

Вызывающий абонент передает в сеть по свободному логическому каналу пакет «запрос соединения», содержащий адрес вызываемого абонента. Вызываемый абонент может не принять запрос на соединение. В этом случае он передает пакет «запрос разъединения», в котором в качестве причины разъединения может быть указано «Номер занят». После этого вызываемый абонент не может использовать логический канал для получения пакета «подтверждение разъединения». Если сеть не может установить соединение с вызываемым абонентом, вызывающему абоненту посылается пакет «указание разъединения», содержащий причину разъединения: нереализуемый вызов, номер занят, неразрешенный вызов, перезагрузка сети и т. д. Если вызываемый абонент принимает запрос на соединение, он передает пакет «согласие на соединение», после чего сеть посылает вызываемому абоненту пакет «подтверждение соединения». Этим заканчивается фаза установления соединения между абонентами. Начиная устанавливать соединение, вызывающий абонент запускает таймер. Если в течение тайм-аута не поступил пакет «подтверждение соединения», абонент передает пакет «за-

прос разъединения», после чего процедура установления соединения может повторяться.

После установления соединения начинается фаза передачи пакетов данных. Протокол X.25 допускает использование следующих значений длины поля данных: 16, 32, 64, 128, 256, 512 и 1024 байт. Предпочтительной является длина 128 байт.

Для ликвидации и сброса всех постоянных и временных виртуальных соединений, установленных с абонентом, используется процедура рестарта, инициируемая абонентом с помощью пакета «запрос рестарта» и сетью с помощью пакета «указание рестарта». При этом ликвидируются соединения, относящиеся ко всем логическим каналам абонента, и стираются все пакеты, передаваемые через эти соединения. Для восстановления потерянных пакетов используются средства более высокого уровня иерархии.

Для передачи срочных данных используются нумерованные пакеты «прерывание от сети» и «прерывание от абонента», несущие в себе один байт данных о причине прерывания. Эти пакеты доставляются получателю независимо от состояния передачи нумерованных пакетов, даже тогда, когда пакеты данных не принимаются. Получение этих пакетов подтверждается соответствующими пакетами-квитанциями. При использовании однонаправленных логических каналов абонент может запросить повторную передачу пакета с помощью пакета «отказ», несущего в себе номер пакета (NCR), начиная с которого нужно провести повторную передачу.

По окончании передачи постоянные виртуальные каналы закрываются и происходит их разъединение.

4.2.4. Перспективы развития сетей X.25. Сети Frame Relay

Сети X.25 эффективно работают на каналах с плохим качеством передачи данных. Вместе с тем современные каналы связи (например, ВОЛС) характеризуются низким уровнем помех. С учетом этого для высокоскоростной передачи данных в GAN разработана новая технология – *Frame Relay (FR)*, которая представляет собой пакетную коммутацию или кадровую ретрансляцию. Она эффективно применяется в межсетевом оборудовании, в таком как мосты (*bridges*) и маршрутизаторы (*routers*).

FR предполагает относительно высокие скорости: от 64 Кбит/с до 1,544 Мбит/с. Она обрабатывает пакеты переменной длины, называемые *фреймами*. FR позволяет применять как постоянные, так и комму-

тируемые виртуальные каналы. Формат фрейма достаточно прост и включает в себя:

- десятибитовое поле идентификатора соединения канала данных;
- трехбитовое поле управления;
- поля указателя данных;
- 16-битовое поле контрольной последовательности.

Технология FR в значительной степени похожа на технологию АТМ. Основное отличие состоит в том, что в АТМ длина пакетов (ячеек) фиксирована, а в FR длина фреймов разная.

В соединениях FR, как и в АТМ, мультиплексирование нескольких виртуальных каналов осуществляется на втором (канальном) уровне, а контроль ошибок и управление потоком отсутствуют. Каждый кадр второго уровня содержит номер логического соединения, используемый для маршрутизации.

4.3. Принципы построения сетей TCP/IP. Глобальная сеть Internet

Модели GAN, построенные на основе протоколов X.25 и TCP/IP, приведены на рис. 44.

Семейство протоколов TCP/IP включает в себя протоколы двух уровней: TCP – протокол управления транспортировкой (*Transport Control Protocol*) и IP – протокол Internet (*Internet Protocol*). Однако семейство протоколов TCP/IP включает в себя и другие протоколы, приведенные в табл. 3.

Таблица 3

Семейство протоколов TCP/IP

Протокол	Назначение
IP (Internet Protocol)	Протокол Internet. Протокол сетевого уровня, обеспечивающий передачу данных между компьютерами
TCP (Transport Control Protocol)	Транспортный протокол (протокол контроля транспортировки). Передает данные между прикладными программами Internet
UDP (User Datagram Protocol)	Протокол пользовательских датаграмм. Передает данные между приложениями, является более простым и менее надежным, чем TCP
ICMP (Internet Control Message Protocol)	Протокол управляющих сообщений Internet. Управляет сетевыми сообщениями об ошибках и другими ситуациями, требующими вмешательства сетевых программ

В отличие от сетей X.25, которые строятся на основе модели ISO/OSI и имеют 7 уровней, сети TCP/IP включают в себя 5 уровней: физический, канальный, сетевой, транспортный и прикладной.



Рис. 44. Модели сетей X.25 и TCP/IP

При этом первые 4 уровня сети TCP/IP определяют способ транспортировки сообщений, которые называются датаграммами, а 5-й уровень (прикладной) – конкретный тип сети. В сети Internet этому уровню соответствуют протоколы HTTP, Telnet, FTP, SMTP, POP3 и др.

4.3.1. Физический уровень сети Internet

Глобальная сеть Internet представляет собой объединение LAN и WAN. В качестве каналов передачи данных, обеспечивающих взаимодействие LAN и WAN, в сети Internet применяются CCC и ВОЛС, основные характеристики которых приведены в разделе 1.

4.3.2. Канальный уровень сети Internet

Основным протоколом сети Internet на канальном уровне является протокол Point-to-Point (PPP). При разработке формата кадра этого протокола был использован протокол HDLC, структура кадра которого была описана ранее в разделе 4.2. Структура кадра протокола PPP приведена на рис. 45. Она включает в себя следующие разделы.

Флаги. Двоичный код 01111110 обозначает начало и конец кадра.

Адрес. Имеет постоянное значение, равное 11111111.

Поле управления. Принимает значение, равное 00000011.

Протокол. Код, определяющий тип передаваемых данных.

Информация. Раздел, содержащий передаваемые данные.

CRC. Контрольная последовательность кадра, формируемая как циклический избыточный код. Метод его формирования в настоящем пособии не рассматривается.

Кадр PPP может содержать данные трех типов: IP-датаграмму, поступившую (инкапсулированную) от протокола сетевого уровня; данные протокола управления соединением LCP; данные протокола управления сетью NCP.

Протокол управления соединением. Для обмена данными по протоколу PPP необходимо настроить канал связи и проверить его состояние. Для этих целей используется протокол LCP, формат пакета которого приведен на рис. 46. Он содержит следующие разделы.

Код. Обозначает тип пакета LCP, помещенного в кадр PPP.

Идентификатор. Обозначает порядковый номер пакета среди совокупности пакетов-запросов и пакетов-ответов, проходящих сквозь различные сетевые уровни, обслуживаемые PPP.

Длина. Этот раздел указывает на общую длину пакета LCP, включая поля «код», «идентификатор», «длина» и собственно «данные».



Рис. 45. Структура кадра протокола PPP

Данные. Поле данных может быть пустым.

Поле «код» может задавать три типа пакетов LCP: конфигурация соединения, окончание сеанса связи, управление соединением.

Флаг	Адрес	Поле управления	Протокол	Информация			
1	2	3	4	5			
				Код	Идентификатор	Длина	Данные

Рис. 46. Структура пакета протокола управления соединением LCP

Пакеты конфигурации соединений LCP. Предназначены для инициализации и установления соединения по протоколу PPP. Существуют четыре разновидности пакетов: «конфигурация-запрос» (Configure-Request), «конфигурация-подтверждение» (Configure-Ack), «конфигурация-неподтверждено» (Configure-Nak) и «конфигурация-отказ» (Configure-Reject).

Если компьютер не способен выполнить какое-либо условие желательной настройки соединения, он должен ответить пакетом «конфигурация-неподтверждено». Поле данных этого пакета содержит список неподдерживаемых вариантов настройки. Протокол LCP также разрешает помещать в поле данных пакета «конфигурация-неподтверждено» список дополнительных вариантов настройки соединения. Компьютер, получивший пакет «конфигурация-неподтверждено», должен ответить на запрос любых дополнительных вариантов настройки.

Протокол PPP продолжает обмениваться пакетами до тех пор, пока оба участника соединения не придут к единому мнению по поводу конфигурации соединения. Модуль PPP, обнаруживший неизвестный ему вариант настройки в пакете-запросе, обязан ответить пакетом «конфигурация-отказ». Поле данных пакета «конфигурация-отказ» содержит список только неизвестных вариантов. Разница между вариантами, помещенными в поле данных пакетов «конфигурация-отказ» и «конфигурация-неподтверждено», состоит в том, что варианты-«отказники» не подлежат дальнейшему обсуждению. Другими словами, PPP может изменить свое мнение о ранее неподтвержденном варианте конфигурации в процессе связи. В то же время варианты, перечисленные в пакете «конфигурация-отказ», больше никогда не будут запрашиваться.

Пакеты окончания сеанса связи PPP. Имеют две разновидности: «окончание-запрос» (Terminate-Request) и «окончание-подтверждено» (Terminate-Ack). Обе разновидности пакетов полностью игнорируют поле данных. Протокол PPP требует, чтобы компьютер, получивший пакет

«окончание-запрос», всегда отвечал передачей пакета «окончание-подтверждено».

Пакеты управления соединением LCP. Используются для управления и отладки во время сеанса связи. Определено пять разновидностей пакетов: «код-отказ» (Code-Reject), «протокол-отказ» (Protocol-Reject), «эхо-запрос» (Echo-Request), «эхо-ответ» (Echo-Reply) и «игнорировать запрос» (Discard Request).

Пакет «код-отказ» передается модулем PPP, принявшим пакет с неизвестным полем «код». Поле данных этого пакета содержит копию поля данных принятого пакета с неизвестным полем «код». Эта копия включает только данные из поля «информация». Пакет «протокол-отказ» передается в ответ на неопознанное значение поля «протокол» пакета PPP. Пакет «протокол-отказ» содержит двухбайтовое поле, идентифицирующее неопознанный протокол, а также его «неопознанные данные» (Rejected-Information). Чтобы протестировать состояние канала связи, PPP шлет пакеты «эхо-запрос» и «эхо-ответ». Модуль PPP, получивший пакет «эхо-запрос», должен ответить пакетом «эхо-ответ».

Пакет «игнорировать-запрос» предназначен для тестирования канала в одном направлении: от локального до удаленного компьютера.

Протокол управления сетью NCP. В процессе управления сетью PPP устанавливает параметры сетевого уровня. По окончании процесса PPP полностью готов к передаче данных вышележащим уровням и может начинать передачу данных. PPP может обслуживать несколько различных сетевых протоколов одновременно. Используя NCP, PPP может «на ходу» открыть новый или завершить обмен по старому сетевому протоколу. Например, PPP ведет обмен пакетами IP. В любой момент времени, не прекращая обмена пакетами IP, можно начать обмен по протоколу DECnet, пользуясь тем же последовательным соединением. Когда обмен пакетами DECnet станет не нужным, можно его завершить, не прекращая соединения по протоколу IP.

Таким образом, PPP при помощи NCP открывает, устанавливает и завершает сетевые соединения для нескольких сетевых протоколов. Для определенного сетевого протокола используется соответствующий протокол управления сетью. Например, NCP для IP отличается от NCP для DECnet.

4.3.3. Сетевой уровень сети Internet

Сетевой уровень Internet использует протокол IP (Internet Protocol) и протокол управляющих сообщений Internet (ICMP). Модуль IP выполняет основную работу сетевого уровня, и поэтому в дальнейшем основное внимание в пособии уделяется этому протоколу.

Адресация в сети Internet. Адрес в сети Internet может иметь несколько IP-адресов. Длина адреса в сети Internet составляет 32 бита, или 4 байта. IP-адрес может представляться в двоичном виде, в записи – «десятичное с точкой», и в символьном виде. IP-адрес в двоичном виде представляется следующим образом:

IP = 11000000 01100110 11111001 00000011.

Этот же адрес как «десятичное с точкой» можно представить так:

IP = 192.102.249.3.

Для задания IP-адресов широко используется система имен доменов (Domain Name System, DNS). Система имен доменов позволяет обращаться к сетевым компьютерам не только по их IP-адресам, но и по индивидуальным адресам, например, вместо IP-адреса 192.102.249.3 можно задать имя компьютера SONET.com.

Каждое из составляющих имени, например *ftp.microsoft.com*, называется меткой. В данном случае имя компьютера состоит из трех меток: *ftp*, *microsoft* и *com*. Метки отделены друг от друга точками.

Термин «домен» определяется как *сфера деятельности, отношений или выполнения каких-либо совместных функций*. Метка *ftp* означает, что данный компьютер является *хостом ftp*, т. е. на нем работает *ftp-сервер*. Метка *microsoft* описывает организацию (сферу деятельности), которой принадлежит компьютер – корпорации Microsoft. Метка *com* обозначает, что данный компьютер выполняет коммерческие функции.

Структура DNS похожа на структуру дерева каталогов. На вершине иерархии находится корневой каталог, не имеющий имени. Каждый домен DNS может разделяться на несколько поддоменов. На рис. 47 показана иерархическая структура системы имен доменов Internet.

Следующий уровень после корневого состоит из трех групп доменов верхнего уровня:

- Агра – это специальный домен, необходимый для преобразования IP-адресов в имена DNS;
- группа организаций, к которой принадлежит владелец данной сети. Она обозначается трехбуквенной меткой, например com, edu или gov;
- группа по стране пребывания или по географическому местоположению. Обозначается двухбуквенной меткой (наименование страны) в соответствии со списком, разработанным национальным институтом стандартов (ISO 3166).

Домены второй группы разделены на шесть основных категорий (табл. 4).

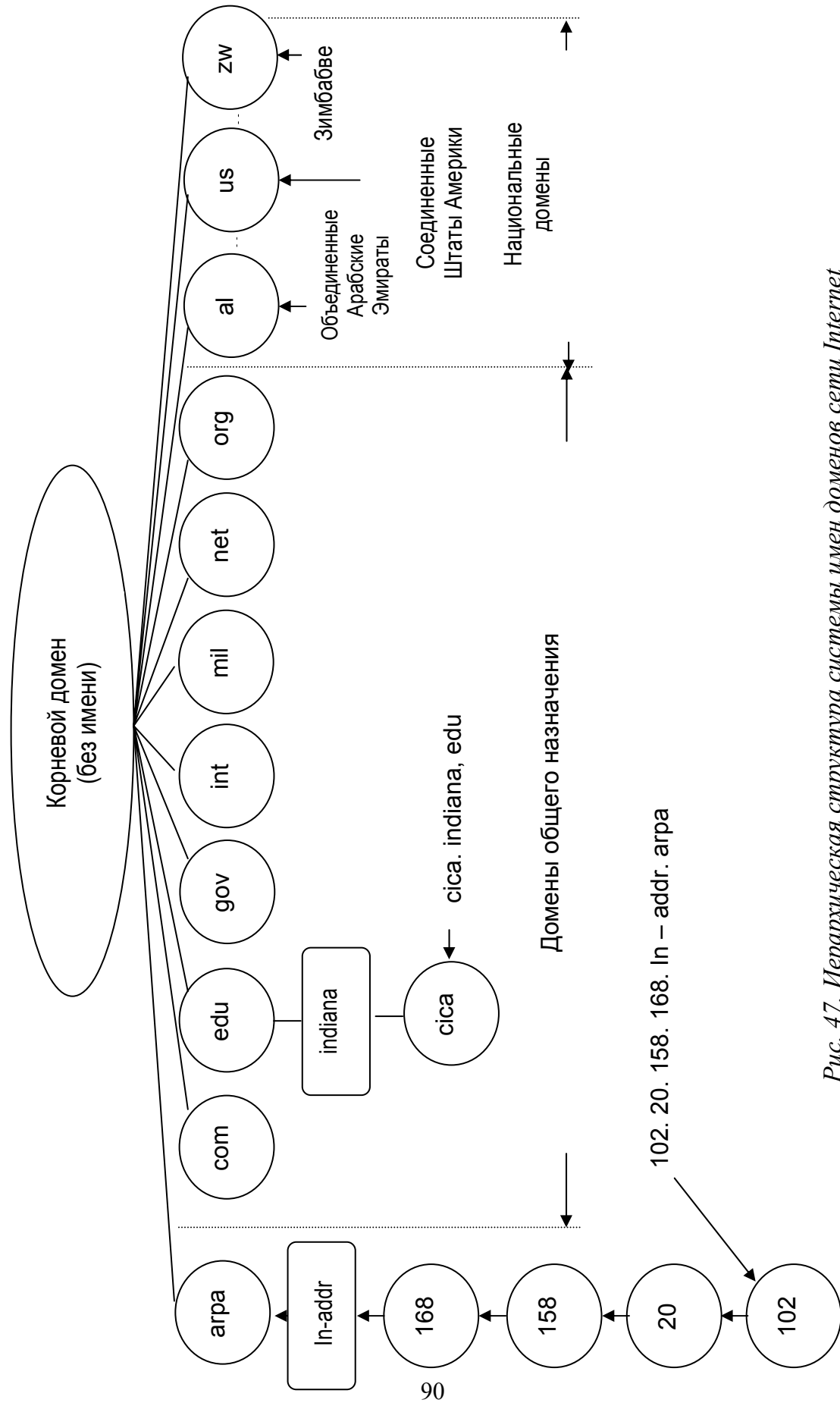


Рис. 47. Иерархическая структура системы имен доменов сети Internet

Список доменов второй группы

Домен	Назначение
com	Коммерческие организации
edu	Образовательные учреждения
gov	Правительственные учреждения США
int	Международные организации
mil	Военные организации США
net	Сеть, не относящаяся к вышеперечисленным категориям
org	Организации, не относящиеся к вышеперечисленным категориям

Общую координацию регистрации доменных имен выполняет Интернет-корпорация по распределению адресов и имен (The Internet Corporation for Assigned Names and Numbers, ICANN). ICANN передает полномочия по присвоению имен различным организациям. Каждая несет ответственность за некоторую ветвь общей DNS. *Ветвь в иерархии, за которую отвечает организация, называется зоной (zone)*. Другими словами, ICANN передает полномочия по назначению имен в определенных зонах (частях иерархии DNS) конкретным организациям. Организация, ответственная за зону DNS, может поделить ее на части и передать полномочия по присвоению имен дальше. Этот процесс продолжается до тех пор, пока одно ответственное лицо не сможет полностью управлять назначением имен в пределах одной четко ограниченной зоны. Это лицо является администратором DNS. Администратор управляет сервером DNS, обслуживающим его или зону.

Проблема преобразования адресов решается путем создания *сервера DNS (сервера имен)*. *Сервер DNS – это программа, преобразующая имена доменов в IP-адреса*. Этот сервер работает на тысячах компьютеров в Internet. Когда программе нужно соединиться с удаленным компьютером, первым делом она соединяется с сервером DNS и просит его найти IP-адрес по известному имени. *Запрос к серверу имен обычно состоит из структуры данных, включающих имя хоста (сетевое имя компьютера), адрес в формате «десятичное с точкой» и 32-разрядный двоичный адрес*.

Система имен доменов является распределенной базой данных: данные о конкретных компьютерах находятся на различных серверах DNS. Общаясь друг с другом, сервер с сервером, любой сервер DNS может преобразовать любой сетевой адрес в Internet. На рис. 48 показана схема работы серверов DNS в Internet.

Корневой сервер (root) знает, какой из серверов может преобразовать адреса каждого из доменов верхнего уровня. Серверы следующего уровня знают о серверах подчиненных им уровней и т. д. DNS используется моделью «клиент-сервер». Программа-клиент в этом случае называется «преобразователь» (resolver). Прикладная программа, желающая преобразовать имя компьютера в его адрес, обращается (через преобразователь) к серверу DNS с запросом. Преобразователь имен должен связаться с корневым сервером DNS и передать ему запрос на преобразование имени в IP-адрес. Корневой сервер, в свою очередь, должен определить, к какому из подчиненных серверов он должен обращаться, т. е. к какому домену принадлежит имя компьютера, указанное в запросе. Сервер DNS второго уровня делает то же самое, и это продолжается до тех пор, пока запрос не достигнет зоны, в которой будет искомая информация. В конце концов выполняемый запрос возвратится обратно к вызывавшей программе и IP-адрес будет найден.

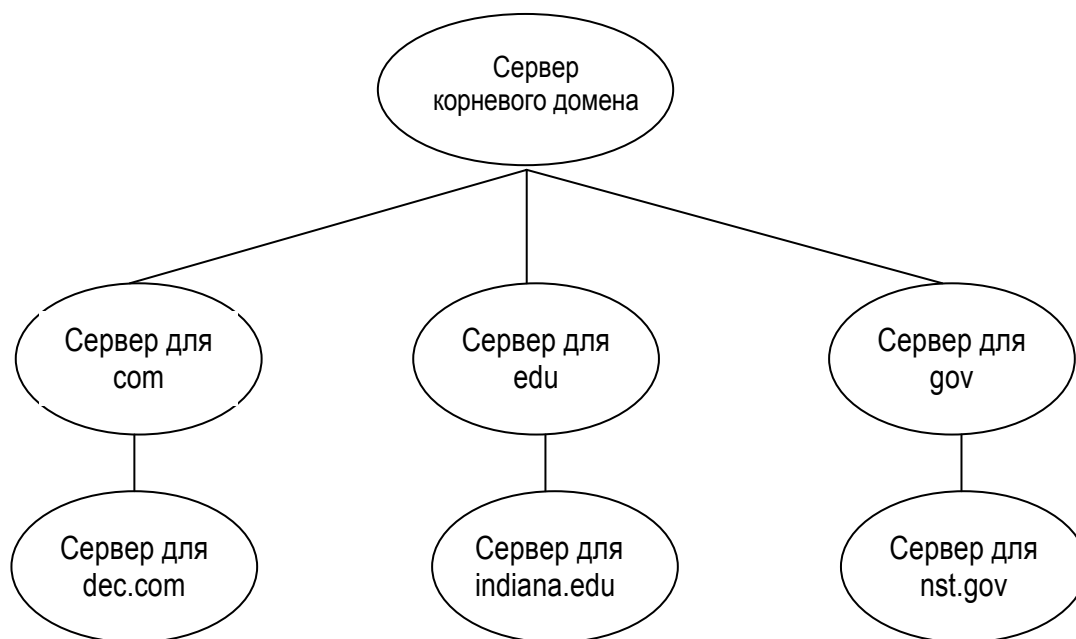


Рис. 48. Взаимосвязь между серверами DNS в сети Internet

32-битный IP-адрес означает номер сети и сетевого компьютера. Так как сеть Internet состоит из тысяч взаимосвязанных сетей, информационный центр сети Internet (ICANN) следит за тем, чтобы номер каждой входящей в Internet сети нигде больше не повторялся. При этом разработчики Internet договорились, что старший байт IP-адреса будет идентифицировать сеть, а младшие три байта – номер компьютера (интерфейса), входящего в эту сеть. Поле адреса, заполненное единицами, обозначает адрес «для всех», т. е. широковещательный (broadcast) адрес,

предназначенный для всех компьютеров в данной сети. *Поле адреса, заполненное одними нулями*, рассматривается как «этот» и означает «этот компьютер», находящийся в этой же сети. Эти специальные форматы поля IP-адресов не могут присваиваться компьютерам сети Internet и служат только для специального использования.

Сети Internet делятся на несколько классов. Старшие биты старшего байта IP-адреса определяют класс адреса в сети Internet. *Класс IP-адреса означает, сколько байтов в адресе служат для идентификации сети*. Система классификации адресов (сетей) приведена в табл. 5.

Таблица 5

Классификация адресов сети Internet

Класс	Старшие биты	Свободные для нумерации сети байты
A	0 ····	1
B	1 0 ···	2
C	1 1 0 ··	3
D	1 1 1 0 ·	Для широковещания
E	1 1 1 1 0	Зарезервировано на будущее

Сети класса A. Биты этого класса и номера сети занимают один байт, оставляя три для нумерации принадлежащих сети компьютеров:



Сеть класса A

Принадлежность классу A определена одним старшим битом, поэтому для нумерации сетей класса A остается семь бит. Это значит, что максимальное количество сетей класса A в Internet составляет 127 (а не 128, так как значение «все нули» зарезервировано). Поскольку сети класса A содержат 24 бита для нумерации компьютеров, теоретически адресное пространство позволяет адресовать 16 777 216 из них. Реально адреса класса A используются тем меньшим количеством сетей, в состав которых входит более 65 536 компьютеров.

Сети класса B. Сети класса B используют два байта для класса и номера сети, остальные 16 битов доступны для нумерации компьютеров.



Сеть класса B

Два старших байта за вычетом двух битов, определяющих класс, т. е. 14 битов, задают адресное пространство сети класса В. Таким образом, теоретически в Internet могут входить 16 384 сети класса В. Шестнадцать доступных для номера компьютера битов теоретически позволяют адресовать 65 536 сетевых компьютеров. Для сетей с большим количеством компьютеров требуется выделять сеть класса А. Сеть класса В выделяется, если количество компьютеров на ней превышает 256 штук.

Сети класса С. У сети класса С поля класса и номера сети уместятся в три байта. Таким образом, для нумерации компьютеров остается только 8 битов.



Сеть класса С

После вычитания трех битов класса сети для ее нумерации остается 21 бит. В результате, в Internet теоретически может входить до 2 097 152 сетей класса С. Поскольку максимальное количество компьютеров в сети класса С не может превышать 256, этот класс предназначен для небольших сетей.

Сети классов D и E. Класс D предназначается для групповой передачи. Адрес групповой передачи представляет группу компьютеров в Internet и используется, чтобы передать сообщение более чем одному компьютеру. ICANN зарезервировал адреса класса E для использования в будущем. Это будет широковещательная (broadcasting) или групповая передача (multicasting).

Распределением IP-адресов занимается информационный центр Internet (ICANN). Он следит, чтобы адреса не выдавались повторно. При этом номера сетей присваиваются администрацией ICANN, а номера компьютеров в сетях – непосредственно сетевыми администраторами. Такая схема обладает значительной гибкостью. Адресное пространство, отведенное отдельной сети, используется наиболее удобным для администратора образом. В целях увеличения эффективности одна сеть может разделяться на несколько подсетей путем деления адресного пространства. Например, сеть класса В. Администратору такой сети отведено 16 битов для нумерации компьютеров. 16 битов – это два байта, один из которых можно использовать для нумерации подсетей, а второй – для нумерации компьютеров. Таким образом, сеть класса В разделяется сетевым администратором на несколько подсетей меньшего размера.

Теоретически сетевой администратор может разделить сеть на 256 подсетей, к каждой из которых могут подключаться 256 компьютеров.

Такая схема позволит вместо одной большой физической сети иметь множество сетей меньшего размера. На самом деле любой внешний по отношению к этой сети компьютер будет передавать данные по определенному адресу формата Internet, т. е. концепция деления на подсети работает только внутри самой сети.

Реализация IP-протокола. IP-протокол реализует датаграммный способ передачи данных. Он формирует (инкапсулирует) IP-датаграмму, которая состоит из IP-заголовка и данных. Размер IP-заголовка всегда кратен 32-битному слову, даже если для этого он должен дополниться до нужной величины. Он содержит всю необходимую для доставки инкапсулированных данных по сети информацию и равен 20 байтам. На рис. 49 приведен формат IP-датаграммы. Она включает в себя следующие разделы.

0		15	16	31
Версия (VERS) 4 бита	Длина заголовка (HLEN) 4 бита	Тип службы (TOS) 8 бит		Общая длина пакета в байтах 16 бит
Идентификатор фрагмента 16 бит			Флаги 3 бита	Смещение фрагмента 13 бит
Время существования (TTL) 8 бит		Протокол 8 бит		Контрольная сумма заголовка 16 бит
IP-адрес источника 32 бита				
IP-адрес получателя 32 бита				
Опции (если есть)		Заполнение (при необходимости)		
Данные				

Рис. 49. Формат датаграммы IPv4

Номер версии (VERS). Протокол Internet все время развивается. Первые четыре бита в IP-заголовке (поле «номер версии») обозначают версию протокола Internet, который создал данную датаграмму. Когда формат данных протокола Internet меняется, номер его версии в датаграмме увеличивается, позволяя другим модулям IP отбрасывать датаграммы, обработать которые они не в состоянии из-за устаревшего формата данных. Модуль IP, принявший IP-датаграмму версии, которую он не способен обработать, может сообщить об этом источнику. В настоящее время применяется IP-протокол V.4 (версия 4).

Длина заголовка (HLEN). Следующие четыре бита IP-заголовка (поле «длина заголовка») задают длину заголовка в 32-битных словах. Данное поле обычно содержит число 5 (пять 32-битных слов равны 20 байтам). В двоичном виде это поле равно 0101.

Тип службы (TOS). Перед разработчиком программ встает вопрос, что выгоднее: увеличение производительности или уменьшение используемой памяти? Этот выбор определяют следующие восемь битов в IP-заголовке (поле «тип службы») определяют приоритет IP-пакета. Сетевой уровень TCP/IP управляет доставкой данных при помощи протокола Internet. Биты поля «тип службы» в IP-заголовке позволяют сетевому уровню принять обоснованное решение по поводу передачи пакетов, основываясь на их, возможно различных, приоритетах. Поле «тип службы» имеет следующую структуру:

0–2	3	4	5	6	7
Приоритет	Задержка	Производительность	Надежность	Стоимость	Не используется

Первые три бита поля «тип службы» образуют подраздел «приоритет». Подраздел «приоритет» может принимать значения от нуля до семи (от 000 до 111) и обозначает уровень важности переносимых данных.

Следующие четыре подраздела поля «тип службы» также определяют приоритеты, которые игнорируются большинством маршрутизаторов и сетевых компьютеров. Эти четыре подраздела определяют приоритеты, зависящие от конкретного приложения. Например, подраздел «задержка» (delay) говорит о том, что задержку в распространении пакета желательно сделать минимальной. Подраздел «пропускная способность» (through put) позволяет увеличить полосу пропускания до максимально возможной величины. Установленный в единицу бит «надежность» (reliability) позволяет сделать доставку пакета максимально надежной. Установка бита «стоимость» (cost) требует минимизировать затраты на доставку данного пакета.

Следующее поле IP-заголовка – поле «длина пакета». Оно имеет длину в шестнадцать битов и задает длину IP-пакета, включая сам заголовок. Стандарт предписывает считать длину пакета в байтах, а не в 32-разрядных словах, как в поле «длина заголовка». Данные из этих двух полей позволяют найти начало и конец инкапсулированных данных, а также подсчитать их длину. Для поля «длина пакета» отведено 16 битов, а это значит, что максимальная длина пакета равна 65 535 байтам.

Наличие поля идентификации в IP-заголовке обусловлено часто случающейся фрагментацией пакетов в Internet. Сетевые компьютеры используют поле идентификации с целью однозначно идентифициро-

вать каждый посланный ими пакет данных. Когда сетевой компьютер получает пакет, он определяет, к какой датаграмме относится определенный фрагмент при помощи поля идентификации.

Важную роль в передаче данных по протоколу IP играет фрагментация. Некоторые сетевые технологии, например Ethernet, имеют ограничение на максимальную длину передаваемого блока данных, называемого блок данных максимальной длины, или MTU. MTU определяет максимальную длину блока данных, которую данная сетевая среда в состоянии перенести. Если блок данных имеет бóльшую длину, он автоматически разбивается на части меньшей длины, каждая из которых передается затем по отдельности.

Фрагментация – это процесс разбиения отдельного пакета данных на некоторое количество пакетов меньшего размера. Фрагментация происходит в случае, если длина пакета превосходит MTU физического или сетевого уровня. Она также происходит, когда пакет попадает в маршрутизатор с MTU меньшим, чем MTU локальной сети источника.

Для управления фрагментацией протокол IP использует первый и последний биты в трех битовом поле флагов. Первый бит называется «фрагментация запрещена» и устанавливается сетевым программным обеспечением для тестирования и отладки. Кроме того, существуют некоторые приложения, данные которых нельзя фрагментировать. Включая режим «фрагментация запрещена», т. е. устанавливая соответствующий бит, следует иметь в виду, что, если модуль IP обнаружит, что фрагментация должна произойти, протокол TCP/IP отбросит IP-пакет и вернет сообщение об ошибке источнику пакета.

Последний бит поля флагов называется «фрагмент-продолжение». В процессе фрагментации пакета протокол IP устанавливает этот бит в единицу во всех фрагментах, кроме последнего. В последнем фрагменте данных бит равен нулю.

Для повышения эффективности и производительности протокол IP пытается послать пакет наибольшего допустимого размера. Иногда фрагментации не избежать. До начала фрагментации протокол IP рассчитывает точку деления (breaking point), равную значению MTU нижележащего уровня сети. Точка деления – это расположение байта в пакете, на котором произойдет разделение.

Точка деления представляет собой смещение или расстояние от начала датаграммы. Каждая точка деления записывается протоколом IP в поле «смещение фрагмента» заголовка только что собранной IP-датаграммы. Таким образом, IP-заголовок каждой датаграммы содержит смещение данного фрагмента относительно начала данных. Значение точки деления используется протоколом IP на другом конце соединения, чтобы правильно собрать фрагментированный пакет.

Время существования (Time-to-Live, TTL). Восьмибитовое поле «время существования» задает срок существования пакета в сети. Протокол ТСП/IP предписывает каждому маршрутизатору на пути между отправителем и получателем уменьшить значение поля «время существования пакета». Каждый маршрутизатор должен контролировать время появления IP-пакета. Отправляя пакет дальше, маршрутизатор уменьшает поле «время существования» на количество секунд, которое пакет ждал в буфере, если пакет был задержан.

Если поле «время существования» становится равным нулю до того, как пакет достигнет места назначения, протокол ТСП/IP уничтожит его и предупредит компьютер-источник пакета об этом событии, пользуясь протоколом управляющих сообщений Internet ICMP.

Протокол. Транспортный уровень ТСП/IP имеет два протокола: протокол управления транспортировкой ТСП и протокол пользовательских датаграмм UDP. Эти протоколы используют протокол IP для доставки данных. Восьмибитовое поле «протокол» в IP-заголовке указывает на протокол-источник данных, инкапсулированных в IP-датаграмму. Например, если значением поля «протокол» является шесть (двоичное 00000110), это значит, что данные сформированы из сегмента ТСП. Значение 17 (двоичное 00010001) означает, что данные принадлежат UDP-датаграмме.

Сетевой уровень пользуется значением в поле «протокол» при передаче данных на транспортный уровень. Значение поля указывает на определенный модуль транспортного уровня, которому принадлежат данные IP-пакета.

Контрольная сумма заголовка. Необходима, т. к. протокол IP является ненадежным протоколом. Поле контрольной суммы в IP-заголовке содержит шестнадцатибитное число, являющееся контрольной суммой только для IP-заголовка. Данные пакета в формировании контрольной суммы участия не принимают. Проверка целостности данных IP-датаграммы возлагается на протоколы более высоких уровней, тех, что создали данные для IP-датаграммы.

Для подсчета контрольной суммы IP-заголовков трактуется как последовательность шестнадцатибитных чисел. В поле контрольной суммы помещается результат дополнения до единицы суммы всех чисел, составляющих заголовки. Поле контрольной суммы при подсчете принимается равным нулю, т. е. компьютер игнорирует значение поля при всех подсчетах контрольной суммы заголовка.

Компьютер, принявший датаграмму, подсчитывает новую контрольную сумму, в том числе и с полем старой контрольной суммы, вычисленной ранее при передаче. Если заголовок не изменится, т. е. его

повреждения не произошло, новая контрольная сумма должна быть «все единицы». Если это не так, т. е. произошла ошибка при передаче, протокол TCP/IP отбрасывает датаграмму. При этом никакого сообщения компьютеру-источнику датаграммы не передается.

Протокол IP-ненадежный протокол. Он не гарантирует доставки данных. Но проверка контрольной суммы заголовка пакета гарантирует, что, если данные дойдут до узла назначения, они дойдут в неизменном виде, иначе модуль IP распознает и отбросит ошибочный пакет. Протокол TCP/IP не требует от модуля IP выдавать какое-либо сообщение о появлении поврежденного пакета. Надежные протоколы, к каковым относится TCP, никогда не полагаются на способность IP выдавать такие сообщения. Вместо этого они используют собственные механизмы.

IP-адрес источника и получателя. 32-битное поле «адрес источника» содержит IP-адрес компьютера – отправителя данных (вернее адрес его сетевого интерфейса). Это поле никогда не изменяется, сколько бы маршрутизаторов ни находилось на пути следования пакета. Поле «адрес источника» всегда содержит адрес первоначального отправителя пакета. Так же, как и адрес источника, адрес получателя является стандартным 32-битным IP-адресом пункта назначения пакета. Он может быть либо индивидуальным, либо состоять из единиц в случае широковещательной передачи.

Для доставки данных в сети Internet используются таблицы IP-маршрутизации. Они представляют собой специальные таблицы, в которых хранятся адреса получателей отправленных датаграмм. При этом программное обеспечение узлов маршрутизации определяет маршруты передаваемых датаграмм с учетом загрузки каналов связи. Назначение таблиц маршрутизации достаточно подробно изложено в разделе 1.

Особенностями таблиц IP-маршрутизации является то, что в них хранятся только номера сетей, а не компьютеров. При этом таблицы IP-маршрутизации основывают свою работу на том факте, что все хосты на одной и той же сети имеют один и тот же сетевой номер.

Каждая запись в таблице маршрутизации состоит из трех следующих полей: сети (network), шлюза (gateway) и флагов (flags). Первые два – это сетевые номера, а поле флагов указывает на то, что эти сети напрямую соединены с сетью, которой принадлежит данная таблица. Поле «сеть» содержит список сетевых идентификаторов. Поле «шлюз» содержит информацию о маршрутизаторе. Это поле указывает маршрутизатор, служащий передатчиком пакетов в сеть, идентификатор которой указан в поле «сеть». Однако это не значит, что маршрутизатор напрямую связан с этой сетью назначения. В таблице указан маршрутизатор, который служит следующим этапом при движении пакета к месту назначения.

Доставка IP-датаграммы делится на непосредственную и промежуточную. При непосредственной передаче, когда компьютер получает пакет, его IP-протокол исследует идентификатор сети назначения, размещенный в заголовке пакета. Затем IP-протокол запрашивает запись для сети с этим идентификатором у таблицы маршрутизации. Если запись найдена, исследуется содержимое поле флагов. Если в поле флагов указано прямое соединение, это значит, что пакет можно доставить, используя формат кадра данных низлежащего уровня соединения (например, в сетях технологии Ethernet или Token Ring). Далее процесс доставки будет непосредственно зависеть от применяемой сетевой технологии.

Таким образом, непосредственная доставка значит, что сеть может преобразовывать адрес IP-получателя в адрес формата канального уровня (например, адрес сети Ethernet). Сеть инкапсулирует IP-датаграмму в кадр данных и передает непосредственно пункту назначения.

В случае промежуточной доставки запись в таблице маршрутизации говорит о том, что устройство с данным адресом не соединено напрямую с сетью, в которую нужно передать пакет. Значит, необходимо осуществить процесс промежуточной доставки. Таблица маршрутизации определенной сети содержит данные только о маршрутизаторах, связанных с ней напрямую. Это значит, что сеть может передать пакет данных, пользуясь непосредственной доставкой, любому из них. А затем промежуточный маршрутизатор передает этот пакет следующему маршрутизатору и так далее до тех пор, пока не будет достигнут адрес назначения.

Опции. Восемьбитное поле опций позволяет тестировать и отлаживать разнообразные сетевые приложения. Опции управляют фрагментацией и маршрутизацией сетевых пакетов.

В настоящее время разработана новая версия протокола IPv6, призванная решить проблемы, с которыми столкнулась предыдущая версия IPv4. В новой версии IPv6 используется длина адреса 128 бит вместо 32, как в IPv4.

Протокол IPv6 уже используется в нескольких сотнях сетей по всему миру (более 3000 сетей на июль 2010 года), но пока еще не получил столь широкого распространения в Интернете, как IPv4. В России используется почти исключительно в тестовом режиме некоторыми операторами связи, а также регистраторами доменов для работы DNS-серверов.

По прогнозам, после того, как адресное пространство в IPv4 закончится (предположительно 2011–2012 гг.), два стека протоколов – IPv6 и IPv4 – будут использоваться параллельно с постепенным увеличением доли трафика IPv6 по сравнению с IPv4. Такая ситуация станет возмож-

ной из-за наличия огромного количества устройств, в том числе устаревших, не поддерживающих IPv6 и требующих специального преобразования для работы с устройствами, использующими только IPv6.

Следует отметить, что из IPv6 убраны вещи, усложняющие работу маршрутизаторов:

- Маршрутизаторы больше не разбивают пакет на части (возможно разбиение пакета с передающей стороны). Для лучшей работы протоколов, требовательных к потерям, минимальный размер пакета поднят до 1280 байтов. Информация о разбиении пакетов вынесена из основного заголовка в расширение.

- *Исчезла контрольная сумма.* С учетом того, что канальные (Ethernet) и транспортные (TCP) протоколы тоже проверяют корректность пакета, контрольная сумма на уровне IP воспринимается как излишняя. Тем более каждый роутер *уменьшает время существования (TTL)* на единицу, что в IPv4 приводило к пересчету суммы.

Несмотря на огромный размер адреса IPv6, благодаря этим улучшениям заголовок пакета удлинился всего лишь вдвое: с 20 до 40 байт.

На рис. 50 приведен формат датаграммы IPv6. Она включает в себя следующие разделы.

Версия протокола (Version). 4-битный код номера версии Internet протокола (версия Internet протокола для IPv6 = 6).

0	4	11	16	24	31
Версия (Version) 4 бита	Приоритет (Traffic Class) 8 бит	Метка потока (Flow Label) 20 бит			
Размер поля данных (Payload Length) 16 бит			Следующий заголовок (Next Header) 8 бит	Предельное число шагов (Hop Limit) 8 бит	
IP-адрес источника (Source Address) 128 бит					
IP-адрес получателя (Destination Address) 128 бит					
Опции (если есть)			Заполнение (при необходимости)		
Данные					

Рис. 50. Формат датаграммы IPv6

Приоритет (Traffic Class). 8-битный код приоритета пакета. Приоритизация пакетов обеспечивается маршрутизаторами на основе первых шести бит поля. Первые три бита определяют класс трафика, оставшиеся биты определяют приоритет удаления. Чем больше значение приоритета, тем выше приоритет пакета. Разработчики IPv6 рекомендуют использовать для определенных категорий приложений следующие коды класса трафика (табл. 6).

Таблица 6

Коды класса трафика

Класс трафика	Назначение
0	Нехарактеризованный трафик
1	Заполняющий трафик (сетевые новости)
2	Несущественный информационный трафик (электронная почта)
3	Резерв
4	Существенный трафик (FTP, HTTP, NFS)
5	Резерв
6	Интерактивный трафик (Telnet, X-terminal, SSH)
7	Управляющий трафик (Маршрутная информация, SNMP)

Метка потока (Flow Label). 20-битный код метки потока (для мультимедиа). Введение в протоколе IPv6 поля «метка потока» позволяет значительно упростить процедуру маршрутизации однородного потока пакетов. Поток – это последовательность пакетов, посылаемых отправителем определенному адресату. При этом предполагается, что все пакеты данного потока должны быть подвергнуты определенной обработке. Характер данной обработки задается дополнительными заголовками. Допускается существование нескольких потоков между отправителем и получателем. Метка потока присваивается узлом-отправителем путем генерации псевдослучайного 20-битного числа. Все пакеты одного потока должны иметь одинаковые заголовки, обрабатываемые маршрутизатором.

При получении первого пакета с меткой потока маршрутизатор анализирует дополнительные заголовки, выполняет предписанные этими заголовками функции и запоминает результаты обработки (адрес следующего узла, опции заголовка переходов, перемещение адресов в заголовке маршрутизации и т. д.) в локальном кэше. Ключом для такой записи является комбинация адреса источника и метки потока. Последующие пакеты с той же комбинацией адреса источника и метки потока обрабатываются с учетом информации кэша без детального анализа всех полей заголовка.

Время жизни записи в кэше составляет не более 6 секунд, даже если пакеты этого потока продолжают поступать.

При обнулении записи в кэше и получении следующего пакета потока пакет обрабатывается в обычном режиме и для него происходит новое формирование записи в кэше. Следует отметить, что указанное время жизни потока может быть явно определено узлом-отправителем с помощью протокола управления или опций заголовка переходов и может превышать 6 секунд.

Размер поля данных (Payload Length). 16-битовое число без знака. Несет в себе код длины поля данных в октетах, которое следует сразу после заголовка пакета. Если код равен нулю, то длина поля данных записана в зоне опций.

Следующий заголовок (Next Header). 8-битовый разделитель. Идентифицирует тип заголовка, который следует непосредственно за IPv6-заголовком.

Предельное число шагов (Hop Limit). 8-битовое целое число без знака. Уменьшается на 1 в каждом узле, через который проходит пакет. При предельном числе шагов, равном нулю, пакет удаляется.

Адрес отправителя (Source Address). 128-битовый адрес отправителя пакета.

Адрес получателя (Destination Address). 128-битовый адрес получателя пакета (возможно, не конечный получатель, если присутствует маршрутный заголовок).

В IPv6 существует три типа адресов: *unicast*, *anycast* и *multicast*.

Unicast. Идентификатор одиночного интерфейса. Пакет, посланный по уникастному адресу, доставляется интерфейсу, указанному в адресе.

Anycast. Идентификатор набора интерфейсов (принадлежащих разным узлам). Пакет, посланный по эникастному адресу, доставляется одному из интерфейсов, указанному в адресе (ближайший, в соответствии с мерой, определенной протоколом маршрутизации).

Multicast. Идентификатор набора интерфейсов (обычно принадлежащих разным узлам). Пакет, посланный по мультикастинг-адресу, доставляется всем интерфейсам, заданным этим адресом.

4.3.4. Транспортный уровень сети Internet

Семейство протоколов TSP/IP включает в себя два транспортных протокола: протокол пользовательских датаграмм UDP и протокол управления транспортировкой TSP. Протокол пользовательских датаграмм ненадежен, не ориентирован на соединение, передает и принимает данные в виде датаграмм. Протокол управления транспортировкой

использует надежный поточно-битовый способ доставки данных, когда сетевое соединение устанавливается в виде виртуальной цепи.

Транспортному уровню соответствует понятие «порт», которое обозначает тип приложения (тип прикладной программы), в отличие от IP-адреса, который обозначает определенный компьютер.

Транспортный уровень перемещает пакеты данных между прикладными программами. При этом он должен распознавать эти программы. Для этого служат номера портов. Любое приложение имеет уникальный номер порта. Когда программа устанавливает соединение с сетью, ей присваивается определенный номер порта.

Протокол пользовательских датаграмм UDP. Этот протокол переносит данные между приложениями, имеющими определенный номер порта. UDP присоединяет к датаграммам пользователей UDP-заголовки, структура которого приведена на рис. 51. UDP-заголовок содержит: «порт-источник», «порт-получатель», «длина сообщения» и «контрольная сумма».

Длина UDP-заголовка – 8 байт.

0	15	16	31
Порт-получатель UDP		Порт-источник UDP	
Длина сообщения UDP		Контрольная сумма UDP	
Область данных UDP			

Рис. 51. Структура UDP-датаграммы

Поля портов состоят из 16-битных целых чисел, представляющих номера портов приложений. Поле «порт источника» содержит номер порта, которым пользуется приложение-источник данных. Поле «порт-получатель» соответственно указывает на номер порта приложения – получателя данных. Поле «длина сообщения» определяет длину (в байтах) UDP-датаграммы, включая UDP-заголовок. Поле «контрольная сумма», в отличие от контрольной суммы IP-заголовка, содержит результат суммирования всей UDP-датаграммы, включая ее данные, область которых начинается сразу после заголовка. Модуль UDP отслеживает появление вновь прибывших датаграмм, сортирует их и распределяет (демультиплексирует) в соответствии с портами назначения.

Протокол транспортного уровня TCP. Транспортный протокол (Transport Control Protocol) TCP служит для передачи данных между сетевыми и прикладными уровнями сетевой модели. Для обеспечения надежной доставки и правильной последовательности данных в общем потоке протокол TCP использует подтверждения. Каждый раз при передаче сообщения модуль TCP запускает таймер. По истечении заданного в нем времени при неполучении подтверждения протокол TCP повторяет попытку передать свое сообщение.

Модуль ТСР не посылает один пакет, ожидая прихода подтверждения, чтобы послать следующий. Вместо этого он использует «принцип скользящего окна». Этот принцип позволяет послать несколько сообщений и только потом ожидать подтверждения. Модуль ТСР регулирует полосу пропускания сети, договариваясь с удаленным узлом о параметрах потока данных. При этом процесс регулировки происходит на протяжении всего соединения ТСР. Регулировка заключается в изменении размеров скользящего окна. При низкой загрузке сети размер скользящего окна увеличивается. При этом скорость выдачи данных на канале связи увеличивается. Если загрузка сети достаточна велика, модуль ТСР уменьшает размер скользящего окна.

Блок данных ТСР принято называть сообщением или сегментом. Сегмент ТСР состоит из ТСР-заголовка, ТСР-опций и данных. На рис. 52 приведена структура сегмента ТСР.

0		15		16		31	
Порт-передатчик (16 битов)				Порт-приемник (16 битов)			
32-битный номер последовательности							
32-битный номер подтверждения							
Длина заголовка (4 бита)		Зарезервировано (6 битов)		Флаги (6 битов)		Размер окна (16 битов)	
Контрольная сумма ТСР (16 битов)				Указатель на данные для неотложной обработки (16 битов)			
Опции (если есть)						Заполнение (при необходимости)	
Данные							

Рис. 52. Структура сегмента ТСР

Порт источника и порт получателя. 16-битные поля источника и получателя однозначно определяют посылающие и принимающие данные приложения или прикладные протоколы (программы). Номера портов источника и получателя в совокупности с IP-адресами сетевых компьютеров (в IP-заголовке) однозначно идентифицируют любое ТСР-соединение. Каждая из сторон ТСР-соединения называется сокетом (Socket).

Номер последовательности. 32-битное поле номера последовательности обозначает первый байт данных из области данных сегмента ТСР. Оно соответствует смещению этого байта относительно начала потока данных. Каждый байт в потоке данных может быть идентифицирован при помощи номера последовательности.

Номер подтверждения. 32-битное поле номера подтверждения обозначает байт данных, который принимающая сторона рассчитывает получить следующим в потоке данных. Например, если последний принятый байт имел номер 500, модуль TCP установит номер подтверждения равным 501.

Длина заголовка. Как и в заголовке IP, поле длины заголовка TCP состоит из четырех битов, обозначающих длину заголовка, измеренную в 32-битных словах. Как и заголовок IP, заголовок TCP имеет длину в 20 байт.

Флаги. Заголовок TCP содержит шесть однобитных полей флагов. Флаг UR сообщает принимающему модулю TCP о наличии данных, требующих немедленной обработки; флаг ACK подтверждает правильность номера подтверждения в заголовке TCP; флаг PSN требует от принимающего модуля немедленно передать принятый сегмент данных приложению-получателю; флаг RST запрашивает у принимающего модуля TCP сброс соединения (прекращения работы приложений); флаг SYN указывает принимающему модулю TCP необходимость синхронизации последовательности; флаг FIN сообщает принимающему модулю TCP о том, что источник закончил передачу данных.

Размер окна. 16-битное поле «размер окна» сообщает принимающему модулю TCP количество байтов, которое собирается принять передатчик. Значение данного поля определяет размер скользящего окна. Как правило, оно равняется нескольким тысячам байтов.

Контрольная сумма TCP. 16-битное поле контрольной суммы TCP содержит сумму, вычисленную по всему сегменту TCP, включая данные. Протокол TCP требует от передатчика, чтобы он включил вычисленную контрольную сумму в поле, а от приемника, чтобы он вычислил ее повторно и сравнил с принятой.

Указатель на данные для неотложной обработки. 16-битное поле указателя определяет положение байта данных в области данных сегмента TCP. Указатель и флаг неотложных данных извещают принимающий модуль TCP о том, что некоторые данные, требующие немедленной обработки, находятся в сегменте и указывают модулю на них.

Опции. Так же как и у протокола IP, заголовок TCP содержит необязательное поле «опции» (options). В ходе установления соединения модули TCP договариваются о максимальной длине сегмента (MSS) и устанавливают соответствующую опцию.

Для обмена данными протокол TCP должен установить соединение. Для установления и прекращения соединения, а также отправки и получения подтверждений TCP заголовок имеет поля «номер последовательности», «номер подтверждения» и поле флагов. Для передачи

сегмента программа-приложение запрашивает модуль TCP для установления соединения. Модуль TCP в свою очередь шлет сообщение TCP с установленным флагом SYN (синхронизации) удаленному порту.

Флаг синхронизации указывает принимающей стороне, что программа-клиент желает установить соединение. Вместе с флагом SYN сегмент TCP несет в себе 32-битный номер последовательности, размещенный в поле «номер последовательности». TCP-модуль удаленного клиента отвечает сегментом TCP с установленным флагом подтверждения ACK и номером подтверждения.

Номер последовательности в общем случае может выбираться произвольным образом. Нумерация данных в потоке передаваемых данных начинается с этого номера. Приемник, получив запрос на установление соединения, посылает обратное сообщение, содержащее его собственный начальный номер.

Все TCP-соединения являются дуплексными. Данные следуют в обоих направлениях одновременно. Поток данных в одном направлении совершенно не зависит от потока данных в противоположном.

Соединение TCP заканчивается обменом пакетами, состоящими из двух стадий. Каждая из взаимодействующих сторон может предложить другой стороне закончить соединение. Для этого сторона – инициатор обмена высылает пакет с установленным флагом «окончание обмена» FIN. В силу дуплексной природы протокола TCP оба потока данных независимы и должны быть завершены по отдельности.

4.3.5. Прикладной уровень сети Internet. Сервисы Internet

В глобальной сети Internet функционирует ряд сетевых протоколов прикладного уровня, которые позволяют абонентам сети получать удаленный доступ к информационным ресурсам, вести активный диалог с другими удаленными абонентами, отправлять и получать почту. *Перечень возможностей, получаемых абонентом при подключении к сети, принято называть основными сервисами Internet.* К их числу относятся нижеперечисленные.

Telnet. Обеспечивает удаленный доступ к серверам на базе ОС UNIX. С помощью программы-клиента Telnet можно войти в систему удаленного компьютера в качестве его терминала и осуществить исполнение команд ОС UNIX (например, соединиться с другим сервером, получить доступ к данным).

FTP. Передача файлов между соединенными посредством сети компьютерами. Этот сервис позволяет устанавливать логическую связь с удаленным узлом, осуществлять поиск необходимого файла в каталогах, выполнять прием и передачу файлов, создавать собственные файлы и каталоги и удалять их.

Поисковые системы (Google, WebCrawler) и тематические каталоги (Yahoo, InfoSeek, Lycos). Предназначены для поиска необходимой информации в сети Internet.

E-mail. Электронная почта, система пересылки сообщений между людьми, имеющими доступ к сети Internet. Для передачи почтовых сообщений используется протокол SMTP. Доставка почты пользователю из почтового ящика выполняется протоколом Post Office Protocol (POP). В системе реализованы такие функции, как: создать сообщение, доставить почту, переслать полученное письмо, уведомить о получении, уведомить о прочтении.

Internet News. Телеконференции по Internet. Это система организации публичных обсуждений по конкретным темам: вычислительная техника, социальные вопросы, новости и т. д. Для организации телеконференций существует список серверов телеконференций.

IRC. Телеконференции реального времени (чат-соединение). Чатом (Chat) называется общение между пользователями с помощью клавиатуры компьютера. При этом в чате могут участвовать одновременно несколько пользователей, подключенных к серверам, работающим в режиме многоканального чата.

HTTP. Доступ к гипертекстовым страницам WWW-серверов. Основными носителями информации в сети Internet являются мультимедийные WWW-сервера, на которых информация размещается в виде Web-страниц. Эти страницы отображают звук, изображение (рисунок, фотографию и т. д.) и гипертекст. Для доступа к WWW-серверам используются специальные программы (browser): Internet Explorer и Netscape Navigator.

Audio Conferencing (аудиоконференции). Этот сервис позволяет осуществлять с помощью компьютеров, оснащенных мультимедийными средствами, селекторную связь как внутри организаций, так и между ними.

RTVC. Видеоконференции реального времени. Видеоконференция – это взаимное общение двух или более лиц с использованием мультимедийных возможностей компьютеров по сети Internet. Компьютер, подключенный к сети, должен быть оснащен видеокамерой, микрофоном и аудиоколонками.

Методические указания

При изучении этого раздела, содержащего описание принципов построения глобальных сетей, необходимо усвоить следующее:

- глобальные компьютерные сети представляют собой объединение компьютерных сетей регионов, стран и материков;
- в качестве аппаратуры передачи данных по телефонным линиям связи в глобальных компьютерных сетях применяются модемы;

- существуют три основных способа модуляции двоичных цифровых сигналов: амплитудная, фазовая и частотная;
- передача данных с помощью модемов осуществляется в дуплексном (одновременно в двух направлениях) или полудуплексном (поочередно в одном направлении) режимах;
- в отличие от синхронного способа передачи данных, когда данные передаются одним потоком (байт за байтом), при асинхронном способе передачи каждый передаваемый байт предваряется стартовым битом и заканчивается одним или двумя стоповыми битами;
- для передачи данных по зашумленным телефонным линиям используются протоколы коррекции ошибок: от MNP1 до MNP10 и V.42;
- в глобальных компьютерных сетях используются два типа протоколов: X.25 и TCP/IP;
- в сетях X.25 на канальном уровне применяется протокол HDLC, обеспечивающий безошибочный прием-передачу данных между двумя соседними компьютерами либо узлами коммутации;
- протокол сетевого уровня сети X.25 передает пакеты с помощью постоянных виртуальных каналов связи или коммутируемых виртуальных соединений;
- для высокоскоростной передачи данных (от 64 Кбит/с до 1,544 Мбит/с) применяется технология Frame Relay (FR), которая представляет собой развитие сетей X.25 для качественных каналов связи;
- семейство протоколов TCP/IP, применяемых в сети Internet, включает в себя протоколы двух уровней: транспортного (TCP) и сетевого (IP);
- на канальном уровне в сети Internet применяется протокол PPP, в основе которого лежит протокол HDLC;
- в сети Internet один и тот же компьютер может иметь несколько IP-адресов;
- для символьного задания IP-адреса в сети Internet используется система имен доменов (DNS);
- в сети Internet существует три класса сетей: А – большие сети, содержащие сотни тысяч компьютеров; В – сети среднего размера, содержащие тысячи компьютеров; С – сети малого размера (локальные сети), содержащие до 256 компьютеров;
- IP-протокол, соответствующий сетевому уровню, реализует датаграммный способ передачи данных;
- в сети Internet используются две версии IP-протокола: IPv4 и IPv6;

- сообщение в сети Internet называется датаграммой, которая состоит из IP-заголовка и данных;
- IP-заголовок датаграммы содержит ее характеристики, включая время существования в сети Internet для IPv4 (его максимальное значение равно 255 с) или предельное число шагов для IPv6 (уменьшается на 1 в каждом узле, через который проходит датаграмма);
- транспортному уровню сети Internet соответствуют два протокола: протокол пользовательских датаграмм UDP и протокол управления транспортировкой TCP;
- блок данных протокола TCP называется сегментом и состоит из заголовка и данных;
- прикладному уровню сети Internet соответствуют несколько протоколов (Telnet, FTP, E-mail, Internet News, IRC, HTTP, Audio Conferencing, RTVC), которые принято называть сервисами Internet.

Глава 5

МОБИЛЬНЫЕ ТЕЛЕКОММУНИКАЦИИ

5.1. Введение в мобильные телекоммуникации

Первые беспроводные телефонные системы были созданы в 1970-е годы. Сначала это были аналоговые сети, в начале 1980-х появился стандарт GSM, ознаменовавший начало перехода на цифровые стандарты как обеспечивающие лучшее распределение спектра, лучшее качество сигнала и бóльшую безопасность. С 90-х годов XX века происходит укрепление позиций беспроводных сетей. Беспроводные технологии прочно входят в нашу жизнь. Быстро развиваясь, они стимулируют создание новых устройств и услуг.

Многообразие новых беспроводных технологий, таких как CDMA, (Code Division Multiple Access – технология с кодовым разделением каналов), GSM (Global for Mobile Communications – глобальная система для мобильных коммуникаций), TDMA (Time Division Multiple Access – множественный доступ с разделением во времени), 802.11, WAP (Wireless Application Protocol – протокол беспроводных технологий), 3G (третье поколение), GPRS (General Packet Radio Service – услуга пакетной передачи данных), Bluetooth, EDGE (Enhanced Data Rates for GSM Evolution – увеличенная скорость передачи данных для GSM), i-mode, говорит о том, что в этой области грядет революция.

Весьма перспективно развитие беспроводных локальных сетей WLAN и сети средних и коротких расстояний Bluetooth. Беспроводные сети развертываются в аэропортах, университетах, отелях, ресторанах, на предприятиях. Значительный импульс развитию беспроводных технологий дала Всемирная паутина и идея работы в Сети при помощи беспроводных устройств.

В конце 90-х годов пользователям была предложена WAP-услуга, не вызвавшая большого интереса. Это были основные информационные услуги – новости, погода, всевозможные расписания. Также вначале не пользовались спросом беспроводные сети WLAN и Bluetooth (в основном из-за высокой стоимости этих средств связи). К середине первого десятилетия XXI века счет пользователей беспроводного Internet-сервиса пошел на десятки миллионов.

С появлением беспроводной Internet-связи на первый план вышли вопросы обеспечения безопасности. Основные угрозы при использовании беспроводных сетей – это перехват сообщений спецслужб, коммер-

ческих предприятий и частных лиц, перехват номеров кредитных карточек, кража оплаченного времени соединения, вмешательство в работу коммуникационных центров. Перечисленные проблемы решаются по мере совершенствования стандартов связи.

В данном разделе содержатся материалы по беспроводным сетям WLAN, Bluetooth и GSM.

5.2. Беспроводная сеть WLAN

Wi-Fi – это современная беспроводная технология соединения компьютеров в локальную сеть и подключения их к Internet. Именно благодаря этой технологии Internet становится мобильным и дает пользователю свободу перемещения не только в пределах комнаты, но и по всему миру.

Под аббревиатурой «Wi-Fi» (от английского словосочетания «Wireless Fidelity», которое можно дословно перевести как «высокая точность беспроводной передачи данных») в настоящее время развивается целое семейство стандартов передачи цифровых потоков данных по радиоканалам.

С увеличением числа мобильных пользователей возникает острая необходимость в оперативном создании коммуникаций для обмена данными между ними. Поэтому естественным образом происходит интенсивное развитие технологий беспроводных коммуникаций. Особенно это актуально в отношении беспроводных локальных сетей, или так называемых WLAN-сетей (Wireless Local Area Network). Сети WLAN – это сети, в которых вместо обычных проводов используются радиоволны. Установка таких сетей рекомендуется там, где развертывание кабельной системы невозможно или экономически нецелесообразно. Особенно они эффективны на предприятиях, сотрудники которых активно перемещаются по территории во время рабочего дня с целью обслуживания клиентов или сбора информации (крупные склады, агентства, офисы продаж, учреждения здравоохранения и др.).

Благодаря функции роуминга между точками доступа пользователи могут перемещаться по территории покрытия сети Wi-Fi без разрыва соединения.

WLAN-сети имеют ряд преимуществ перед обычными кабельными сетями:

- WLAN-сеть можно быстро развернуть, что удобно при проведении презентаций или работе вне офиса;
- пользователи мобильных устройств при подключении к локальным беспроводным сетям могут легко перемещаться в рамках действующих зон сети;
- WLAN-сеть может оказаться единственным выходом, если невозможна прокладка кабеля для обычной сети.

Вместе с тем необходимо помнить об ограничениях беспроводных сетей. Это, как правило, меньшая скорость, подверженность влиянию помех и более сложная схема обеспечения безопасности при передаче информации.

Институт инженеров по электротехнике и электронике IEEE (Institute of Electrical and Electronics Engineers) сформировал в 1990 году группу по разработке стандарта 802.11 для беспроводных локальных сетей на базе радиоборудования с частотой 2,4 ГГц и скоростями передачи данных 1 и 2 Мбит/с. Работы по созданию стандарта были завершены через 7 лет, и в июне 1997 года была ратифицирована его первая спецификация. Стандарт IEEE 802.11 является стандартом для продуктов WLAN.

5.2.1. Физическая среда передачи данных

Для построения WLAN-сети используются Wi-Fi-адаптеры и точки доступа.

Адаптер (рис. 53) представляет собой устройство, которое подключается через слот расширения PCI, PCMCIA, CompactFlash. Существуют также адаптеры с подключением через порт USB 2.0. Wi-Fi-адаптер выполняет ту же функцию, что и сетевая карта в проводной сети. Он служит для подключения компьютера пользователя к беспроводной сети. Благодаря платформе Centrino все современные ноутбуки имеют встроенные адаптеры Wi-Fi, совместимые со многими современными стандартами. Wi-Fi-адаптерами, как правило, снабжены и КПК (карманные персональные компьютеры), что также позволяет подключать их к беспроводным сетям.



Рис. 53. Адаптеры беспроводной сети

Для доступа к беспроводной сети адаптер может устанавливать связь непосредственно с другими адаптерами. Такая сеть называется *беспроводной одноранговой сетью*, или *Ad Hoc* («к случаю»). Адаптер также может устанавливать связь через специальное устройство – *точку доступа*. Такой режим называется *инфраструктурой*.

Для выбора способа подключения адаптер должен быть настроен на использование либо Ad Hoc, либо инфраструктурного режима.

Точка доступа (рис. 54) представляет собой автономный модуль со встроенным микрокомпьютером и приемно-передающим устройством.

Через точку доступа осуществляется взаимодействие и обмен информацией между беспроводными адаптерами, а также связь с проводным сегментом сети. Таким образом, точка доступа играет роль коммутатора.



Рис. 54. Точка доступа беспроводной сети

Точка доступа имеет сетевой интерфейс (uplink port), при помощи которого она может быть подключена к обычной проводной сети. Через этот же интерфейс может осуществляться и настройка точки.

Точка доступа может использоваться как для подключения к ней клиентов (базовый режим точки доступа), так и для взаимодействия с другими точками доступа с целью построения распределенной сети (Wireless Distributed System – WDS). Это режимы беспроводного моста «точка–точка» и «точка – много точек», беспроводной клиент и повторитель.

Доступ к сети обеспечивается путем передачи широкоэмитательных сигналов через эфир. Принимающая станция может получать сигналы в диапазоне работы нескольких передающих станций. Станция-приемник использует идентификатор зоны обслуживания (Service Set Identifier – SSID) для фильтрации получаемых сигналов и выделения того, который ей нужен.

Зоной обслуживания (Service Set – SS) называются логически сгруппированные устройства, обеспечивающие подключение к беспроводной сети.

Базовая зона обслуживания (Basic Service Set – BSS) – это группа станций, которые связываются друг с другом по беспроводной связи. Технология BSS предполагает наличие особой станции, которая называется *точкой доступа* (access point).

5.2.2. Физический уровень

Стек протоколов стандарта IEEE 802.11 соответствует общей структуре стандартов комитета 802, т. е. состоит из физического уровня и канального уровня с подуровнями управления доступом к среде MAC (Media Access Control) и логической передачи данных LLC (Logical Link Control). Как и у всех технологий семейства 802, технология 802.11 определяется двумя нижними уровнями, т. е. физическим уровнем и уровнем MAC, а уровень LLC выполняет свои стандартные общие для всех технологий LAN функции (рис. 55).

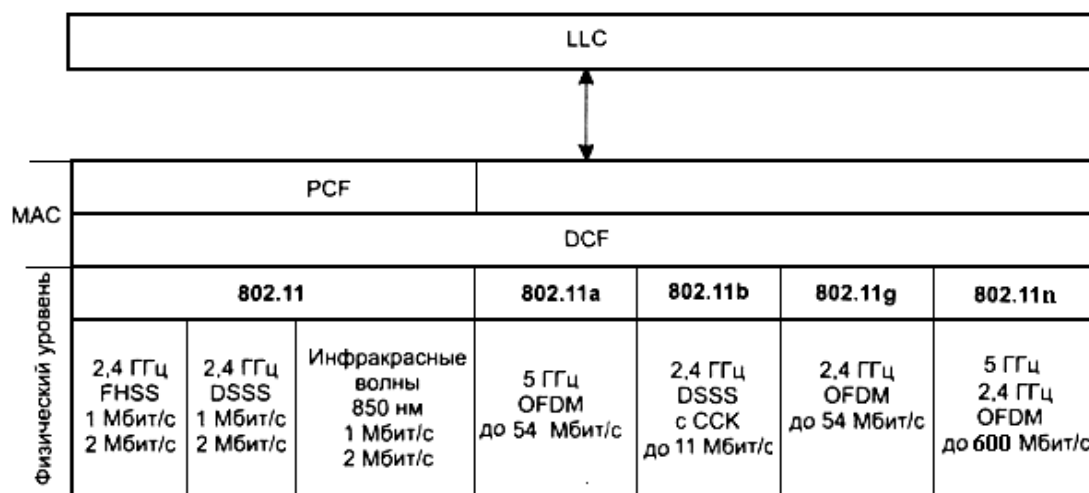


Рис. 55. Стек протоколов IEEE 802.11

На физическом уровне существует несколько вариантов спецификаций, которые отличаются используемым частотным диапазоном, методом кодирования и, как следствие, – скоростью передачи данных. Все варианты физического уровня работают с одним и тем же алгоритмом уровня MAC, но некоторые временные параметры уровня MAC зависят от используемого физического уровня.

В основе всех беспроводных протоколов семейства 802.11 лежит технология расширения спектра (Spread Spectrum, SS).

Спектром сигнала называется область частот, составляющих данный сигнал.

Такая технология подразумевает, что первоначально узкополосный (в смысле ширины спектра) полезный информационный сигнал при передаче преобразуется таким образом, что его спектр оказывается значительно шире спектра первоначального сигнала, т. е. спектр сигнала как бы «размазывается» по частотному диапазону. Одновременно с расширением спектра сигнала происходит и перераспределение спектральной энергетической плотности сигнала – энергия сигнала также «размазывается» по спектру. В результате максимальная мощность преобразованного сигнала оказывается значительно ниже мощности исходного сигнала. При этом уровень полезного информационного сигнала может в буквальном смысле сравниваться с уровнем естественного шума. В итоге сигнал становится в каком-то смысле «невидимым»: он просто теряется на уровне естественного шума.

Собственно, именно в изменении спектральной энергетической плотности сигнала и заключается идея расширения спектра. Если подходить к проблеме передачи данных традиционным способом, как это делается в радиоэфире, где каждой радиостанции отводится свой диапазон вещания, то неизбежно придется столкнуться с проблемой ограничения радиодиапазона, предназначенного для совместного использования. Поэтому необходимо найти такой способ передачи информации, при котором пользователи могли бы сосуществовать в одном частотном диапазоне и при этом не мешать друг другу. Именно эту задачу и решает технология расширения спектра.

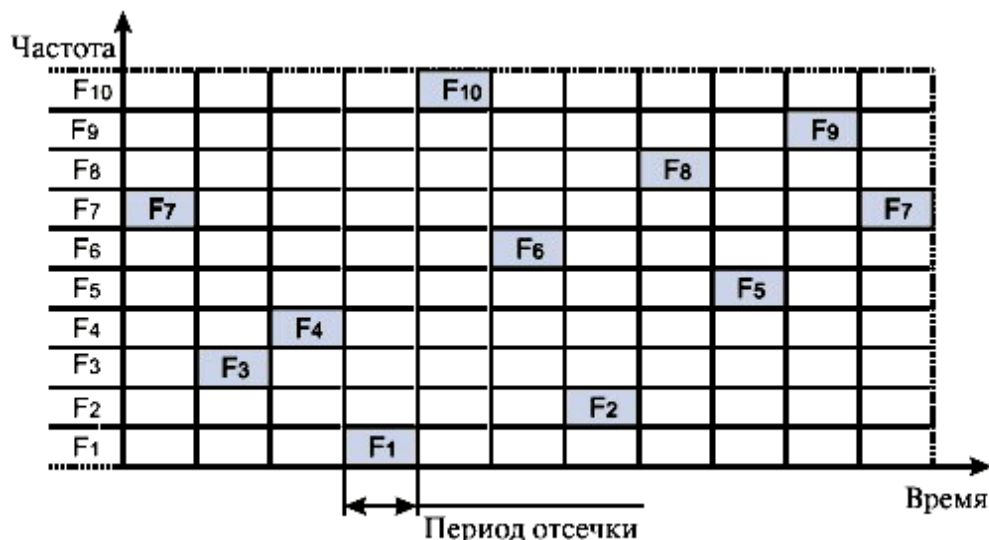
Исходный стандарт 802.11 определяет две такие технологии:

- технологию расширения спектра путем скачкообразной перестройки частоты (FHSS) в диапазоне 2,4 ГГц;
- технологию широкополосной модуляции с расширением спектра методом прямой последовательности (DSSS) в диапазоне 2,4 ГГц.

В беспроводных локальных сетях технологии FHSS передача ведется с постоянной сменой несущей в пределах широкого диапазона частот. В результате мощность сигнала распределяется по всему диапазону и прослушивание какой-то определенной частоты дает только небольшой шум. Последовательность несущих частот является псевдослучайной, известной только передатчику и приемнику. Попытка подавления сигнала в каком-то узком диапазоне также не слишком ухудшает сигнал, так как подавляется только небольшая часть информации. Идею этого метода иллюстрирует рис. 56.

В течение фиксированного интервала времени передача ведется на неизменной несущей частоте. На каждой несущей частоте для передачи дискретной информации применяются стандартные методы модуляции, такие как частотная или фазовая. Чтобы приемник синхронизировался

с передатчиком в начале каждого периода передачи в течение некоторого времени, передаются синхробиты. Так что полезная скорость этого метода кодирования оказывается меньше из-за постоянных накладных расходов на синхронизацию.



Последовательность перестройки частот: $F_7-F_3-F_4-F_1-F_{10}-F_6-F_2-F_8-F_5-F_9-F_7$

Рис. 56. Расширение спектра скачкообразной перестройкой частоты

Несущая частота меняется в соответствии с номерами частотных подканалов, вырабатываемых алгоритмом псевдослучайных чисел. Псевдослучайная последовательность зависит от некоторого параметра, который называют *начальным числом*. Если приемнику и передатчику известны алгоритм и значение начального числа, то они меняют частоты в одинаковой последовательности, называемой последовательностью псевдослучайной перестройки частоты.

Если частота смены подканалов ниже, чем скорость передачи данных в канале, то такой режим называют *медленным расширением спектра*; в противном случае мы имеем дело с *быстрым расширением спектра*.

Метод быстрого расширения спектра более устойчив к помехам, поскольку узкополосная помеха, которая подавляет сигнал в определенном подканале, не приводит к потере бита, так как его значение повторяется несколько раз в различных частотных подканалах. В этом режиме не проявляется эффект межсимвольной интерференции, потому что ко времени прихода задержанного вдоль одного из путей сигнала система успевает перейти на другую частоту.

Метод медленного расширения спектра таким свойством не обладает, но зато он проще в реализации и сопряжен с меньшими накладными расходами.

Беспроводные локальные сети FHSS поддерживают скорости передачи 1 и 2 Мбит/с. Устройства FHSS делят полосу частот от 2,402 до 2,480 ГГц на 79 неперекрывающихся каналов. Ширина каждого из 79 каналов составляет 1 МГц.

В методе прямого последовательного расширения спектра DSSS также используется весь частотный диапазон, выделенный для одной беспроводной линии связи. В отличие от метода FHSS, весь частотный диапазон занимает не за счет постоянных переключений с частоты на частоту, а за счет того, что каждый бит информации заменяется N -битами, так что тактовая скорость передачи сигналов увеличивается в N раз. А это, в свою очередь, означает, что спектр сигнала также расширяется в N раз. Достаточно соответствующим образом выбрать скорость передачи данных и значение N , чтобы спектр сигнала заполнил весь диапазон.

Цель кодирования методом DSSS та же, что и методом FHSS, – повышение устойчивости к помехам. Узкополосная помеха будет искажать только определенные частоты спектра сигнала, так что приемник с большой степенью вероятности сможет правильно распознать передаваемую информацию.

Код, которым заменяется двоичная единица исходной информации, называется *расширяющей последовательностью*, а каждый бит такой последовательности – *чипом*.

Соответственно, скорость передачи результирующего кода называют *чиповой скоростью*. Двоичный ноль кодируется инверсным значением расширяющей последовательности. Приемники должны знать расширяющую последовательность, которую использует передатчик, чтобы понять передаваемую информацию.

Количество битов в расширяющей последовательности определяет коэффициент расширения исходного кода. Как и в случае FHSS, для кодирования битов результирующего кода может использоваться любой вид модуляции.

Чем больше коэффициент расширения, тем шире спектр результирующего сигнала и выше степень подавления помех. Но при этом растет занимаемый каналом диапазон спектра. Обычно коэффициент расширения имеет значение от 10 до 100.

Очень часто в качестве значения расширяющей последовательности берут последовательность Баркера (Barker), которая состоит из 11 бит: 10110111000. Если передатчик использует эту последовательность, то передача трех битов 110 ведет к передаче следующих битов:

10110111000 10110111000 01001000111.

Последовательность Баркера позволяет приемнику быстро синхронизироваться с передатчиком, т. е. надежно выявлять начало последовательности. Приемник определяет такое событие, поочередно сравнивая получаемые биты с образцом последовательности. Действительно, если сравнить последовательность Баркера с такой же последовательностью, но сдвинутой на один бит влево или вправо, мы получим меньше половины совпадений значений битов. Даже при искажении нескольких битов, с большой долей вероятности приемник правильно определит начало последовательности, сможет правильно интерпретировать получаемую информацию.

Метод DSSS в меньшей степени защищен от помех, чем метод быстрого расширения спектра, так как мощная узкополосная помеха влияет на часть спектра, а значит и на результат распознавания единиц или нулей.

Беспроводные локальные сети DSSS используют каналы шириной 22 МГц, благодаря чему многие WLAN могут работать в одной и той же зоне покрытия. В Северной Америке и большей части Европы, в том числе и в России, каналы шириной 22 МГц позволяют создать в диапазоне 2,4...2,483 ГГц три неперекрывающихся канала передачи. Эти каналы показаны на рис. 57.

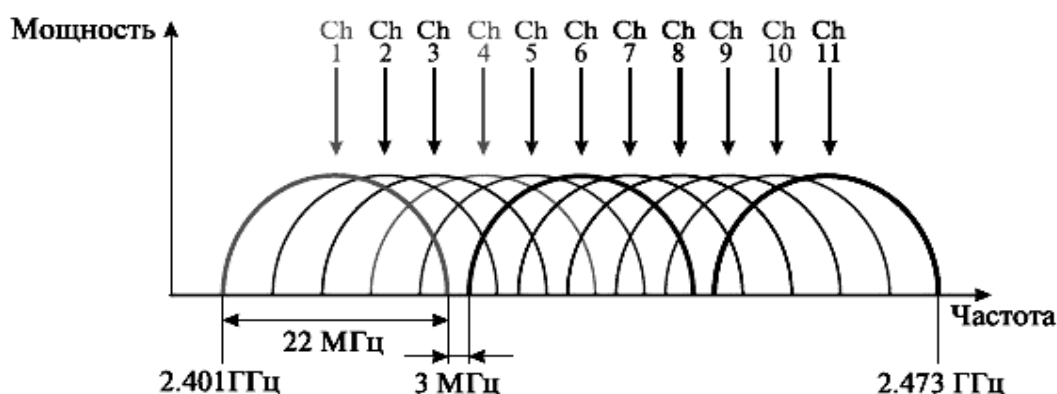


Рис. 57. Каналы, используемые в технологии DSSS

Передача данных в беспроводных локальных сетях может осуществляться в диапазоне инфракрасных волн. Средой передачи являются инфракрасные волны диапазона 850 нм, которые генерируются либо полупроводниковым лазерным диодом, либо светодиодом. Так как инфракрасные волны не проникают через стены, область покрытия LAN ограничивается зоной прямой видимости. Стандарт предусматривает три варианта распространения излучения: ненаправленную антенну, отражение от потолка и фокусное направленное излучение. В первом случае узкий луч рассеивается с помощью системы линз. Фокусное направ-

ленное излучение предназначено для организации двухточечной связи, например между двумя зданиями.

Из всех существующих стандартов беспроводной передачи данных IEEE 802.11 на практике используются три стандарта: 802.11a, 802.11b и 802.11g.

Стандарт IEEE 802.11a имеет большую ширину полосы из семейства стандартов 802.11 при скорости передачи данных до 54 Мбит/с. В отличие от базового стандарта, ориентированного на область частот 2,4 ГГц, спецификациями 802.11a предусмотрена работа в диапазоне 5 ГГц. В качестве метода модуляции сигнала выбрано ортогональное частотное мультиплексирование (OFDM). Суть этого механизма состоит в том, что весь доступный частотный диапазон разбивается на достаточно много поднесущих (от нескольких сотен до тысяч). Одному каналу связи (приемнику и передатчику) назначают для передачи несколько таких несущих, выбранных из множества по определенному закону. Передача ведется одновременно по всем поднесущим, т. е. в каждом передатчике исходящий поток данных разбивается на N субпоток, где N – число поднесущих, назначенных данному передатчику. Распределение поднесущих в ходе работы может динамически изменяться, что делает данный механизм не менее гибким, чем метод временного уплотнения. К недостаткам 802.11a относятся более высокая потребляемая мощность радиопередатчиков для частот 5 ГГц, а также меньший радиус действия.

Стандарт IEEE 802.11b завоевал наибольшую популярность у производителей оборудования для беспроводных сетей благодаря высокой скорости передачи данных (до 11 Мбит/с), а также ориентации на диапазон 2,4 ГГц. Поскольку оборудование, работающее на максимальной скорости 11 Мбит/с, имеет меньший радиус действия, чем на более низких скоростях, то стандартом 802.11b предусмотрено автоматическое снижение скорости при ухудшении качества сигнала.

Стандарт IEEE 802.11g является логическим развитием 802.11b и предполагает передачу данных в том же частотном диапазоне. Кроме того, стандарт 802.11g полностью совместим с 802.11b, т. е. любое устройство 802.11g должно поддерживать работу с устройствами 802.11b. Максимальная скорость передачи в стандарте 802.11g составляет 54 Мбит/с, поэтому на сегодня это наиболее перспективный стандарт беспроводной связи.

Стандарт 802.11n был утвержден 11 сентября 2009 года организацией IEEE (Institute of Electrical and Electronics Engineers). Теоретически 802.11n способен обеспечить скорость передачи данных до 600 Мбит/с. Разработчики спецификации 802.11n позаботились о том, чтобы компоненты на ее базе сохраняли совместимость с устройствами стандарта

802.11b или 802.11g в диапазоне 2,4 ГГц и с устройствами 802.11a – в диапазоне 5 ГГц.

5.2.3. Канальный уровень

Организация совместного использования среды передачи данных беспроводными локальными сетями определяется на более высоком канальном уровне, который делится на два подуровня: управление логическим каналом LLC и управление доступом к среде MAC. На рис. 58 изображен формат кадра MAC IEEE 802.11.

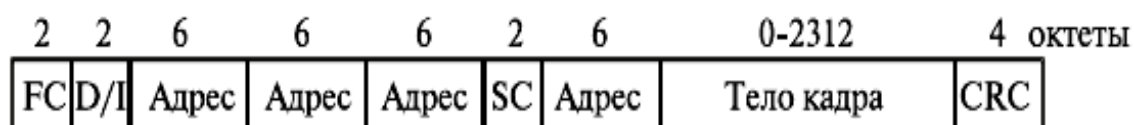


Рис. 58. Формат кадра MAC IEEE 802.11:
FC – управление кадром;
D/I – идентификатор длительности/соединения;
SC – управление очередностью

Поля кадра имеют следующее назначение.

- *Управление кадром.* Указывается тип кадра и предоставляется управляющая информация.
- *Идентификатор длительности/соединения.* Если используется поле длительности, указывается время (в микросекундах), на которое требуется выделить канал для успешной передачи кадра MAC. В некоторых кадрах управления в этом поле указывается идентификатор соединения.
- *Адреса.* Число и значение полей адреса зависит от контекста. Возможны следующие типы адресов: источника, назначения, передающей станции, принимающей станции.
- *Управление очередностью.* Содержит 4-битовое подполе номера фрагмента, используемое для фрагментации и повторной сборки, и 12-битовый порядковый номер, используемый для нумерации кадров, передаваемых между приемником и передатчиком.
- *Тело кадра.* Содержит модуль данных протокола LLC или управляющую информацию MAC.
- *Контрольная последовательность кадра.* 32-битовая проверка четности с избыточностью.

Приведенная общая структура применяется для информационных и управляющих кадров, хотя могут использоваться не все поля.

5.2.4. Передача данных в беспроводной сети WLAN

На MAC-уровне определяются два основных типа архитектуры беспроводных сетей – Ad Hoc и Infrastructure Mode.

В режиме Ad Hoc (рис. 59), который называют также Independent Basic Service Set (IBSS), или режимом Peer to Peer (точка-точка), станции непосредственно взаимодействуют друг с другом. Для этого режима нужен минимум оборудования: каждая станция должна быть оснащена беспроводным адаптером. При такой конфигурации не требуется создания сетевой инфраструктуры. Основными недостатками режима Ad Hoc являются ограниченный диапазон действия возможной сети и невозможность подключения к внешней сети (например, к Интернету).

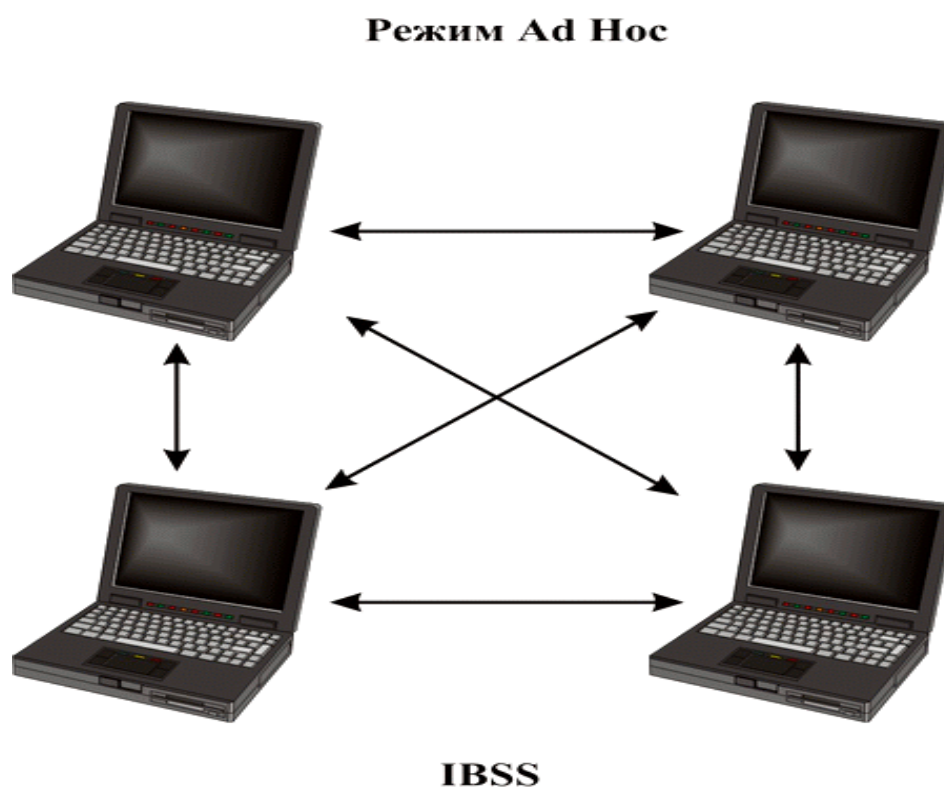


Рис. 59. Режим функционирования Ad Hoc

В режиме Infrastructure Mode (рис. 60) станции взаимодействуют друг с другом не напрямую, а через точку доступа (Access Point), которая выполняет в беспроводной сети роль своеобразного концентратора (аналогично тому, как это происходит в традиционных кабельных сетях). Существуют два режима взаимодействия с точками доступа – BSS (Basic Service Set) и ESS (Extended Service Set). В режиме BSS все станции связываются между собой только через точку доступа, которая может выполнять также роль моста к внешней сети. В режиме ESS суще-

ствуется инфраструктура нескольких сетей BSS, причем сами точки доступа взаимодействуют друг с другом, что позволяет передавать трафик от одной BSS к другой. Между собой точки доступа соединяются с помощью либо сегментов кабельной сети, либо радиомостов.

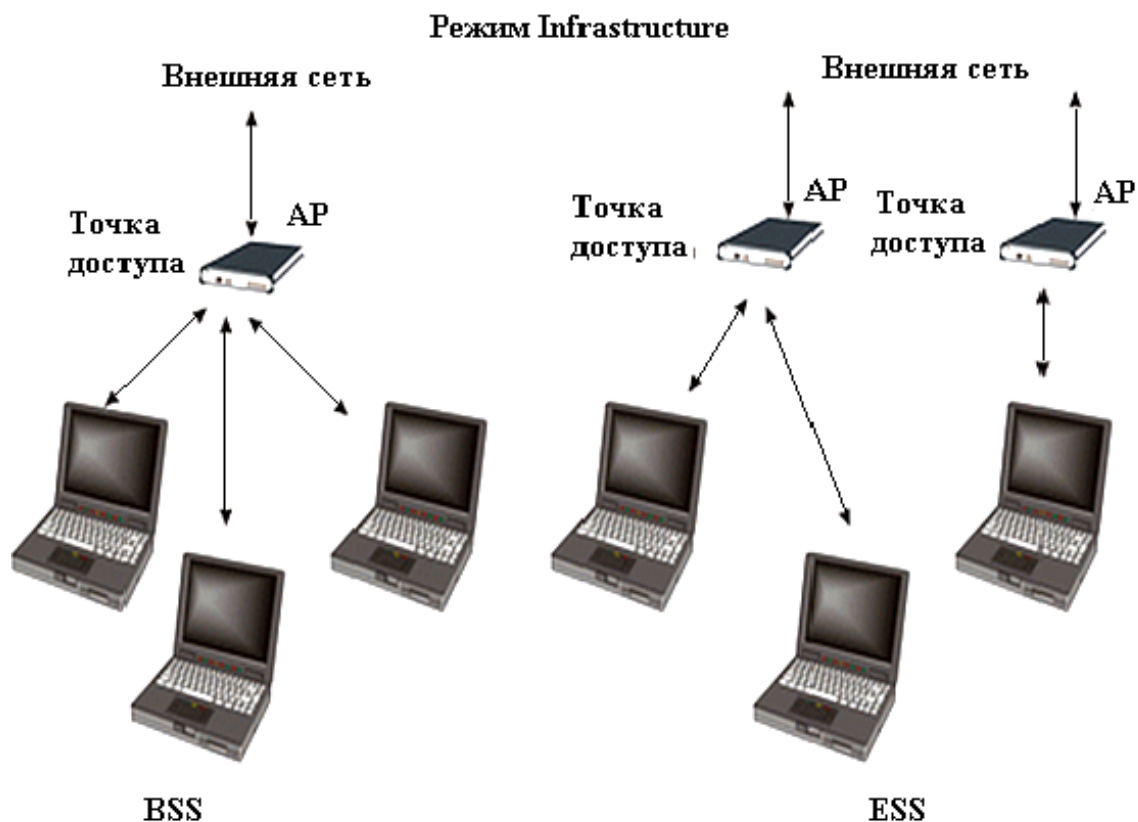


Рис. 60. Режим функционирования Infrastructure Mode

Кроме двух различных режимов функционирования беспроводных сетей, на MAC-уровне определяются правила коллективного доступа к среде передачи данных. Необходимость существования таких регламентирующих правил вполне очевидна. Представим себе ситуацию, когда каждый узел беспроводной сети, не соблюдая никаких правил, стал бы передавать данные в эфир. В результате интерференции нескольких таких сигналов узлы, которым предназначалась отправленная информация, не смогли бы не только ее получить, но и понять, что данная информация адресована им. Именно поэтому необходимо существование жестких регламентирующих правил, которые определяли бы коллективный доступ к среде передачи данных.

На MAC-уровне протокола 802.11 определяются два типа коллективного доступа к среде передачи данных: функция распределенной координации (Distributed Coordination Function, DCF) и функция централи-

зованной координации (Point Coordination Function, PCF). Рассмотрим более подробно каждый из этих механизмов.

Передача данных с использованием функции распределенной координации (DCF) основана на методе коллективного доступа с обнаружением несущей и механизмом избежания коллизий (Carrier Sense Multiple Access/Collision Avoidance, CSMA/CA). При такой организации каждый узел, прежде чем начать передачу, «прослушивает» среду, пытаясь обнаружить несущий сигнал, и только при условии, что среда свободна, может начать передачу данных.

В этом случае велика вероятность возникновения коллизий: когда два или более узлов сети одновременно (или почти одновременно) решат, что среда свободна, и начнут передавать данные. Для того чтобы снизить вероятность возникновения подобных ситуаций, используется механизм избежания коллизий (Collision Avoidance, CA). Суть данного механизма заключается в следующем. Каждый узел сети, убедившись, что среда свободна, прежде чем начать передачу, выжидает в течение определенного промежутка времени. Этот промежуток является случайным и складывается из двух составляющих: обязательного промежутка DIFS (DCF Interframe Space) и выбираемого случайным образом промежутка обратного отсчета (backoff time). В результате каждый узел сети перед началом передачи выжидает в течение случайного промежутка времени, что, естественно, значительно снижает вероятность возникновения коллизий, поскольку вероятность того, что два узла сети будут выжидать в течение одного и того же промежутка времени, чрезвычайно мала.

Для того чтобы гарантировать всем узлам сети равноправный доступ к среде передачи данных, необходимо соответствующим образом определить алгоритм выбора длительности промежутка обратного отсчета (backoff time). Промежуток обратного отсчета хотя и является случайным, но в то же время определяется на основании множества некоторых дискретных промежутков времени, т. е. равен целому числу элементарных временных промежутков, называемых тайм-слотами (Slot Time). Для выбора промежутка обратного отсчета каждый узел сети формирует так называемое окно конкурентного доступа (Contention Window, CW), используемое для определения количества тайм-слотов, в течение которых станция выжидала перед передачей. Фактически окно CW – это диапазон для выбора количества тайм-слотов, причем минимальный размер окна определяется в 31 тайм-слот, а максимальный размер – в 1023 тайм-слота. Промежуток обратного отсчета – это количество тайм-слотов, определяемое исходя из размера окна CW:

$$\text{Backoff time} = \text{Random} [\text{CW}_{\min}, \text{CW}_{\max}] \cdot \text{Slot Time}.$$

Когда узел сети пытается получить доступ к среде передачи данных, после обязательного промежутка ожидания DIFS запускается процедура обратного отсчета, т. е. включается обратный отсчет счетчика тайм-слотов, начиная от выбранного значения окна CW. Если в течение всего промежутка ожидания среда оставалась свободной (счетчик обратного отсчета равен нулю), то узел начинает передачу.

После успешной передачи окно CW формируется вновь. Если же за время ожидания передачу начал другой узел сети, то значение счетчика обратного отсчета останавливается и передача данных откладывается. После того как среда станет свободной, данный узел снова начинает процедуру обратного отсчета, но уже с меньшим размером окна CW, определяемого предыдущим значением счетчика обратного отсчета, и, соответственно, с меньшим значением времени ожидания. При этом очевидно, что чем большее число раз узел откладывает передачу по причине занятости среды, тем выше вероятность того, что в следующий раз он получит доступ к среде передачи данных (рис. 61).

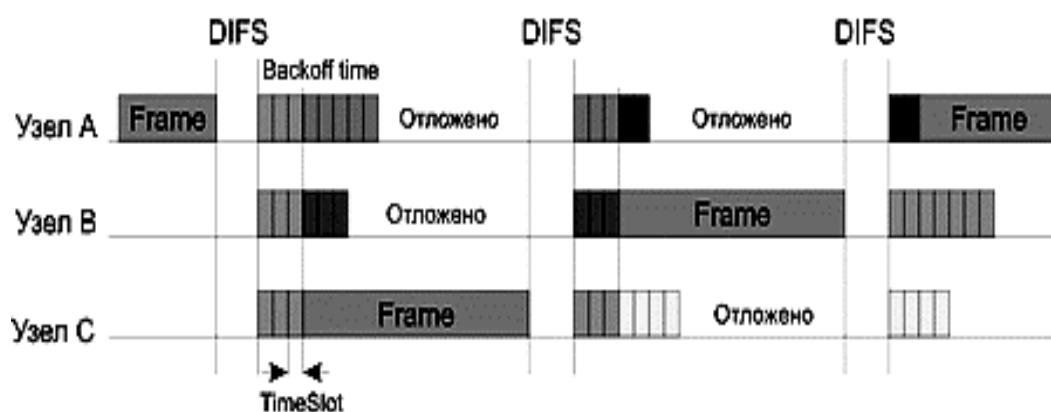


Рис. 61. Реализация равноправного доступа к среде передачи данных в методе DCF

Рассмотренный алгоритм реализации коллективного доступа к среде передачи данных гарантирует равноправный доступ всех узлов сети к среде. Однако при таком подходе вероятность возникновения коллизий, хотя и мала, все-таки существует. Понятно, что снизить вероятность возникновения коллизий можно путем увеличения максимального размера формируемого окна CW. В то же время это увеличит время задержек при передаче и тем самым снизит производительность сети. Поэтому в методе DCF для минимизации коллизий используется следующий алгоритм. После каждого успешного приема кадра принимающая сторона через короткий промежуток SIFS (Short Interframe Space) подтверждает успешный прием, посылая ответную квитанцию – кадр ACK (ACKnowledgement), рис. 62. Если в процессе передачи данных возник-

ла коллизия, то передающая сторона не получает кадр АСК об успешном приеме. В этом случае размер CW-окна для передающего узла увеличивается почти вдвое. Так, если для первой передачи размер окна равен 31 слоту, то для второй попытки передачи он уже составляет 63 слота, для третьей – 127 слотов, для четвертой – 255, для пятой – 511, а для всех последующих – 1023 слота. Таким образом, для каждой i -й передачи (если все предыдущие оказались безуспешными) размер CW-окна увеличивается по следующему правилу:

$$CW_i = 2CW_{i-1} + 1.$$

Таким образом, увеличение размера окна происходит динамически, по мере роста числа коллизий, что позволяет, с одной стороны, уменьшить временные задержки и, с другой стороны, снизить вероятность возникновения коллизий.

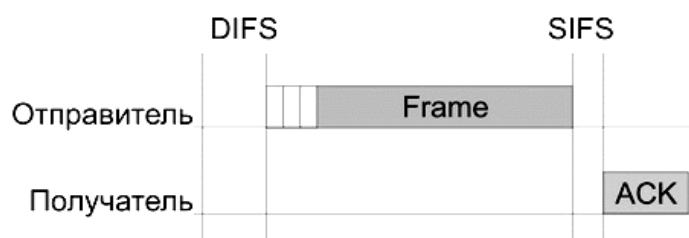


Рис. 62. Кадры квитанции, отсылаемые в случае успешной передачи данных

Говоря об алгоритме реализации равноправного доступа к среде передачи данных, необходимо также учитывать и размер кадра данных. Действительно, если кадры данных будут слишком большими, то при возникновении коллизий придется повторно передавать большой объем информации, что приведет к снижению производительности сети. Кроме того, при большом размере кадров данных узлы сети вынуждены простаивать в течение довольно продолжительного времени, прежде чем начать передачу.

В то же время использование кадров данных небольшого размера, хотя и позволяет гарантировать равноправный доступ всех узлов к среде передачи данных и минимизирует издержки при возникновении коллизий, не может не отразиться негативно на полезном сетевом трафике. Дело в том, что каждый кадр, наряду с полезной информацией, содержит информацию служебную (заголовок кадра). При уменьшении размера кадра сокращается величина именно полезной информации (пользовательских данных), что обуславливает передачу по сети избыточного количества служебной информации. Поэтому размер кадра – это своего рода золотая середина, от правильного выбора которой зависит эффективность использования среды передачи данных.

Рассмотренный механизм регламентирования коллективного доступа к среде передачи данных имеет одно узкое место – так называемую проблему скрытых узлов. Из-за наличия естественных препятствий возможна ситуация, когда два узла сети не могут «слышать» друг друга напрямую. Такие узлы называют скрытыми.

Для того чтобы разрешить проблему скрытых узлов, функция DCF опционально предусматривает возможность использования алгоритма RTS/CTS.

В соответствии с алгоритмом RTS/CTS каждый узел сети, перед тем как послать данные в «эфир», сначала отправляет специальное короткое сообщение, которое называется RTS (Ready to send) и означает готовность данного узла к отправке данных. Такое RTS-сообщение содержит информацию о продолжительности предстоящей передачи и об адресате и доступно всем узлам в сети (если только они не скрыты от отправителя). Это позволяет другим узлам задержать передачу на время, равное объявленной длительности сообщения. Приемная станция, получив сигнал RTS, отвечает посылкой сигнала CTS (Clear to send), свидетельствующего о готовности станции к приему информации. После этого передающая станция посылает пакет данных, а приемная станция должна передать кадр АСК, подтверждающий безошибочный прием. Последовательность отправки кадров между двумя узлами сети показана на рис. 63.

Теперь рассмотрим ситуацию, когда сеть состоит из четырех узлов: *A*, *B*, *C* и *D* (рис. 64). Предположим, что узел *C* находится в зоне досягаемости только узла *A*, узел *A* находится в зоне досягаемости узлов *C* и *B*, узел *B* находится в зоне досягаемости узлов *A* и *D*, а узел *D* находится в зоне досягаемости только узла *B*. Следовательно, в такой сети имеются скрытые узлы: узел *C* скрыт от узлов *B* и *D*, узел *A* – от узла *D*.

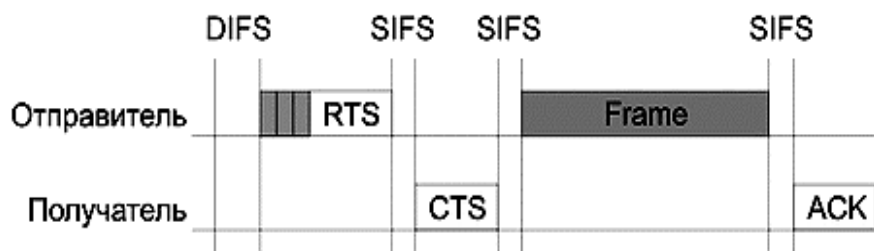


Рис. 63. Взаимодействие между двумя узлами сети в соответствии с алгоритмом RTS/CTS

В подобной сети алгоритм RTS/CTS позволяет справиться с проблемой возникновения коллизий, которая не решается посредством рассмотренного базового способа организации коллективного доступа в DCF. Действительно, пусть узел *A* пытается передать данные узлу *B*. Для это-

го он посылает сигнал RTS, который, помимо узла *B*, получает также узел *C*, но не получает узел *D*. Узел *C*, получив данный сигнал, блокируется, т. е. приостанавливает попытки передавать сигнал до момента окончания передачи между узлами *A* и *B*. Узел *B* в ответ на полученный сигнал RTS посылает кадр CTS, который получают узлы *A* и *D*. Узел *D*, получив данный сигнал, также блокируется на время передачи между узлами *A* и *B*.

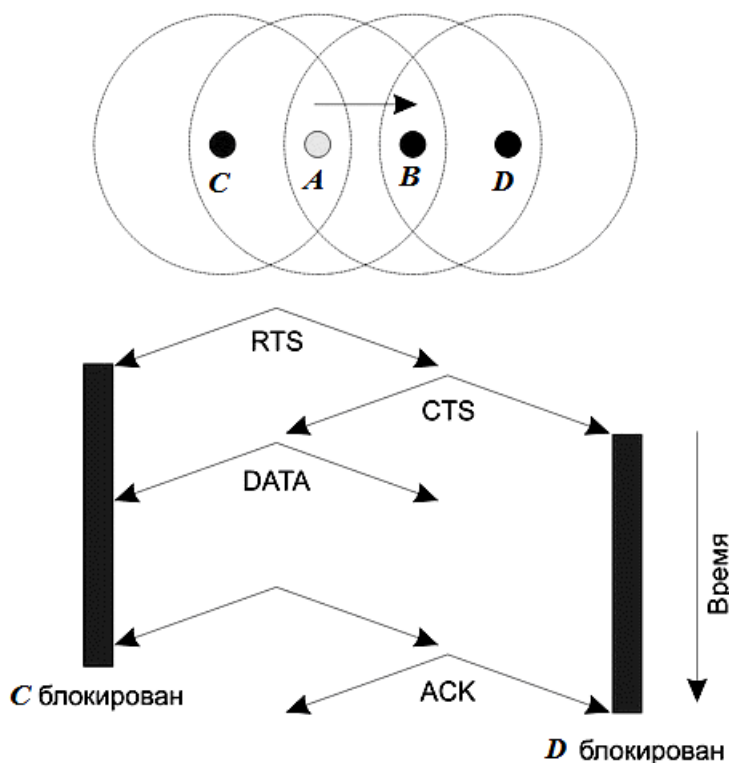


Рис. 64. Решение проблемы скрытых узлов в алгоритме RTS/CTS

У алгоритма RTS/CTS имеются свои подводные камни, которые в определенных ситуациях могут приводить к снижению эффективности использования среды передачи данных. Например, в некоторых ситуациях возможно такое явление, как распространение эффекта ложных блокировок узлов, что в конечном счете может привести к блокировке в сети.

Рассмотрим сеть, показанную на рис. 65. Пусть узел *B* пытается передать данные узлу *A*, посылая ему кадр RTS. Поскольку этот кадр получает также и узел *C*, то он блокируется на время передачи между узлами *A* и *B*. Узел *D*, пытаясь передать данные узлу *C*, посылает кадр RTS, но поскольку узел *C* заблокирован, то он не получает ответа и начинает процедуру обратного отсчета с увеличенным размером окна. В то же время кадр RTS, посланный узлом *D*, получает и узел *E*, который, ложно предполагая, что за этим последует сеанс передачи данных от узла *D* к узлу *C*, блокируется. Это ложная блокировка, поскольку ре-

ально между узлами *D* и *C* передачи нет. Более того, если узел *F* попытается передать данные ложно заблокированному узлу *E* и пошлет свой кадр RTS, то он ложно заблокирует узел *G*.

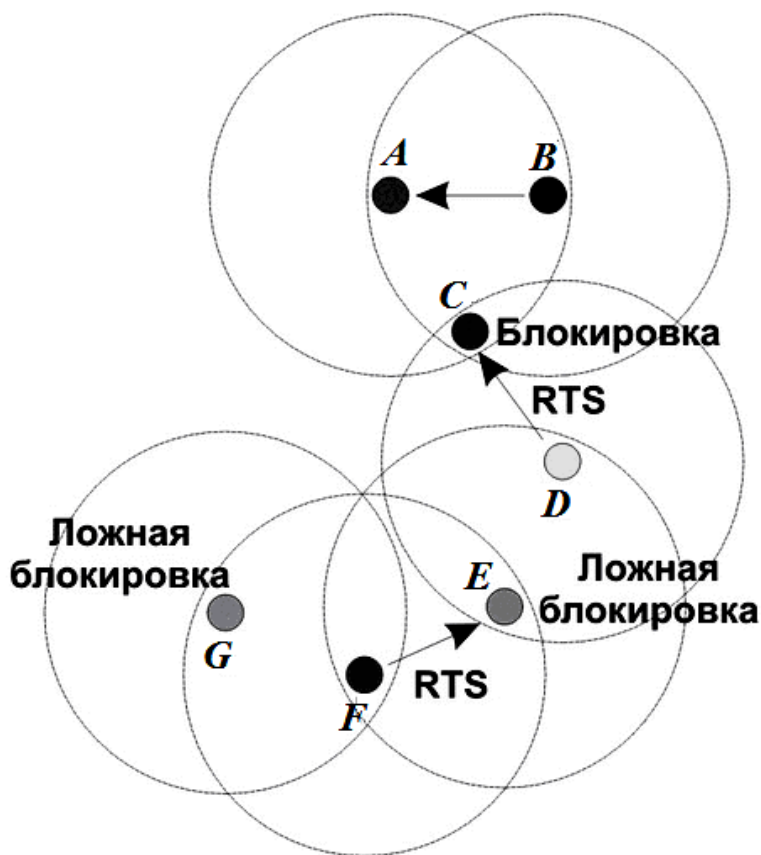


Рис. 65. Возникновение ложных блокировок узлов сети

Описанное явление ложной блокировки узлов может приводить к кратковременной блокировке всей сети.

Максимальная длина кадра данных 802.11 равна 2346 байтам, длина RTS-кадра – 20 байтам, CTS-кадра – 14 байтам. Так как RTS- и CTS-кадры гораздо короче, чем кадр данных, потери данных в результате коллизии RTS- или CTS-кадров гораздо меньше, чем при коллизии кадров данных. Процедура обмена RTS- и CTS-кадрами не обязательна. От нее можно отказаться при небольшой нагрузке сети, поскольку в такой ситуации коллизии случаются редко, а значит не стоит тратить дополнительное время на выполнение процедуры обмена RTS- и CTS-кадрами.

При помехах иногда случается, что теряются большие фреймы данных, поэтому можно уменьшить длину этих фреймов путем *фрагментации*. Фрагментация фрейма – это выполняемая на уровне MAC функция, назначение которой – повысить надежность передачи фреймов

через беспроводную среду. Под фрагментацией понимается дробление фрейма на меньшие фрагменты и передача каждого из них отдельно (рис. 66).

Предполагается, что вероятность успешной передачи меньшего фрагмента через зашумленную беспроводную среду выше. Получение каждого фрагмента фрейма подтверждается отдельно; следовательно, если какой-нибудь фрагмент фрейма будет передан с ошибкой или вступит в коллизию, передавать повторно придется только его, а не весь фрейм. Это увеличивает пропускную способность среды.

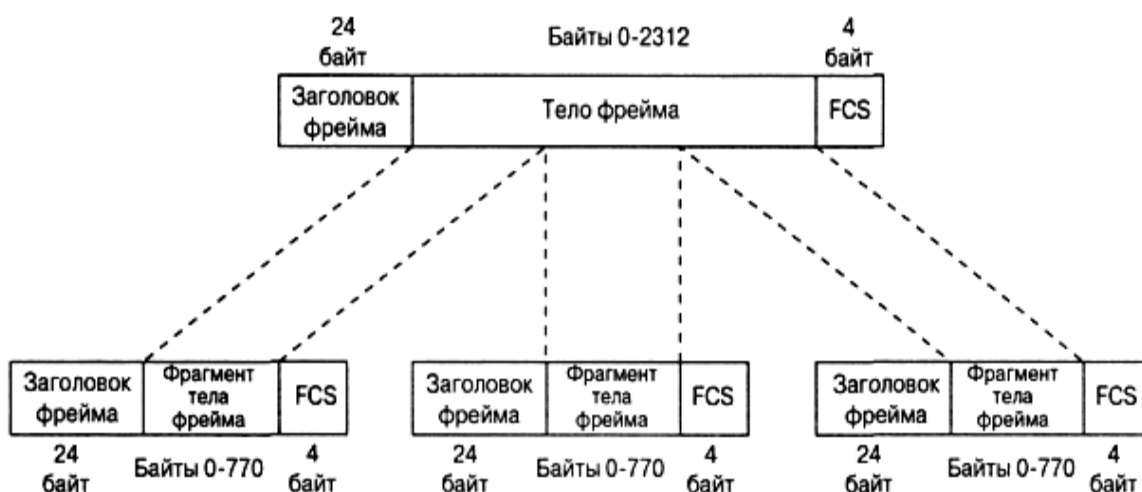


Рис. 66. Фрагментация фрейма

Размер фрагмента может задавать администратор сети. Фрагментации подвергаются только одноадресные фреймы. Широковещательные или многоадресные фреймы передаются целиком. Кроме того, фрагменты фрейма передаются пакетом, с использованием только одной итерации механизма доступа к среде DCF.

Хотя за счет фрагментации можно повысить надежность передачи фреймов в беспроводных локальных сетях, она приводит к увеличению «накладных расходов» MAC-протокола стандарта 802.11. Каждый фрагмент фрейма включает информацию, содержащуюся в заголовке 802.11 MAC, а также требует передачи соответствующего фрейма подтверждения. Это увеличивает число служебных сигналов MAC-протокола и снижает реальную производительность беспроводной станции. Фрагментация – это баланс между надежностью и непроизводительной загрузкой среды.

Рассмотренный выше механизм распределенной координации DCF является базовым для протоколов 802.11 и может использоваться как в беспроводных сетях, функционирующих в режиме Ad-Hoc, так и в сетях, функционирующих в режиме Infrastructure, т. е. в сетях, инфраструктура которых включает точку доступа.

Для сетей в режиме Infrastructure более естественным является несколько иной механизм регламентирования коллективного доступа, известный как функция централизованной координации (Point Coordination Function, PCF). Отметим, что механизм PCF является опциональным и применяется только в сетях с точкой доступа.

В случае использования механизма PCF один из узлов сети (точка доступа) является центральным и называется центром координации (Point Coordinator, PC). На центр координации возлагается задача управления коллективным доступом всех остальных узлов сети к среде передачи данных на основе определенного алгоритма опроса или исходя из приоритетов узлов сети. Иными словами, центр координации опрашивает все узлы сети, внесенные в его список, и на основании этого опроса организует передачу данных между всеми узлами сети. Важно, что такой подход полностью исключает конкурирующий доступ к среде, как в случае механизма DCF, и делает невозможным возникновение коллизий, а для зависимых от времени приложений гарантирует приоритетный доступ к среде. Таким образом, PCF может использоваться для организации приоритетного доступа к среде передачи данных.

Функция централизованной координации не отрицает функцию распределенной координации, а, скорее, дополняет ее, накладываясь поверх. Фактически в сетях с механизмом PCF реализуется как механизм PCF, так и традиционный механизм DCF. В течение определенного промежутка времени реализуется механизм PCF, затем – DCF, а потом все повторяется заново.

Для того чтобы иметь возможность чередовать режимы PCF и DCF, необходимо, чтобы точка доступа, выполняющая функции центра координации и реализующая режим PCF, имела бы приоритетный доступ к среде передачи данных. Это можно сделать, если использовать конкурентный доступ к среде передачи данных (как и в методе DCF), но для центра координации разрешить использовать промежуток ожидания, меньший DIFS. В этом случае, если центр координации пытается получить доступ к среде, то он ожидает (как и все остальные узлы сети) окончания текущей передачи и, поскольку для него определяется минимальный режим ожидания после обнаружения «тишины» в эфире, первым получает доступ к среде. Промежуток ожидания, определяемый для центра координации, называется PIFS (PCF Interframe Space), причем $SIFS < PIFS < DIFS$.

Режимы DCF и PCF объединяются в так называемом суперфрейме, который образуется из промежутка бесконкурентного доступа к среде, называемого CFP (Contention-Free Period), и следующего за ним промежутка конкурентного доступа к среде CP (Contention Period), рис. 67.

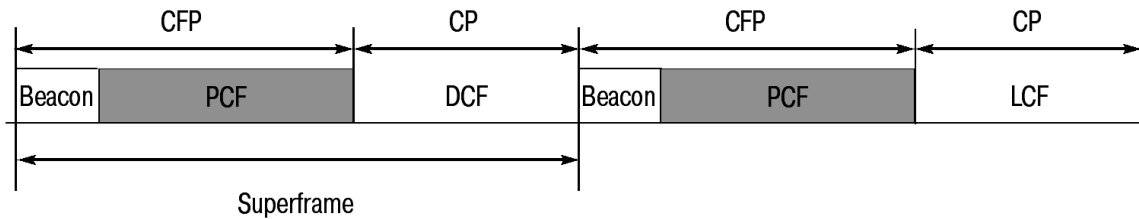


Рис. 67. Объединение режимов PCF и DCF в одном суперфрейме

Суперфрейм начинается с кадра-маячка (beacon), получив который все узлы сети приостанавливают попытки передавать данные на время, определяемое периодом CFP. Кадры-маячки несут служебную информацию о продолжительности CFP-промежутка и позволяют синхронизировать работу всех узлов сети.

Во время режима PCF точка доступа опрашивает все узлы сети о кадрах, которые стоят в очереди на передачу, посылая им служебные кадры CF_POLL.

Опрашиваемые узлы в ответ на получение кадров CF_POLL посылают подтверждение CF_ACK. Если подтверждения не получено, то точка доступа переходит к опросу следующего узла.

Кроме того, чтобы иметь возможность организовать передачу данных между всеми узлами сети, точка доступа может передавать кадр данных (DATA) и совмещать кадр опроса с передачей данных (кадр DATA+CF_POLL). Аналогично узлы сети могут совмещать кадры подтверждения с передачей данных DATA+CF_ACK (рис. 68).

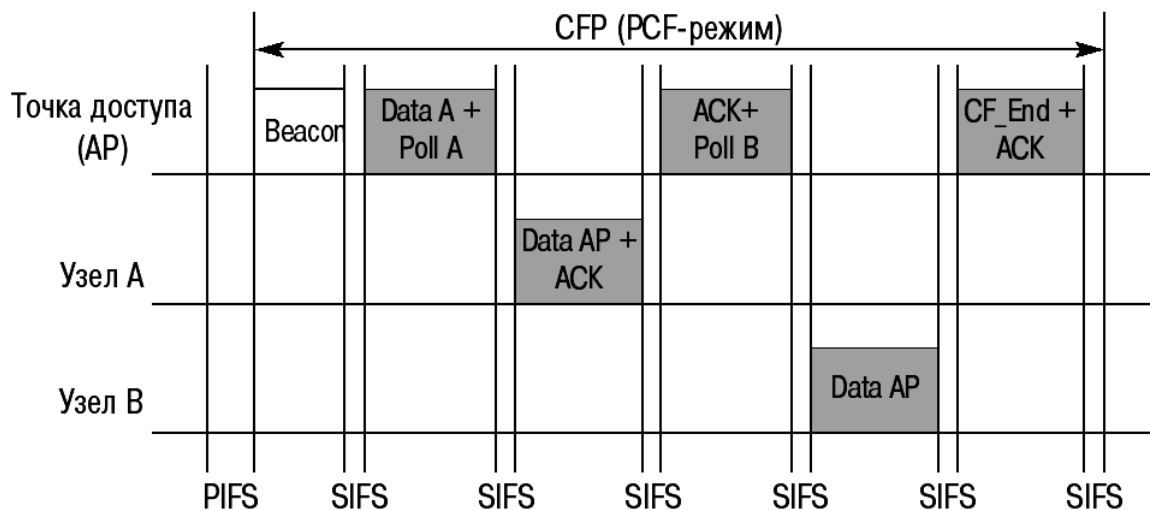


Рис. 68. Организация передачи данных между узлами сети в режиме PCF

Допускаются следующие типы кадров во время режима PCF:

- DATA – кадр данных;
- CF_ACK – кадр подтверждения;
- CF_POLL – кадр опроса;

- DATA+CF_ACK – комбинированный кадр данных и подтверждения;
- DATA+CF_POLL – комбинированный кадр данных и опроса;
- DATA+CF_ACK+CF_POLL – комбинированный кадр данных, подтверждения и опроса;
- CF_ACK+CF_POLL – комбинированный кадр подтверждения и опроса.

5.3. Беспроводная сеть Bluetooth

В 1994 году начались работы по изучению возможности использования мобильных сетевых коммуникаций. Компании IBM, Nokia, Intel и Toshiba создали консорциум для разработки стандарта беспроводной связи между компьютерами посредством устройств с ограниченным радиусом действия.

Проект получил название Bluetooth. Он являлся конкурентом стандарта IEEE 802.11 (оба стандарта используют один и тот же частотный диапазон, одни и те же 79 каналов). Главной его целью являлось удаление любых кабелей из телефонии, а если получится – и из локальных сетей. Очевидно, что в нынешнем виде Bluetooth не может вытеснить 802.11, хотя бы из-за ограничений на максимальный размер сети. Но эта технология быстро развивается и трудно предсказать, какое место она займет в самые ближайшие годы. В 1999 году был издан 1500-страничный документ v1.0. После этого группа компаний IEEE взяла этот документ за основу стандарта 802.15 (физический уровень и уровень передачи данных).

5.3.1. Физическая среда передачи данных

Основу сети Bluetooth составляют пикосети (piconet), состоящие из одного главного узла и до семи клиентских, размещенных в радиусе 10 м (рис. 69). Все узлы такой сети работают на одной частоте и разделяют общий канал. В одной достаточно большой комнате могут располагаться несколько пикосетей. Эти сети могут связываться друг с другом через мосты. Пикосети, объединенные вместе, составляют рассеянную сеть (scatternet). Поскольку в каждой пикосети имеется свой главный узел (master), последовательность и фазы переключения их частот не будут совпадать. Если пикосети взаимодействуют друг с другом, то это приводит к понижению их пропускной способности.

Устройство Bluetooth может выступать в качестве клиента в нескольких пикосетях, но главным узлом (master) может быть только в одной пикосети. Кроме 7 активных клиентских узлов, главный узел может поддерживать до 255 пассивных (спящих) узлов, переведенных управляющим узлом в режим пониженного энергопотребления.

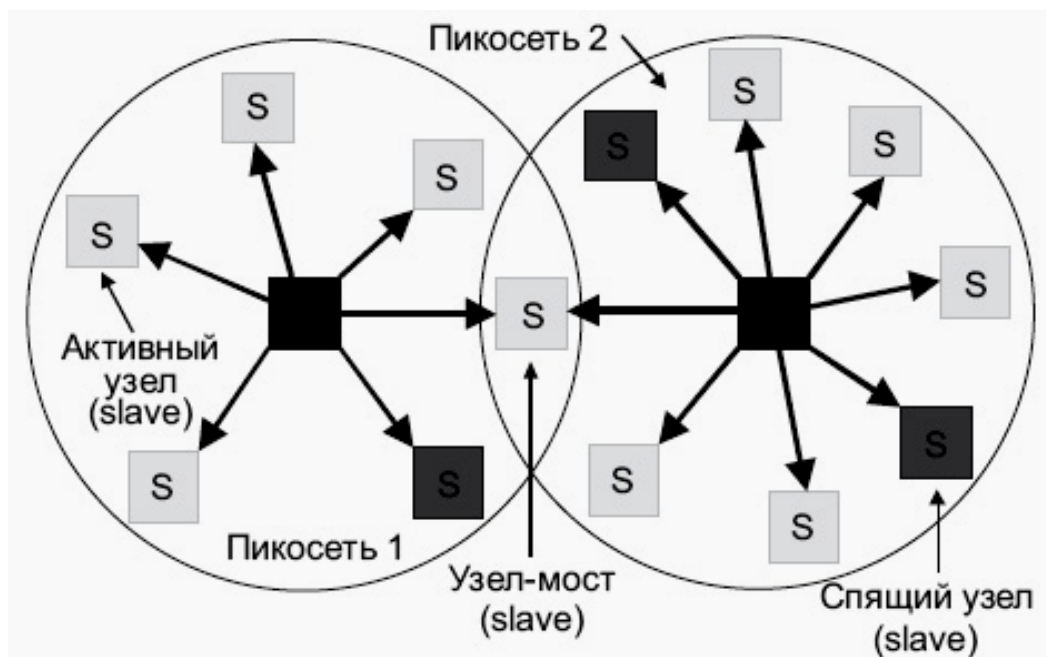


Рис. 69. Две пикосети, образующие рассеянную сеть

Мастер и клиент могут меняться ролями. Это выполняется в два этапа.

1. Происходит отключение обоих участников процесса от пикосети и осуществляется переключение TDD-трансиверов (Time Division Duplex).
2. Если требуется, узлы старой пикосети образуют новую пикосеть.

Когда узел получил подтверждение на свой пакет запроса, он будет использовать параметры новой пикосети, заданные новым мастером. На этом переключение мастер–клиент завершается.

Самым низким уровнем протокола является уровень радиосвязи. На этом уровне данные передаются от главного узла к подчиненному, бит за битом. Все узлы пикосети перестраивают частоту одновременно, последовательность частот определяется главным узлом. Главный узел (master) является источником синхронизации для всех клиентов пикосети.

Выше уровня радиосвязи размещен уровень немодулированной передачи. Он преобразует поток бит в кадры и определяет базовые форматы. Передача со стороны главного узла производится в четные такты, а со стороны подчиненных узлов – в нечетные.

Структура протоколов Bluetooth не следует моделям OSI, TCP/IP и 802, однако ведутся работы по адаптации Bluetooth к модели IEEE 802. В спецификации определено 5 уровней: физический, базовый, управления каналом, сетевой и уровень приложений. Физический уровень протокола соответствует базовым принципам моделей OSI и 802.

5.3.2. Физический уровень

В 2002 году IEEE утвердил стандарт 802.15.1. Пока стандарт 802.15 и Bluetooth не идентичны, но ожидается их объединение в самом ближайшем будущем. Технология Bluetooth использует нелицензируемый (практически везде, кроме России) частотный диапазон 2,4000...2,4835 ГГц.

Кодирование сигнала осуществляется по схеме GFSK (Gaussian Frequency Shift Keying): логическому 0 и 1 соответствуют две разные частоты. В оговоренной частотной полосе выделяется 79 радиоканалов по 1 МГц каждый. В некоторых странах используется меньшее число каналов (например, во Франции – 23). Каждый из каналов структурируется с помощью выделения временных слотов (доменов) длительностью 625 мкс (разделение по времени).

По мощности передатчики делятся на три класса: 100 мВт (для связи до 100 м); 2 мВт (до 10 м) и 1 мВт (~ 10 см). BER (Bit Error Rate) для приемника должна находиться на уровне < 0,1 %.

Протокол использует коммутацию каналов и пакетов. Передача данных выполняется с использованием алгоритма доступа TDDMA (Time Division Duplex Multiple Access). Каждый пакет передается с использованием иного частотного канала по отношению к предыдущему. Производится 1600 переключений частоты в секунду.

5.3.3. Канальный уровень

На рис. 70 показан формат заголовка кадра протокола Bluetooth. Структура заголовка регламентируется базовым уровнем.

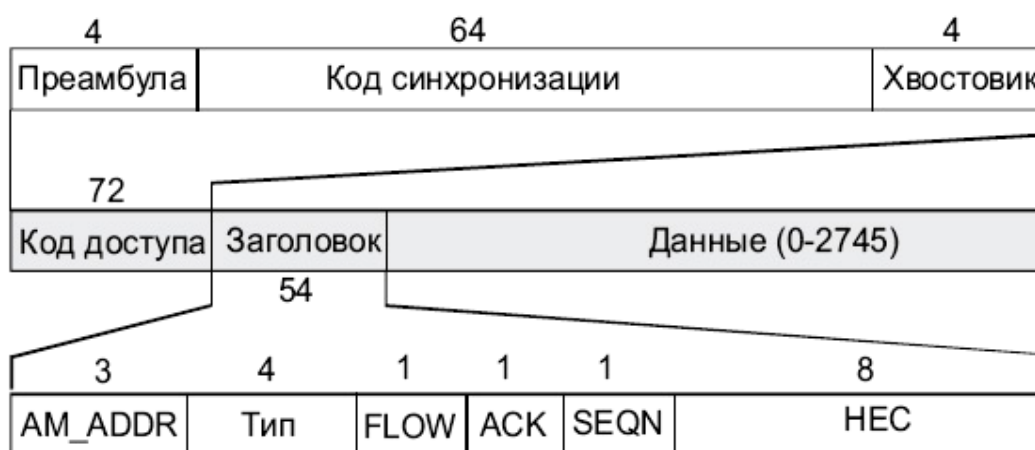


Рис. 70. Формат кадра протокола Bluetooth

Предусмотрено три типа кодов доступа: САС (Channel Access Code – код доступа к каналу), ДАС (Device Access Code – код доступа к устройству) и IAC (Inquiry Access Code – код запроса). Код доступа к каналу САС идентифицирует пикосеть, в то время как ДАС используется для запросов соединения и для их откликов (paging). IAC служит для информационных запросов.

Поле «код синхронизации» (64 бита) состоит из 24-битового адреса узла – инициатора соединения (paging). Алгоритм вычисления адреса узла гарантирует невозможность перепутывания идентификаторов разных устройств даже в случае приема их с ошибками.

Поле «хвостовик» служит для обеспечения синхронизации.

Поле «заголовок» содержит 18-битовый заголовок кадра, который повторяется трижды ($18 \cdot 3 = 54$ бита). Он содержит в себе флаги подтверждения и нумерации, а также средства управления потоком.

Поле «адрес» (AM_ADDR – 3 бита – MAC-адрес) определяет один из восьми узлов, которому предназначен кадр. AM_ADDR однозначно определяет один из сетевых клиентов пикосети.

Поле «тип» (4 бита) характеризует тип передаваемого кадра, метод коррекции ошибок и число временных интервалов, из которых состоит кадр.

Бит FLOW (поток) устанавливается подчиненным узлом и уведомляет о том, что его буфер заполнен.

Бит ACK (подтверждение) указывает на подтверждение, посылаемое вместе с кадром. Если этот бит равен 1, предыдущий пакет успешно доставлен.

Бит SEQN (последовательность) служит для нумерации кадров, что помогает обнаруживать повторные передачи. Для каждого очередного пакета этот бит инвертируется. Данный протокол предполагает ожидание, поэтому одного бита оказывается достаточно.

Поле НЕС представляет собой 8-битовую контрольную сумму. Принимающая сторона анализирует все три копии заголовка, бит за битом. Значение бита определяется мажоритарной схемой (2 или 3 совпадающих бита из трех определяют истинное значение).

Кадры могут иметь длину 1, 3 или 5 тактов. Все кадры передаются между главным и подчиненным узлами по логическому каналу, называемому соединением.

5.3.4. Передача данных в беспроводной сети Bluetooth

Режимы работы беспроводной сети Bluetooth приведены в табл. 7.

Таблица 7

Режимы работы сети Bluetooth

Название режима	Описание режима
Active	В активном режиме устройство Bluetooth участвует в работе канала. Главный узел (master) диспетчеризует обмены на основе запросов трафика, поступающих от участников. Кроме того, этот режим предусматривает регулярные обмены с целью синхронизации клиентов. Активные клиенты прослушивают домены master-to-slave пакетов. Если к активному клиенту нет обращений, он может пребывать в пассивном состоянии (sleep) до очередной передачи со стороны главного узла
Sniff	Устройства, синхронизованные в рамках пикосети, могут перейти в режим экономного расходования энергии, когда их активность понижается. В режиме SNIFF устройство-клиент прослушивает пикосеть с пониженной частотой. Этот режим имеет наивысшую скважность рабочего цикла (наименьшую экономию энергии) из 3 экономичных режимов (sniff, hold и park)
Hold	Устройства, синхронизованные в рамках пикосети, могут перейти в режим экономного расходования энергии, когда их активность понижается. Главный узел пикосети может перевести клиента в режим HOLD, когда работает только внутренний таймер. Устройство-клиент может запросить перевод в режим HOLD. Передача данных возобновляется мгновенно, когда устройство выходит из режима HOLD. Клиент имеет промежуточную скважность (промежуточный уровень экономии энергии) из указанных 3 режимов (sniff, hold и park)
Park	В режиме PARK устройство еще синхронизовано в рамках пикосети, но не принимает участия в обменах. Пассивные устройства отказываются от своих MAC-адресов (AM_ADDR), прослушивают трафик главного модуля с целью ресинхронизации и отслеживают широковещательные сообщения. Данный режим имеет минимально возможную скважность (максимальную экономию энергии) из указанных 3 режимов (sniff, hold и park). Устройства, находящиеся в режиме park, должны посылать пакеты широковещательно, так как лишены собственного активного адреса

5.4. Беспроводная сеть связи GSM

В 80–90-х годах XX века весьма активное развитие получила мобильная телефония. В последнее время услуги мобильной связи стали применяться и для передачи цифровых и мультимедийных данных. Мобильные телекоммуникации используют диапазоны в интервале 50 МГц...1,8 ГГц.

5.4.1. Физическая среда передачи данных

Мобильные системы работают при малых выходных мощностях передатчика, что ограничивает размер зоны приема. Вне этой зоны другие передатчики могут функционировать независимо. Такие зоны называются сотами (ячейками). По аналогии с пчелиными сотами их часто изображают шестигранными, хотя реально они могут иметь самую причудливую форму, в зависимости от профиля местности. Ячейки должны перекрываться так, как показано на рис. 71.

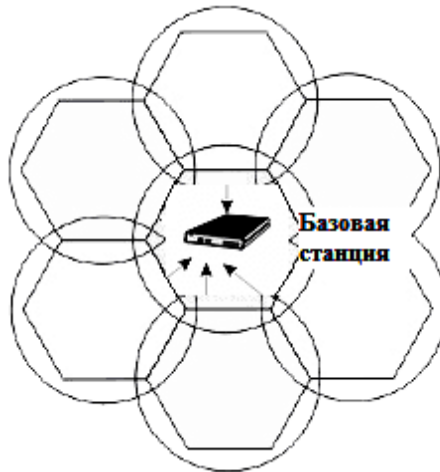


Рис. 71. Схема расположения ячеек при сотовой связи

Их перекрытие должно обеспечить перекрытие всей зоны телекоммуникаций. В центре ячейки находится базовая станция – ретранслятор. Станция содержит в себе компьютер и приемопередатчик, соединенный с антенной. Сигнал передатчика падает по мере удаления от центра ячейки, где он должен быть расположен. Там же должен находиться и приемник. В пределах ячейки предусмотрено несколько каналов для приема/передачи, разнесенных по частоте. Такие системы могут обслуживать пейджерную или мобильную телефонную сеть. Пейджерные каналы однонаправлены, а телефонные двунаправлены (рис. 72). Пейджерные системы требуют небольшой полосы пропускания, а одно сообщение редко содержит более 30 байт. Большинство современных пейджерных систем работает в частотном диапазоне 930...932 МГц.

В небольших системах все базовые станции соединены с MTSO (Mobile Telephone Switching Office). В больших сетях может потребоваться несколько MTSO, которые, в свою очередь, управляются MTSO следующего уровня, и т. д. Узловая MTSO соединена со станцией коммутируемой телефонной сети. В любой момент каждый мобильный телефон логически находится в одной определенной ячейке и управляется

одной базовой станцией. Когда телефон покидает ячейку, базовая станция обнаруживает падение уровня сигнала и запрашивает окружающие станции об уровне сигнала для данного аппарата.

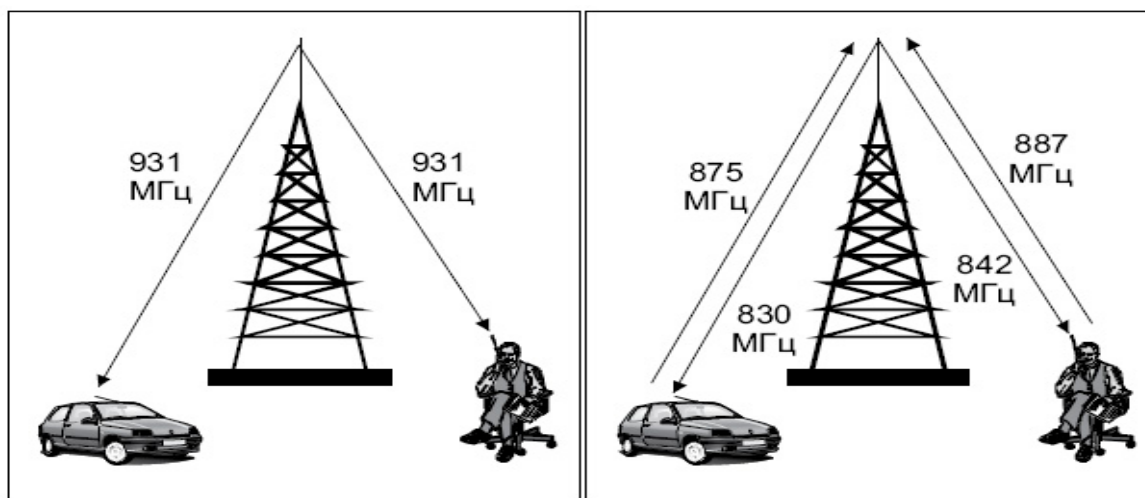


Рис. 72. Каналы пейджерной и мобильной телефонной сети

Управление аппаратом передается станции с наибольшим входным сигналом. Телефон информируется о смене управляющей станции, при этом предлагается переключиться на новый частотный канал (в смежных ячейках должны использоваться разные частотные каналы).

Эти каналы управляются центральным коммутатором ячейки (MSC – Mobile Service Switching Centre). Пользователь использует канал до тех пор, пока находится в пределах ячейки. При переходе в соседнюю ячейку он получает новый канал (hand-off), что должно быть практически незаметно для пользователя и занимает около 300 мс. Присвоением частот управляет MTSO.

5.4.2. Физический уровень

В рамках американского стандарта первого поколения AMPS (Advanced Mobile Phone Service) формируется 40 МГц-канал в интервале 800...900 МГц. Этот диапазон делится пополам, 20 МГц выделяется для передачи и столько же для приема. Данные диапазоны делятся, в свою очередь, на 666 двусторонних каналов, каждый по 30 кГц. Эти каналы расщепляются на 21 субканал, сгруппированные по 3. Обычно, как показано на рис. 71, гексагональные ячейки группируются по 7 (центральная и 6 ее соседей). Имея 666 каналов, можно выделить три набора по 31 каналу для каждой ячейки.

В случае возникновения необходимости увеличения числа каналов достаточно уменьшить размер ячейки: число ячеек увеличится и, как

следствие, увеличится число каналов на единицу площади. Это утверждение справедливо для всех систем мобильной связи. В хорошо спланированной сети плотность ячеек пропорциональна плотности пользователей.

AMPS для разделения каналов применяет метод мультиплексирования по частоте. Каждый канал AMPS может использоваться для аналоговых и цифровых коммуникаций.

Каждый мобильный телефон в AMPS имеет 32-битовый серийный номер и телефонный номер, характеризуемый 10 цифрами. Телефонный номер представляется как код зоны (3 десятичные цифры) и номер подписчика (7 десятичных цифр). Когда телефон включается, он сканирует список из 21 управляющих канала и находит тот, у которого наиболее мощный сигнал. Управляющая информация передается в цифровой форме, хотя сам голосовой сигнал является аналоговым. При нормальной работе мобильный телефон перерегистрируется в MTSO каждые 15 мин.

При осуществлении вызова пользователь набирает номер телефона и нажимает кнопку send. Аппарат посылает набранный номер и свой идентификационный код. Базовая станция принимает вызов и передает его MTSO. Если звонящий является клиентом MTSO или ее партнером, отыскивается свободный канал и мобильный телефон переключается на него, ожидая, когда адресат снимет трубку.

В режиме приема аппарат постоянно прослушивает канал пейджинга, чтобы обнаружить обращенный к нему вызов. Осуществляется обмен командными сообщениями с MTSO, после чего раздается звонок вызова.

AMPS базируется на аналоговой модуляции. В последнее время аналоговая модуляция повсеместно вытесняется цифровой.

В Европе принят единый стандарт для систем мобильной связи – GSM (Group Special Mobile, второе поколение мобильных средств связи, действует в более чем 50 странах). GSM использует диапазоны 900 и 1800 МГц. GSM имеет 200 полнодуплексных каналов на ячейку с полосой частот 200 кГц, что позволяет ей обеспечить пропускную способность 270,833 бит/с на канал. Каждый из 124 частотных каналов делится в GSM между восемью пользователями (мультиплексирование по времени). Теоретически в каждой ячейке может существовать 992 канала, на практике многие из них недоступны из-за интерференции с соседними ячейками.

Восемь выделенных на рис. 73 доменов соответствуют одному и тому же каналу (клиенту принадлежит канал 2). Четыре из них служат для связи клиента с базой, а 4 других – для связи базы с клиентом. Если мобильной станции выделена частота 890.4 и 935.4 и домен 2 желает

что-то передать базовой станции, будут задействованы нижние 4 (затененные на рисунке) домена. В них будут помещаться данные до тех пор, пока вся информация не будет передана.

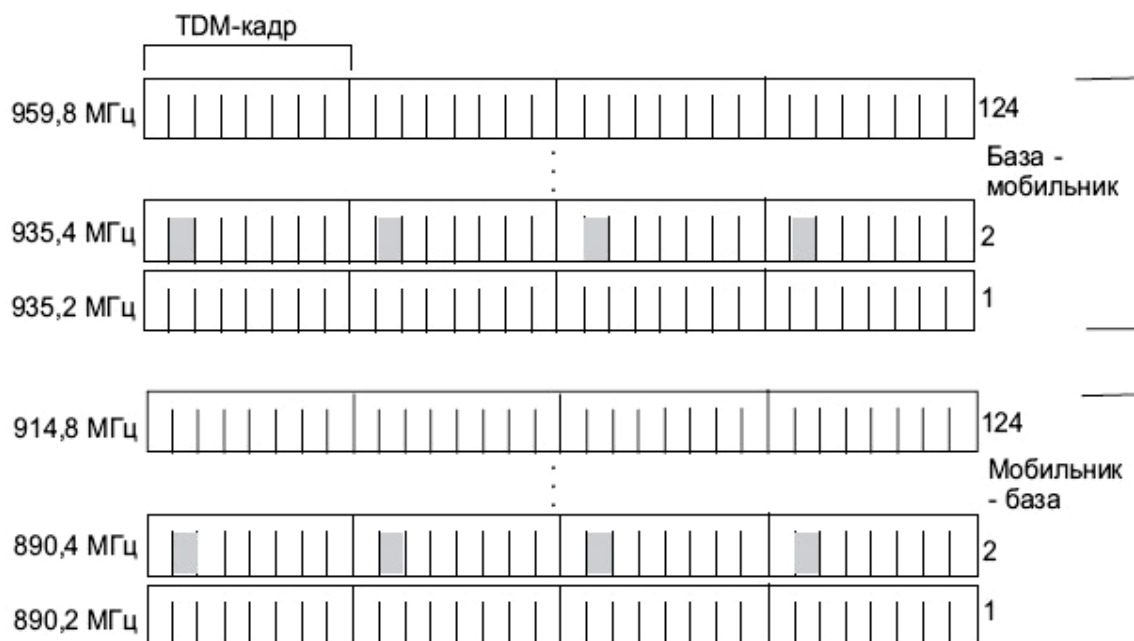


Рис. 73. Частотные каналы GSM

Сети третьего поколения 3G работают на частотах около 2 ГГц, передавая данные со скоростью 2 Мбит/с. Они позволяют организовать видеотелефонную связь, смотреть на мобильном телефоне фильмы и телепрограммы.

В мире сосуществуют два стандарта 3G: UMTS и CDMA2000. UMTS распространен в основном в Европе, CDMA2000 – в Азии и США.

Сети 3G должны обеспечивать определенные значения скорости передачи для различных степеней мобильности абонента:

- до 2,048 Мбит/с при низкой мобильности (скорость менее 3 км/ч) и локальной зоне покрытия;
- до 144 кбит/с при высокой мобильности (до 120 км/ч) и широкой зоне покрытия;
- до 64 (144) кбит/с при глобальном покрытии (спутниковая связь).

К семейству 4G, как правило, относят технологии, которые позволяют передавать данные в сотовых сетях со скоростью выше 100 Мбит/сек. В широком понимании 4G – это еще и технологии беспроводной передачи Internet-данных – Wi-Fi (скоростные варианты этого стандарта) и WiMAX (в теории скорость может превышать 1 Гбит/с). Главное отличие сетей четвертого поколения от предыдущего, третьего, заключается в том, что технология 4G полностью основана на протоколах

пакетной передачи данных, в то время как 3G соединяет в себе передачу как голосового трафика, так и пакетов данных. Пересылка данных в 4G осуществляется по протоколу IPv6 (IP версии 6).

5.4.3. Канальный уровень

Система мультиплексирования по времени имеет специфическую, иерархическую структуру. Отдельные временные домены объединяются в мультифреймы. Упрощенная схема структуры показана на рис. 74.



Рис. 74. Структура кадров в GSM

Каждый временной домен (TDM) содержит 148-битовый кадр данных, начинающийся и завершающийся последовательностью из трех нулей. Кадр имеет два 57-битовых поля данных, каждое из них имеет специальный бит, который указывает на то, что лежит в кадре – голос или данные. Между информационными полями размещается поле синхронизации (Sync). Хотя информационный кадр имеет длительность 547 мкс, передатчику позволено передавать его лишь раз в 4615 мкс, так как остальное время зарезервировано для передачи другими станциями. Если исключить накладные расходы, каждому соединению выделена полоса (без учета сжатия данных) 9,600 бит/с.

Восемь информационных кадров образуют TDM-кадр, а 26 TDM-кадров объединяются в 128-микросекундный мультифрейм. Как видно из рис. 73, позиция 12 в мультифрейме занята для целей управления, а 25-я зарезервирована для будущих применений.

5.4.4. Передача данных в беспроводной сети GSM

Алгоритм обслуживания мобильной связи достаточно сложный. Из рис. 70 видно, что области перекрываются (иначе бы существовали «мертвые» зоны без связи). Существуют даже субобласти, накрываемые тремя MSC. По этой причине процедура должна четко определить, с каким из MSC клиент должен быть связан и при каких условиях его следует переключить на соседний MSC, не прерывая связи.

Система должна также компенсировать падение сигнала, иногда достаточно резкое, чтобы обеспечить комфортную связь и безошибочную передачу информации. По этой причине частота ошибок (BER) в таких сетях составляет 10^{-3} (против 10^{-6} для обычных стационарных цифровых каналов связи).

Следует иметь в виду, что в условиях города сигнал падает пропорционально не квадрату, а четвертой степени расстояния. На распространение радиоволн в городе влияют ориентация улиц (до 20 дБ), туннели (до 30 дБ) и листва деревьев в сельской местности (до 18 дБ).

5.5. Организация связи беспроводных сетей с региональными сетями

В январе 2003 года был принят стандарт 802.16 уровня MAC (табл. 8), который предназначен для реализации широкополосных каналов последней мили в городских сетях (MAN). Его задачей является обеспечение сетевого уровня между локальными (IEEE 802.11) и региональными сетями (WAN), где планируется применение разрабатываемого стандарта IEEE 802.20. Эти стандарты совместно со стандартом IEEE 802.15 (PAN – Personal Area Network – Bluetooth) и 802.17 (мосты уровня MAC) образуют взаимосогласованную иерархию протоколов беспроводной связи.

Стандарт покрывает диапазон частот от 2 до 11 ГГц. Базовая станция (BS), следующая стандарту 802.16, размещается в здании или на вышке и осуществляет связь со станциями клиентов (SS) по схеме точка–мультиточка. Возможен сеточный режим связи, когда любые клиенты могут осуществлять связь между собой непосредственно, а антенные системы, как правило, являются всенаправленными. Базовая станция предоставляет соединение с основной сетью и радиоканалы к другим станциям. Диапазон рабочих расстояний может достигать 50 км (в случае прямой видимости) при типовом радиусе сети 7...10 км, где пропу-

ская способность может быть гарантированной. Предусмотрен также режим мультиточка–мультиточка. Клиентская станция может быть радиотерминалом или повторителем (более типично) для организации локального трафика. Схема взаимодействия радиосетей в случае использования стандарта IEEE 802.16 показана на рис. 75.

Таблица 8

Основные характеристики семейства стандарта 802.16

Название стандарта	802.16	802.16a	802.16e
Дата принятия	декабрь 2001	январь 2003	середина 2004
Частотный диапазон	10...66 ГГц	2...11 ГГц	2...6 ГГц
Быстродействие	32...135 Мбит/с для 28 МГц канала	до 75 Мбит/с для 28 МГц канала	до 15 Мбит/с для 5 МГц канала
Ширина канала	20, 25 и 28 МГц	Регулируемая 1,5...20 МГц	Регулируемая 1,5...20 МГц
Радиус действия	2...5 км	7...10 км, макс. радиус 50 км	2...5 км
Условия работы	Прямая видимость	Работа на отражениях	Работа на отражениях



Рис. 75. Применение стандарта IEEE 802.16 в системе радиокommunikаций

Трафик может проходить через несколько повторителей, прежде чем достигнет клиента. Антенны в этом случае являются направленными с возможностью дистанционной настройки. Терминальная станция клиента обычно имеет остронаправленную антенну. По этой причине положение антенны должно быть жестко фиксировано и устойчиво к ветру и другим потенциальным источникам вибрации. Широкополос-

ные системы доступа к радиосети, помимо BS и SS, содержат клиентское терминальное оборудование (TE), оборудование основной сети, межузловые каналы и повторители (RS). Повторители используются, когда между конечными точками канала нет прямой видимости. Повторитель передает сигнал от BS к одной или нескольким SS.

Канал связи предполагает наличие двух практически независимых направлений обмена: отправитель–получатель (uplink – восходящий канал) и получатель–отправитель (downlink – нисходящий канал; по аналогии со спутниковыми каналами). Эти два субканала используют разные не перекрывающиеся частотные диапазоны.

Следует отметить, что BS обычно размещаются на высоких зданиях и имеют всенаправленные антенны и это увеличивает вероятность обеспечения прямой видимости. С другой стороны, SS чаще размещаются на небольших высотах, что уменьшает вероятность гарантированной прямой видимости.

Стандартный полнодуплексный канал базовой станции может иметь пропускную способность 75 Мбит/с. Такой канал обеспечивает до 60 соединений T1 и сотни связей с домами, использующими DSL-подключения (при полосе 20 МГц). При этом гарантируются минимальные задержки, что важно при передаче голоса.

Стандарт 802.16 может решать задачи, которые возникают в каналах с асимметричным трафиком. Сейчас они часто решаются клиентами и сервис-провайдерами путем заказа выделенных линий. Внедрение нового стандарта позволит отказаться от выделенных каналов, можно будет обойтись во многих случаях исключительно беспроводными средствами.

Продвижением стандарта 802.16 занимается консорциум WiMAX (World Interoperability for Microwave Access), куда входят Fujitsu, Intel и Nokia.

Методические указания

В этом разделе рассматривались вопросы построения мобильных телекоммуникаций; при изучении необходимо усвоить следующие понятия:

- Wi-Fi – это современная беспроводная технология соединения компьютеров в локальную сеть и подключения их к Internet.
- Технология Wi-Fi ориентирована на построение беспроводных локальных сетей WLAN, сетей средних и коротких расстояний Bluetooth и сетей связи GSM.
- Сети WLAN – это сети, в которых вместо обычных проводов используются радиоволны. Для построения WLAN-сети используются Wi-Fi-адаптеры и точки доступа.

- Стандарт IEEE 802.11 является стандартом для продуктов WLAN. На практике используются три стандарта: 802.11a, 802.11b и 802.11g.

- Стандарт 802.11 определяет две основные технологии передачи данных по радиоканалу: технологию расширения спектра путем скачкообразной перестройки частоты (FHSS) в диапазоне 2,4 ГГц и технологию широкополосной модуляции с расширением спектра методом прямой последовательности (DSSS) в диапазоне 2,4 ГГц.

- В сетях WLAN на MAC-уровне выделяются два основных типа архитектуры беспроводных сетей – Ad Hoc и Infrastructure Mode. В режиме Ad Hoc станции непосредственно взаимодействуют друг с другом. В режиме Infrastructure Mode станции взаимодействуют друг с другом не напрямую, а через точку доступа.

- На MAC-уровне протокола 802.11 существуют два типа коллективного доступа к среде передачи данных: функция распределенной координации DCF и функция централизованной координации PCF.

- Передача данных с использованием функции DCF основана на методе коллективного доступа с обнаружением несущей и механизмом избежания коллизий CSMA/CA.

- Для сетей в режиме Infrastructure (с точкой доступа) применяется функция централизованной координации PCF.

- Сети средних и коротких расстояний Bluetooth базируются на стандарте 802.15.

- Основу сети Bluetooth составляют пикосети (piconet), состоящие из одного главного узла и до семи клиентских, размещенных в радиусе 10 м.

- В технологии Bluetooth кодирование сигнала осуществляется по схеме GFSK (логическому 0 и 1 соответствуют две разные частоты), передача данных выполняется с использованием алгоритма доступа TDDMA (каждый пакет передается с использованием иного частотного канала по отношению к предыдущему).

- В сетях мобильной связи GSM используется принцип сотовой ячейки, в центре которой находится базовая станция – ретранслятор.

- Второе поколение мобильных средств связи 2G имеет 200 полнодуплексных каналов на ячейку с пропускной способностью 270 Кбит/с на канал.

- Сети третьего поколения 3G работают на частотах около 2 ГГц, передавая данные со скоростью 2 Мбит/с.

- Сети четвертого поколения 4G позволяют передавать данные со скоростью выше 100 Мбит/с по протоколу IPv6.

- Стандарт 802.16 уровня MAC предназначен для реализации широкополосных каналов последней мили в городских сетях. Его задачей является обеспечение связи между сетями WLAN (IEEE 802.11), Bluetooth (IEEE 802.15) и региональными сетями.

СПИСОК ЛИТЕРАТУРЫ

1. Вейцман К. Распределенные системы линии и микро-ЭВМ: пер. с англ. – М.: Финансы и статистика, 1983. – 382 с.
2. Ганжа Д. Коммутаторы АТМ // LAN. – 1997. – № 6. – С. 21–23.
3. Гуцин В.А. Введение в FDDI // Сети. – 1994. – № 6. – С. 7–11.
4. Джамса К., Коун К. Программирование для INTERNET в среде Windows: пер. с англ. – СПб.: Питер-Пресс, 1996. – 660 с.
5. Дэвис Д. и др. Вычислительные сети и сетевые протоколы: пер. с англ. – М.: Мир, 1982. – 563 с.
6. Крол Э. Все об INTERNET: пер. с англ. – Киев: BHV, 1995. – 592 с.
7. Куо Ф. Протоколы и методы управления в сетях передачи данных: пер. с англ. – М.: Радио и связь, 1985. – 480 с.
8. Райс Л. Эксперименты с локальными сетями микро-ЭВМ: пер. с англ. – М.: Мир, 1990. – 268 с.
9. Флинт Д. Локальные сети ЭВМ: пер. с англ. – М.: Финансы и статистика, 1986. – 360 с.
10. Семенов Ю.А. Алгоритмы и протоколы каналов и сетей передачи данных [Электронный ресурс] // INTUIT.ru. – URL: <http://www.intuit.ru/department/network/algoprotnet/8/> (дата обращения: 05.05.2010).
11. Пролетарский А.В. и др. Беспроводные сети Wi-Fi [Электронный ресурс] // INTUIT.ru. – URL: <http://www.intuit.ru/department/network/wifi/> (дата обращения: 05.02.2010).
12. Леонов В. Беспроводные сети – как это работает [Электронный ресурс] // INTUIT.ru. – URL: <http://www.ferra.ru/online/networks/25619/> (дата обращения: 05.05.2010).

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ.....	3
ГЛАВА 1. ОБЩИЕ ПРИНЦИПЫ ПОСТРОЕНИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ	4
1.1. Введение в компьютерные сети	4
1.2. Многоуровневая архитектура компьютерной сети	7
1.2.1. Физический уровень	9
1.2.2. Канальный уровень.....	14
1.2.3. Сетевой уровень.....	16
1.2.4. Транспортный уровень	22
1.2.5. Сеансовый уровень	23
1.2.6. Представительный уровень	23
1.2.7. Прикладной уровень	23
1.3. Организация взаимодействия абонентов компьютерной сети	24
ГЛАВА 2. ЛОКАЛЬНЫЕ КОМПЬЮТЕРНЫЕ СЕТИ	30
2.1. Общие принципы построения локальных компьютерных сетей.....	30
2.1.1. Физическая среда передачи данных	31
2.1.2. Физический уровень.....	32
2.1.3. Канальный уровень	33
2.1.4. Верхние уровни модели IEEE 802.....	34
2.2. Локальная компьютерная сеть Ethernet	35
2.2.1. Физическая среда передачи данных	35
2.2.2. Физический уровень.....	36
2.2.3. Канальный уровень	39
2.2.4. Передача данных в локальной сети Ethernet	40
2.2.5. Перспективы развития локальной сети Ethernet.....	44
2.3. Локальная компьютерная сеть ARCNet	45
2.3.1. Физическая среда передачи данных	46
2.3.2. Физический уровень.....	46
2.3.3. Канальный уровень	46
2.3.4. Передача данных в локальной сети ARCNet	49
2.3.5. Перспективы развития локальной сети ARCNet	50
2.4. Локальная компьютерная сеть Token Ring.....	50
2.4.1. Физическая среда передачи данных	50
2.4.2. Физический уровень.....	50
2.4.3. Канальный уровень	51
2.4.4. Передача данных в локальной сети Token Ring.....	52
2.4.5. Перспективы развития локальной сети Token Ring.....	55

ГЛАВА 3. РЕГИОНАЛЬНЫЕ КОМПЬЮТЕРНЫЕ СЕТИ.....	58
3.1. Общие принципы построения региональных компьютерных сетей.....	58
3.2. Региональная компьютерная сеть FDDI	59
3.2.1. Физическая среда передачи данных	60
3.2.2. Физический уровень.....	61
3.2.3. Канальный уровень	62
3.2.4. Передача данных в региональной сети FDDI	62
3.3. Региональная компьютерная сеть ATM.....	64
3.3.1. Общие принципы технологии ATM.....	66
3.3.2. Физический уровень.....	67
3.3.3. Канальный уровень	67
3.3.4. Передача данных в региональной сети ATM	68
ГЛАВА 4. ГЛОБАЛЬНЫЕ КОМПЬЮТЕРНЫЕ СЕТИ.....	73
4.1. Общие принципы построения глобальных компьютерных сетей.....	73
4.2. Принципы построения сетей X.25.....	79
4.2.1. Канальный уровень	79
4.2.2. Сетевой уровень	81
4.2.3. Передача данных в глобальной сети X.25.....	82
4.2.4. Перспективы развития сетей X.25. Сети Frame Relay	83
4.3. Принципы построения сетей TCP/IP. Глобальная сеть Internet	84
4.3.1. Физический уровень сети Internet	85
4.3.2. Канальный уровень сети Internet.....	85
4.3.3. Сетевой уровень сети Internet.....	88
4.3.4. Транспортный уровень сети Internet	103
4.3.5. Прикладной уровень сети Internet. Сервисы Internet.....	107
ГЛАВА 5. МОБИЛЬНЫЕ ТЕЛЕКОММУНИКАЦИИ	111
5.1. Введение в мобильные телекоммуникации	111
5.2. Беспроводная сеть WLAN	112
5.2.1. Физическая среда передачи данных	113
5.2.2. Физический уровень.....	115
5.2.3. Канальный уровень	121
5.2.4. Передача данных в беспроводной сети WLAN	122
5.3. Беспроводная сеть Bluetooth	133
5.3.1. Физическая среда передачи данных	133
5.3.2. Физический уровень.....	135
5.3.3. Канальный уровень	135
5.3.4. Передача данных в беспроводной сети Bluetooth.....	137

5.4. Беспроводная сеть связи GSM	137
5.4.1. Физическая среда передачи данных	138
5.4.2. Физический уровень.....	139
5.4.3. Канальный уровень	142
5.4.4. Передача данных в беспроводной сети GSM	143
5.5. Организация связи беспроводных сетей с региональными сетями....	143
СПИСОК ЛИТЕРАТУРЫ.....	147

Учебное издание

КОМАГОРОВ Владимир Петрович

АРХИТЕКТУРА СЕТЕЙ И СИСТЕМ ТЕЛЕКОММУНИКАЦИЙ

Учебное пособие

Научный редактор
*доктор технических наук,
профессор В.А. Силич*

Выпускающий редактор *Т.С. Савенкова*

Редактор *Е.А. Тетерина*

Компьютерная верстка *В.П. Комагоров, В.П. Аршинова*

Дизайн обложки *П.Е. Шырыкалова*

Подписано к печати 16.05.2012. Формат 60×84/16. Бумага «Снегурочка».

Печать XEROX. Усл. печ. л. 8,84. Уч.-изд. л. 8,0.


Заказ 640-12. Тираж 100 экз.



Национальный исследовательский Томский политехнический университет
Система менеджмента качества

Издательства Томского политехнического университета сертифицирована
NATIONAL QUALITY ASSURANCE по стандарту BS EN ISO 9001:2008



ИЗДАТЕЛЬСТВО  ТПУ. 634050, г. Томск, пр. Ленина, 30
Тел/факс: +7 (3822) 56-35-35, www.tpu.ru