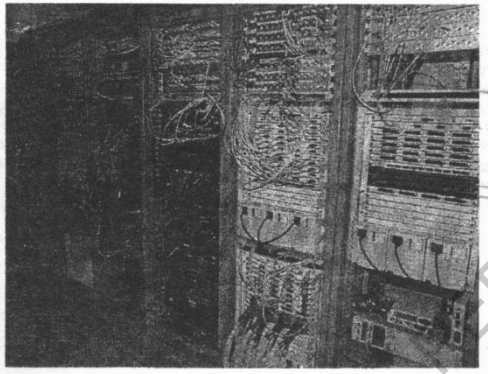
Министерство образования Республики Беларусь

Учреждение образования
«Гомельский государственный университет
имени Франциска Скорины»

АППАРАТНОЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ СЕТЕЙ

Допущено Министерством образования Республики Беларусь
в качестве учебного пособия
для студентов высших учебных заведений
по специальности
«Автоматизированные системы обработки информации»



Гомель
УО «ГГУ им. Ф. Скорины»
2009

УДК 004.7 : 004.3 : 004.4 (075.8)
ББК 32.973.202 – 018.2 – 04 я73
А 769

Авторы: Демиденко О. М., Воруев А. В., Кучеров А. И., Кулинченко В. Н.

Рецензенты:
В. П. Загорский, доцент, канд. техн. наук, доцент каф. «Робототехнические системы» УО «БНТУ»; каф. ИТАС УО «БГУИР»

Рекомендовано научно-методическим советом учреждения образования «Гомельский государственный университет имени Франциска Скорины»

А 769 **Аппаратное и программное обеспечение сетей**: учебное пособие для студентов вузов по специальности «Автоматизированные системы обработки информации» / О. М. Демиденко [и др.]; М-во образования РБ, Гомельский государственный университет имени Франциска Скорины. – Гомель : ГГУ им. Ф. Скорины, 2009. – 232 с.
ISBN 978–985–439–404–6

В книге приведен материал о происхождении современных сетевых структур, рассмотрены модели описания сетей и сетевые протоколы; описаны структуры вычислительных сетей, виды сред передачи данных и их свойств; разъясняются методы доступа к среде, принципы работы активного оборудования сетей, описаны технологии локальных сетей. Изложены вопросы: организации адресации в компьютерных сетях и поиска маршрута в сетевой среде; организации управления компонентами сети; работы со средами сетевых операционных систем; кратко описаны методы сетевого мониторинга и сетевой диагностики.

Адресована студентам вузов специальности «АСОИ».

УДК 004.7 : 004.3 : 004.4 (075.8)
ББК 32.973.202 – 018.2 – 04 я73

ISBN 978–985–439–404–6

Содержание

Введение

Содержание предлагаемого учебного пособия соответствует содержанию лекционного курса «Аппаратное и программное обеспечение сетей» учебного плана студентов специальности I-53 01 02 – «Автоматизированные системы обработки информации» (Образовательный стандарт: РД РБ 02100.5.111-98).

В пособии излагаются основные принципы построения компьютерных сетей, теоретические основы современных сетевых технологий, принципы построения логической и физической структуры сетей, виды и свойства сред передачи информационных сигналов, виды и свойства сетевого оборудования, эталонная модель взаимодействия открытых систем, методы доступа к среде передачи, сетевые протоколы, интерфейсы и службы, общие понятия системного администрирования и защиты данных.

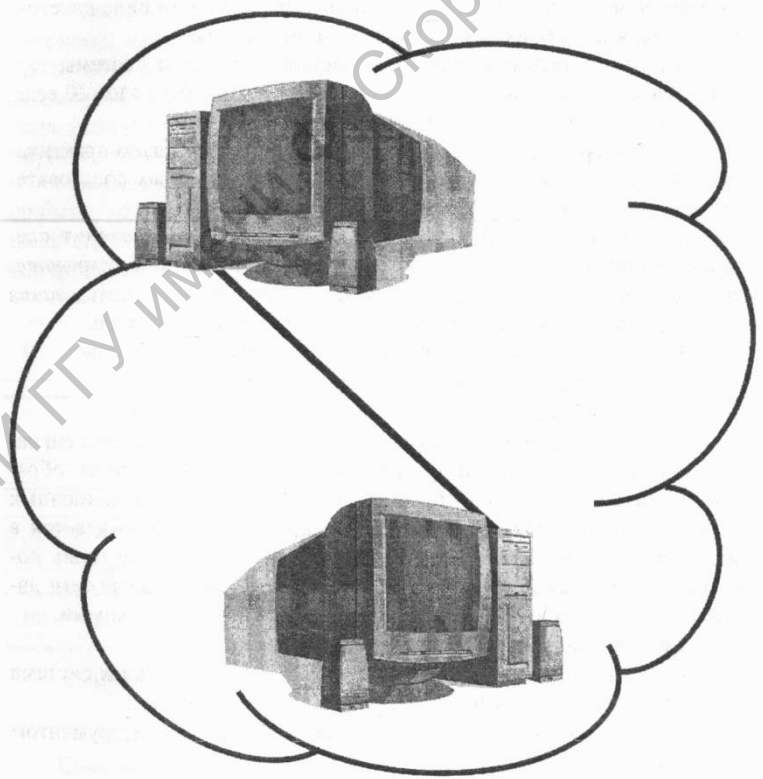
Материал изложен в виде кратких ответов на вопросы учебной дисциплины, снабжен необходимым иллюстративным материалом и рекомендуется к использованию при подготовке к контрольным мероприятиям.

Для успешного усвоения изложенного материала учащийся должен иметь необходимый базовый набор знаний по архитектуре современных вычислительных систем и принципах работы современных операционных систем.

Для более глубокого изучения вопросов, затрагиваемых в пособии, необходимо изучение специализированной литературы.

В словаре терминов определяются используемые в книге наиболее распространенные термины и сокращения, применяемые в сфере коммуникационных технологий. Словарь размещен в конце учебного пособия.

1 Введение в компьютерные сети



1.2 Локальные вычислительные сети

Локальная вычислительная сеть (*Local Area Network – LAN*) – это структура, объединяющая компьютеры, сосредоточенные на небольшой территории. Обычно радиус удаления не превышает 1–2 км, хотя в отдельных случаях локальная сеть может иметь и более протяженные размеры. В общем случае локальная сеть представляет собой коммуникационную систему, принадлежащую одной организации.

Функциональное назначение сети, или спектр решаемых ею задач, узко направлено. Например, использование файлов, хранящихся на дисках других компьютеров сети, совместное использование устройств печати, модемов, факсов, доступ к единым базам данных, внутренняя электронная почта и др.

Локальная сеть может применяться для управления производственным процессом конкретного предприятия. Причем эти задачи могут начинаться с обычного документооборота и заканчиваться удаленным управлением любыми технологическими процессами.

Более сложные задачи предъявляют высокие требования к надежности процесса передачи информации. Например, такая функция, как распределенная обработка данных, требует наличия механизма установления однозначной последовательности выполняемых действий, т. е. необходимо решение задачи синхронизации в распределенной системе, что далеко не просто.

Однако, большинство локальных сетей ориентированы на решение простых пользовательских задач. В таких случаях каждая рабочая станция или узел сети, как правило, автономно обладает необходимыми ресурсами для решения поставленных перед нею задач, а ресурсы локальной сети необходимы для получения задания и отправки результатов, хранения больших объемов данных, совместного использования дорогостоящих устройств. Схема такой сети приведена на рисунке 1.2.

Примерный жизненный цикл локальной сети можно разбить на шесть этапов (таблица 1.1), каждый из которых включает в себя набор инженерных задач.

Этапы 3–5 этого цикла должны регулярно повторяться. В противном случае либо сеть перестанет соответствовать современным стандартам, либо начнется процесс ее саморазрушения.

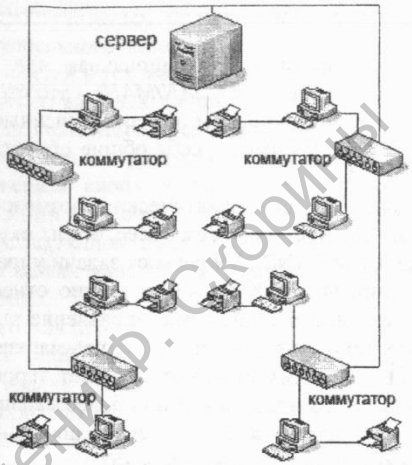


Рисунок 1.2 – Пример схемы локальной вычислительной сети

Таблица 1.1 – Примерный жизненный цикл локальной сети

№	Этап	Содержание работ по этапу
1	Разработка проекта	– предпроектное обследование объекта; – составление, оформление и согласование технического задания; – выбор необходимой конфигурации серверов и рабочих мест для использования их в составе информационной системы компьютерной сети; – выбор необходимого сетевого оборудования; – подготовка полного проекта сети в соответствии с требованиями заказчика.
2	Монтаж	– выполнение проекта, монтаж структурированной кабельной системы; – установка и настройка активного сетевого оборудования; – установка и настройка сетевого программного обеспечения на серверы и рабочие места; – установка систем защиты информации от несанкционированного доступа.
3	Тестирование	– проведение анализа работы сети для определения «узких мест» и их устранение; – анализ информационной безопасности сети; – проверка систем защиты информации от несанкционированного доступа; – проверка работы активного сетевого оборудования.
4	Обслуживание	– построение систем резервного копирования информационных ресурсов предприятия; – формирование политики безопасности предприятия, реализация систем разграничения доступа к информационным ресурсам; – проведение обучения персонала по использованию локальной сети на рабочих местах; – гарантийное и послегарантийное обслуживание элементов сети.
5	Модернизация	– установка сетевых операционных систем нового поколения; – установка дополнительного прикладного программного обеспечения; – установка дополнительных или более новых версий систем управления и мониторинга сетей; – обновление системы защиты информации от несанкционированного доступа; – расширение возможностей использования современных технологий, в частности, системы электронного документооборота, сетевых баз данных, приема/передачи факсов, досгупа в Internet.
6	Демонтаж	– уведомление пользователей с последующим отключением их от сети; – отключение доступа к сетевым ресурсам; – демонтаж и утилизация активного оборудования; – демонтаж и утилизация элементов структурированной кабельной системы.

1.3 Городские сети

Местная, региональная, муниципальная или городская сеть (*Site/Metropolitan Area Network – SAN/MAN*) – это структура, объединяющая вычислительные системы, рассредоточенные по территории одного региона, включающего в себя общие объекты или субъекты управления.

Такие крупные системы практически невозможно разработать и внедрить одному собственнику, тем более, что их окупаемость достаточно невелика. Сети SAN/MAN решают задачи управления хозяйством и организации услуг. К их числу можно отнести: расписание движения общественного транспорта, управление рынком вакансий, функцию информирования населения, Internet–магазины и т. п.

Современная сеть SAN/MAN охватывает территорию диаметром около 40–50 км, обладает двумя или более маршрутами доставки сообщения между узлами сети, применяет широкий спектр современного коммуникационного оборудования.

Можно утверждать, что чаще всего сети SAN/MAN – это пример сообщества, состоящего из более мелких сетей: локальных, частных, домашних, а также вычислительных систем отдельных пользователей. Способы их объединения могут быть различными, основываться на применении различных типов передающих сред и иметь различные источники финансирования. Тем не менее, мотив объединения всегда один – ускорение и удешевление информационного обмена и доступа к сетевым услугам.

К числу популярных пользовательских сервисов (кроме упомянутых ранее), которые можно организовать только в сетях такого масштаба, можно добавить следующие: организация оперативного документооборота между предприятиями, организациями и частными лицами; организация безналичного расчета посредством использования кредитных карт; наконец, желание пользователей получить доступ к сфере развлечения, в том числе цифровому телевидению и компьютерным играм.

Следует заметить, что качество и количество технологий, применяемых для организации связи между сетями, непрерывно растет. Одновременно меняются требования к надежности и безопасности передаваемой информации. Таким образом, сети SAN/MAN сегодняшнего дня сильно отличаются от своих предшественников и самые современные из них вскоре могут потребовать серьезной модернизации.

Самым распространенным примером муниципальной сети являются системы кабельного телевидения. Они стали правопреемниками эфирных телесетей в тех местах, где качество передачи сигнала посредством радиосигнала было слишком низким.

Вначале стали появляться специализированные, разработанные прямо на объектах сетевые структуры. Затем компании-разработчики занялись продвижением своих систем на рынок, начали заключать договора с городскими органами управления и в итоге охватили целые территории. Следующим шагом стало создание телевизионных программ и даже целых каналов, предназначенных только для кабельного телевидения.

Когда Internet стал привлекать к себе массовую аудиторию, операторы кабельного телевидения поняли, что, внеся небольшие изменения в систему, можно сделать так, чтобы по тем же каналам в неиспользуемой части спектра передавались (причем в обе стороны) цифровые данные. С этого момента кабельное телевидение стало постепенно превращаться в муниципальную компьютерную сеть. В первом приближении систему SAN/MAN можно представить себе такой, как она изображена на рисунке 1.3. На этом рисунке видно, что по одним и тем же линиям передается и телевизионный, и цифровой сигналы.

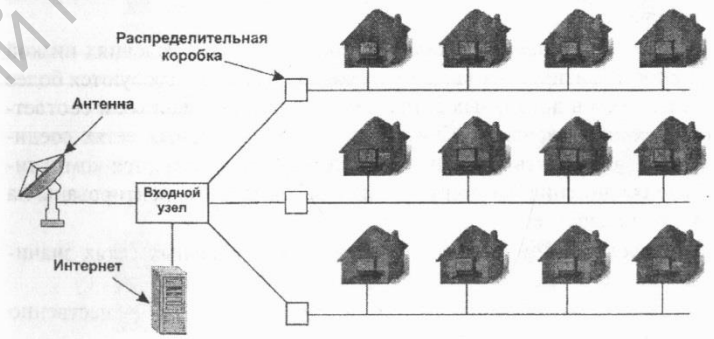


Рисунок 1.3 – Муниципальная сеть на базе кабельного ТВ

Поскольку городская территория разделяется на сферы обслуживания между несколькими провайдерами – большую роль в организации согласованной работы сети SAN/MAN играют органы местного управления.

1.4 Глобальные вычислительные сети

Глобальная вычислительная сеть (*Global/World Area Network – GAN/WAN*) – охватывает максимальную территорию. Теоретически эта сеть может объединить все вычислительные системы на земном шаре для решения одной общей задачи. При этом созданные системы управления такой сетью уже сама по себе весьма сложная задача.

По этому признаку глобальные сети можно разделить на распределенные и централизованные. Централизованные лучше защищены от несанкционированных акций, распределенные же отличаются большей надежностью при передаче данных, а также большей живучестью.

Глобальные сети решают задачи управления хозяйством в наиболее крупном размере, например, расписание движения международного транспорта, предварительный заказ билетов, бронирование мест в гостиницах, Internet-магазины и т. п. (рисунок 1.4)

Свойства глобальных сетей удобнее рассматривать в сравнении их с локальными вычислительными сетями:

– *по протяженности и качеству линий связи* локальные сети, по определению, отличаются от глобальных небольшими расстояниями между узлами сети. Это в принципе делает возможным использование в локальных сетях более качественных и более дорогих линий связи;

– *по сложности методов передачи данных* в условиях низкой надежности физических каналов в глобальных сетях требуются более сложные, чем в локальных сетях методы передачи данных и соответствующее оборудование. Считается, что в глобальных сетях соединения не могут быть постоянными. Нередко используются коммутируемые соединения, да и другие виды соединений ориентированы на временный характер;

– *число информационных ресурсов* в глобальных сетях значительно больше;

– *скорость обмена данными* в локальных сетях, существенно выше, чем в глобальных;

– высокие скорости обмена данными позволяют предоставлять пользователю в локальных сетях более *широкий спектр услуг.*

Глобальные сети нередко используются сетями меньшего масштаба для организации связи между собой и/или организации удаленного доступа отдельных клиентов (рисунок 1.5).

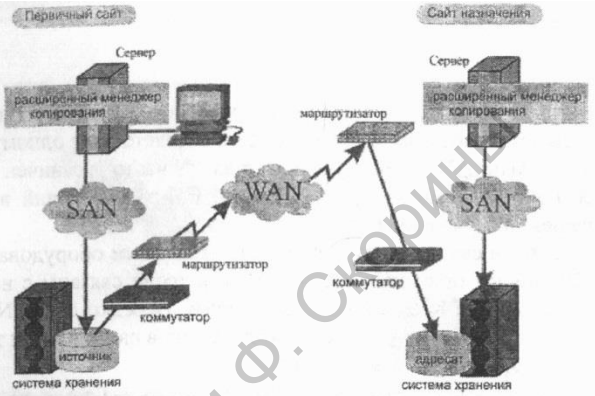


Рисунок 1.4 – Обмен данными между сетями с использованием структуры WAN

Рисунок 1.5 – Взаимодействие разноуровневых типов сетей

1.5 Частные сети

Сферу действия частной сети (*Private Network – PN*) можно ограничить сферой деятельности частного провайдера. Территориальный охват и ответственность сети PN чаще всего соответствует одному сегменту сети SAN/MAN. Спектр услуг в сетях PN часто ограничен организацией почтового обмена, ретрансляцией FM-радиостанций и предоставлением доступа в Internet.

Технологии связи между узлами и центральным оборудованием в сетях PN имеют оригинальный характер и тесно связаны с начислением платежей за предоставляемые услуги. Нередко сеть PN возникает на основе существующей системы каналов связи. Среди таких примеров часто встречаются следующие:

– *сети на основе каналов кабельного телевидения* – доставка информации конечному пользователю производится так же, как и доставка телевизионного сигнала (рисунок 1.6). Адаптер пользователя декодирует смешанный сигнал, выделяет информационную составляющую, транслируемую как обычный телевизионный канал посредством *мультиплексирования*. Скорость трансляции от 384 Кбит/с до 1,5 Мбит/с, если запросы пользователя передаются провайдеру стандартным способом, например, через модем. Скорость доступа 56 Кбит/с. Если используется кабель с двусторонней трансляцией, то пользователь может получить 1,5 Мбит/с в обе стороны. Пример технологии – сети *Community Antenna TeleVision – CATV*;

– *сети на основе систем энергоснабжения* – перспективная система доставки информации. Поскольку электросеть проникает в каждую комнату любого дома, то компьютер пользователя получает достаточный уровень мобильности. Для передачи сигнала через электросеть используется мультиплексирование OFDM. Существующие образцы позволяют организовать сетевое подключение от 14 до 85 Мбит/с на удалении узлов сети до 2 000 м (рисунок 1.7);

– *сети сотовых операторов* – сотовые системы используют три различных метода мультиплексирования голосовых и информационных данных на арендуемом диапазоне радиочастот: FDMA, TDMA и CDMA. Скорость обслуживания сетевых запросов колеблется от 9,6 Кбит/с до 76,8 Кбит/с (для TDMA) и от 100 Кбит/с до 2 Мбит/с (для CDMA);

– *хаотически возникшие пользовательские сетевые сегменты* на базе технологий локальных вычислительных сетей.

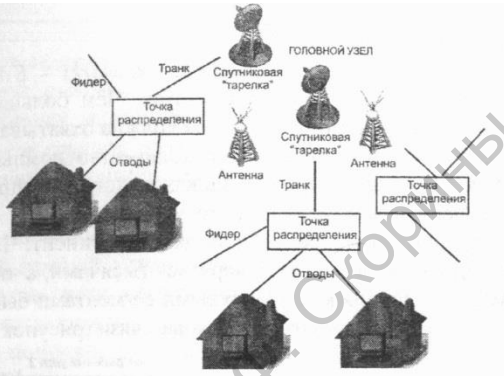


Рисунок 1.6 – Сеть каналов частной беспроводной сети

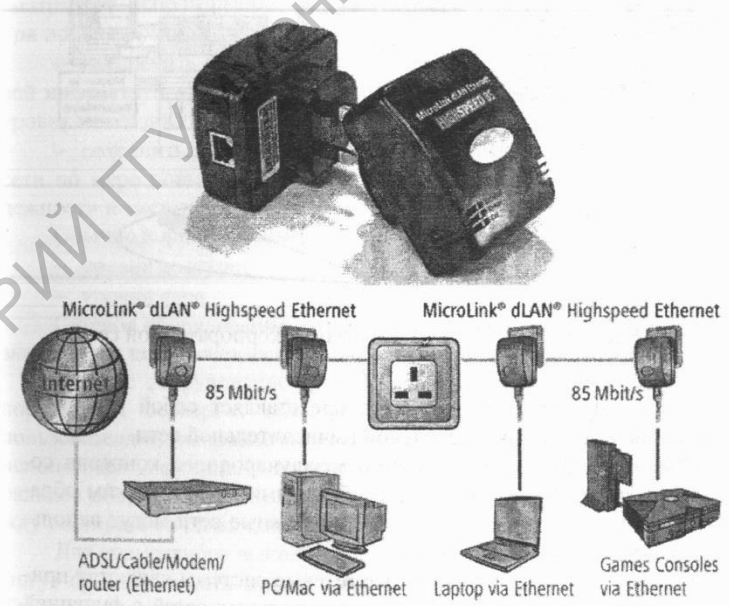


Рисунок 1.7 – Оборудование сетей на основе сетей энергопотребления

1.6 Корпоративные сети

Корпоративную сеть (*Enterprise Wide Networks – EWN*) можно определить как сеть масштаба предприятия. Чем больше масштаб предприятия – тем большее пространство должна охватывать сеть.

Такие сети объединяют большое количество компьютеров во всех офисах и промышленных площадках одного предприятия или организации. Сегменты такой сети могут быть сложно связаны и способны покрывать город, регион или даже континент. Число пользователей и компьютеров может измеряться тысячами, а число серверов – сотнями. Расстояния между сетевыми сегментами бывают такими, что приходится использовать глобальные связи (рисунок 1.8).

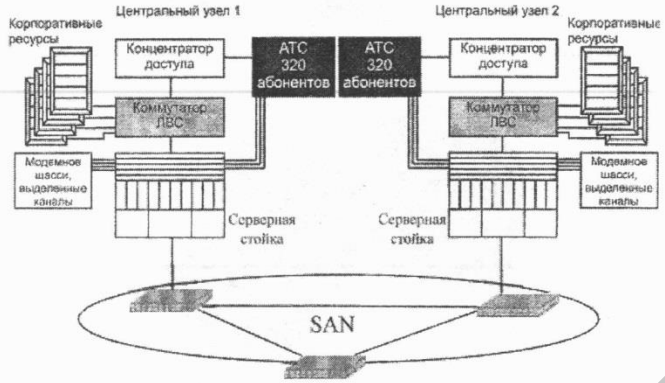


Рисунок 1.8 – Пример реализации корпоративной сети

Логически корпоративная сеть представляет собой структуру управления, аналогичную локальной вычислительной сети.

Физически корпоративная сеть международного концерна сопоставима по масштабу охвата с глобальными сетями. Таким образом, для выполнения своих задач корпоративные сети могут использовать каналы связи других сетей.

Самые простые корпоративные сетевые системы являются примерами расширенных локальных вычислительных сетей с функцией удаленного доступа к сетевым ресурсам пользователями данной сети, подключающимися, например, с домашнего компьютера (SOHO-клиент).

Для корпоративной сети характерны:

– *масштабность* – тысячи пользовательских компьютеров, сотни серверов, огромные объемы хранимых и передаваемых по линиям связи данных, множество разнообразных приложений;

– *высокая степень гетерогенности* – различные типы компьютеров, коммуникационного оборудования, операционных систем и приложений;

– *использование глобальных связей*.

Главной задачей корпоративной сети при использовании публичных каналов связи является обеспечение защиты передаваемых данных от несанкционированного доступа. Рекомендуется решать эту задачу с помощью схем шифрования. Для этого разработан широкий спектр аппаратных средств и программных решений.

Типовое решение по построению корпоративной сети предусматривает использование иерархического подхода. Такой подход при проектировании сетевой структуры позволяет:

– обеспечить высокую отказоустойчивость и целостность сетевой инфраструктуры в случае выхода из строя единичных устройств уровня точки доступа или магистрали здания;

– сохранить вложенные инвестиции при дальнейшем развитии сети по мере повышения требований к ее производительности, надежности и масштабируемости.

Обычно корпоративные сети строятся на базе двух уровней:

– уровня доступа;

– уровня ядра.

Сетевое оборудование, относящееся к уровню доступа, предназначено для подключения пользователей к корпоративной сети.

Сетевое оборудование уровня ядра обеспечивает доступ к корпоративным серверам, высокоскоростное взаимодействие между пользователями, направление потоков данных по назначению за счет использования функций маршрутизации. Здесь же находится магистральное оборудование, которое обеспечивает пересылку данных между главными точками концентрации трафика в сети.

Для совместного выполнения каких-либо проектов организации могут организовывать многоуровневое взаимодействие своих сетей. Такое объединение корпоративных сетей, взаимодействующих друг с другом посредством Internet, называется *extranet* (экстрасеть).

1.7 Домашние сети

Домашняя сеть (*Home Network – HN*) – явление довольно новое и на данный момент слабо формализованное. Роль сетей HN бывает разной и для сетей, в состав которых они входят, и для пользователей.

Так для корпоративной сети внешняя домашняя сеть может стать дополнительным сегментом.

Для частной сети провайдера – объектом, нуждающимся в предоставлении дополнительного сетевого оборудования, необходимого для обеспечения связи между HN и корпоративной сетью.

Для пользователя – в зависимости от характера его требований и квалификации, домашняя сеть может выполнять функции:

– рабочего места служащего компании (SOHO-клиент);

– системы управления домашним хозяйством («умный дом»);

– инструментом доступа к внешним источникам информации и материальных ценностей (посредством сети Internet);

– центром развлечений и т. д.

Тем не менее, для сетей HN характерны те же признаки, что и для вышеописанных типов:

– как правило, сеть HN предназначена для решения фиксированного спектра задач, практически неизменных в течение долгого времени;

– каждый узел имеет своего собственного владельца, а сетевая инфраструктура общая или принадлежит провайдеру.

Быстрый рост числа домашних сетей в последнее время можно объяснить следующими фактами:

– быстрый рост производительности вычислительных систем при параллельном снижении цен позволяет одному пользователю приобрести в личное владение достаточное количество вычислительной техники для решения поставленных задач;

– морально устаревшее оборудование обесценивается настолько, что часть пользователей, обновляя компьютер, оставляют старый комплект, для решения вспомогательных задач;

– технологии разработки и использования распределенных вычислений стали доступными для применения обычным пользователям;

– при разработке бытовых устройств последнего поколения особое внимание уделяется вопросам их подключения к различным информационным системам.

Например, в 1998 г. компания Samsung Electronics представила технологию построения домашних сетей *Home Wide Web (HWW)*. Согласно спецификации HWW, с помощью интерфейса IEEE 1394 (рисунок 1.9) в единую сеть объединяются компьютерные системы, бытовая электронная аппаратура, устройства коммуникаций, охранные системы, противопожарное оборудование и т. п. Обмен данными в сети происходит по протоколу IP. Графический пользовательский интерфейс выполнен в соответствии со спецификацией HTML.

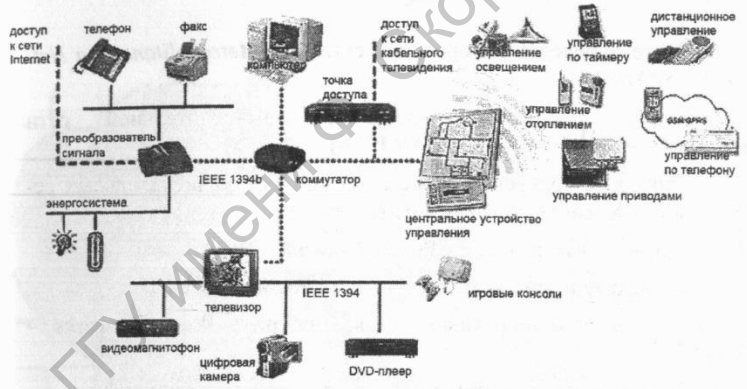


Рисунок 1.9 – Один из вариантов совмещения информационных потоков по технологии FireWire

На этом рисунке представлены основные устройства расширенной сети управления домашним хозяйством и шины, к которым они подключены, а также дополнительные функции, на решение которых направлена эта сеть (справа от центрального устройства управления).

Сейчас для выполнения подобных задач все больше используется беспроводная технология WiFi. Эффективность применения мобильных решений при подключении к домашней сети бытовых устройств обусловило быстрый рост числа их видов. Единственным сдерживающим фактором можно считать отсутствие единого стандарта беспроводной связи, поддержанного всеми производителями.

Остается ожидать, что в ближайшие годы именно расширение возможностей домашних компьютерных сетей создаст условия для интенсивного развития новых технологий в сфере применения вычислительных сетей.

Вопросы для самоконтроля

1 Дайте определение информационной сети и сети обработки данных.

2 Приведите примеры классификаций компьютерных сетей.

3 Дайте определение локальной вычислительной сети.

4 Приведите пример примерного жизненного цикла локальной сети.

5 Дайте определение городской сети (*Site/Metropolitan Area Network – SAN/MAN*).

6 Дайте определение глобальной вычислительной сети (*Global/World Area Network - GAN/WAN*).

7 Проведите сравнение свойств глобальных вычислительных сетей с локальными вычислительными сетями.

8 Что такое частные сети (Private Network – PN)?

9 Приведите примеры классификации частных сетей.

10 Что такое корпоративная сеть (Enterprise Wide Networks – EWN)?

11 Какими характеристиками обладает корпоративная сеть?

12 Какова главная задача корпоративной сети?

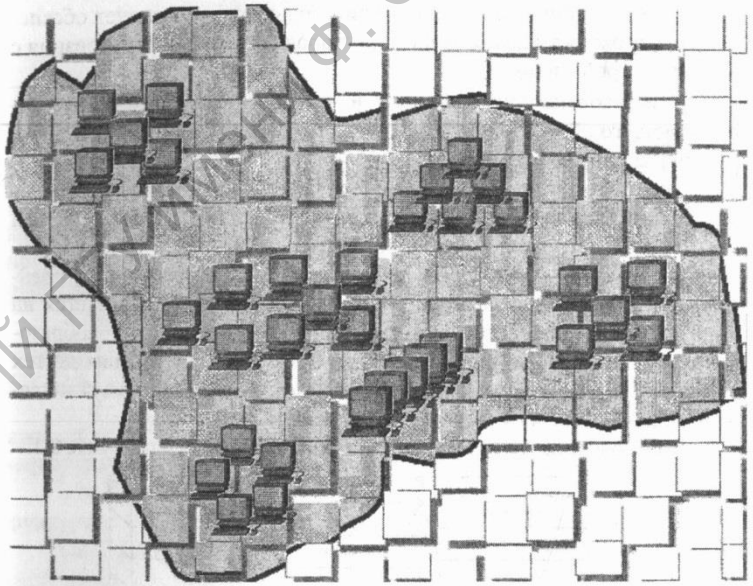
13 Как и на основе какого подхода строятся типовые структуры корпоративных сетей?

14 Сформулируйте определение домашней сети (Home Network – HN).

15 Какие функции выполняет домашняя сеть с точки зрения провайдера и пользователя?

16 Какими факторами обусловлен быстрый рост домашних сетей в последнее время?

2 Модели описания сетей и сетевые протоколы



2.1 Теоретические модели описания сетевого взаимодействия

Сетевая модель – теоретическое описание принципов работы набора сетевых протоколов, взаимодействующих друг с другом.

Применение сетевых моделей позволяет решать следующий ряд вопросов:

– обеспечение передачи информации между различными типами локальных и глобальных сетей;

– стандартизация сетевого оборудования, что позволяет устройствам одного производителя взаимодействовать с устройствами других производителей;

– сохранение капиталовложений пользователей за счет обеспечения возможности взаимодействия старого сетевого оборудования с новыми устройствами;

– разработка программного и аппаратного обеспечения, использующего общие интерфейсы для передачи как внутри сети, так и между различными сетями.

Чаще других применяется модель OSI, разработанная в 1974 году Международной организацией стандартизации ISO. Модель OSI состоит из семи уровней, расположенных один поверх другого: *физического, канального, сетевого, транспортного, сеансового, представительского, прикладного*. Передача информации начинается на прикладном уровне. Затем информация претерпевает ряд преобразований и определенных приращений на более нижних уровнях до тех пор, пока данные не достигнут физического уровня и не будут по сети переданы второму участнику соединения – приемнику.

Взаимодействие между уровнями OSI изображено на рисунке 2.1.

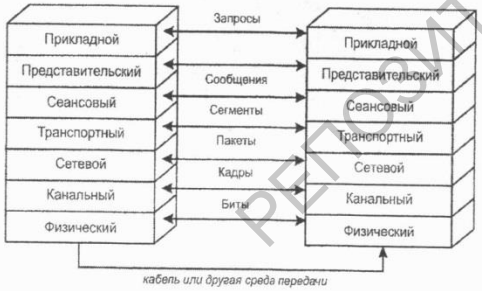


Рисунок 2.1 – Модель взаимодействия уровней в OSI

Модель DoD разрабатывалась вместе с протоколом TCP/IP как часть проекта ARPAnet [5]. Это достаточно простая модель. Она содержит всего четыре уровня (рисунок 2.2).

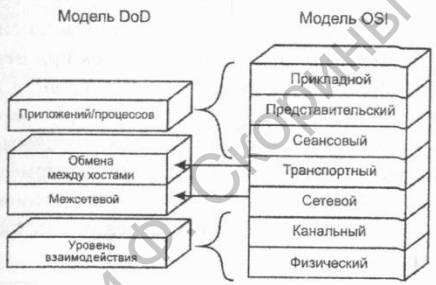


Рисунок 2.2 – Соответствие уровней модели DoD уровням модели OSI

Уровни модели DoD выполняют описанные ниже функции:

– *уровень приложений/процессов*– верхний уровень модели DoD выполняет функции трех верхних уровней модели OSI: прикладного, представления и сеансового. В источниках по TCP/IP можно встретить утверждение, что уровень приложений шифрует данные, создает точки проверки и управляет сеансом связи;

– *уровень взаимодействия* – во многих источниках, включая четырехуровневые диаграммы DoD, этот уровень называется так же, как соответствующий ему уровень модели OSI — транспортный;

– *межсетевой уровень* – этот уровень довольно точно соответствует сетевому уровню модели OSI. На межсетевом уровне выполняется маршрутизация сигнала на основе логических цифровых адресов;

– *уровень сетевого интерфейса* –этот уровень выполняет функции канального и транспортного уровней модели OSI. [5]

Считается, что модель протокола TCP/IP совпадает с теоретической основой модели DoD. На самом деле они описаны в разных стандартах. Для модели DoD – RFC 760 «DoD standard internet protocol» (январь 1980), а для TCP/IP – RFC 1180 «A TCP/IP Tutorial» (январь 1991). При этом следует учитывать, что ранее 1991 года уже существовали стандарты RFC, описывающие части стека протоколов TCP/IP, поскольку они являлись частью сетей стандарта DoD.

Далее в пособии будут использоваться обе эти модели при описании свойств оборудования и программных систем, участвующих в сетевом обмене.

2.2 Физический и канальный уровни модели OSI

Физический уровень описывает: все физические среды передачи данных (кабель, оптоволокно, радиоволны и др.), сетевые разъемы, компоновку сети, методы передачи и кодирования сигналов, устройства передачи, методы распознавания ошибок при передаче сигналов [2,5]. Сетевые сигналы могут быть представлены в аналоговом или цифровом (дискретном) виде. Аналоговый сигнал может изменяться непрерывно и выглядит как волна с положительными и отрицательными перепадами напряжения. В дискретной форме для представления единиц и нулей используются различные способы представления сигналов. Некоторые формы представления дискретных сигналов представлены на рисунке 2.3.

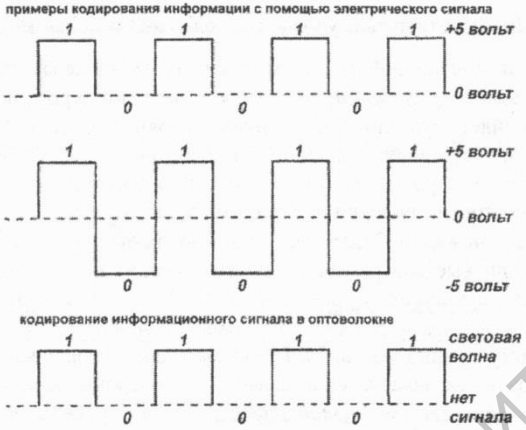


Рисунок 2.3 – Примеры цифровых сигналов

Физический уровень управляет скоростью передачи данных, анализом потока ошибок и уровнями напряжения сигнала.

Задача *канального уровня* в локальной сети [2,4] – компоновать передаваемые биты данных в виде фреймов (*frame – кадр*). Каждый фрейм должен быть сформирован таким образом, чтобы после передачи данных от узла к узлу их можно было бы собрать в исходном порядке. Этот уровень кодирует данные в виде фреймов, после чего отформатированные фреймы поступают на физический уровень, где передающий узел может отправить их в коммуникационную среду.

Принимающий узел получает фрейм от физического уровня, декодирует электрический сигнал, преобразует его во фрейм и проверяет наличие ошибок во фрейме. Фрейм может иметь структуру, указанную на рисунке 2.4.

Рисунок 2.4 – Формирование кадра данных согласно модели OSI

Канальный уровень содержит два подуровня [5]: более высокий – управление логическим каналом (LLC) и более низкий – протокол управления доступом к передающей среде (MAC). Подуровень LLC обеспечивает надежность коммуникаций путем установки канала передачи данных между двумя узлами и поддержку устойчивости этого канала. Подуровень MAC распознает физический адрес, содержащийся в каждом фрейме. Он управляет совместной работой множества устройств внутри одной сети.

Два типа сервисов используются для взаимодействия подуровня LLC и сетевого уровня. Первый тип представлен службой без установки соединения, которая не требует наличия логического соединения между передающим и принимающим узлами. В этом случае не выполняется проверка очередности фреймов. Второй тип представлен службой с установкой соединения, для которой перед началом передачи данных устанавливается логическая связь между передающим и принимающим узлами. Каждый фрейм содержит порядковый номер, который проверяется принимающим узлом, и это гарантирует то, что фреймы обрабатываются в том же порядке, в котором они были посланы. Установленный канал связи обеспечивает скорость передачи информации. Принимающий узел дает подтверждение передающему узлу в получении посланной информации. При возникновении ошибок данные передаются повторно.

Оба описанных уровня являются ключевыми при организации передачи данных. Их свойства определяют выбор сетевого оборудования и максимальный уровень скорости информационного обмена.

2.3 Сетевой и транспортный уровни модели OSI

Сетевой уровень управляет прохождением пакетов по сети. Все сети содержат физические маршруты передачи информации (кабельные тракты). Сетевой уровень анализирует адресную информацию протокола передачи пакетов и посылает их по более подходящему маршруту – физическому или логическому, обеспечивая максимальную эффективность сети. Также этот уровень обеспечивает пересылку пакетов между сетями через маршрутизаторы.

Контролируя прохождение пакетов, сетевой уровень выступает в роли «управляющего трафиком»: он направляет пакеты по наиболее эффективному из нескольких возможных трактов передачи данных. Для определения наилучшего маршрута сетевой уровень постоянно собирает информацию о расположении различных сетей и узлов, этот процесс называется обнаружением маршрута (*discovery*).

Сетевой уровень может отправлять данные по параллельным маршрутам, либо выбирать единственный маршрут на весь сеанс связи, создавая виртуальные каналы (*virtual circuit*). Виртуальные каналы представляют собой логические коммуникационные линии для передачи и приема данных. Виртуальные каналы, представленные только на сетевом уровне, образуются между сетевыми узлами, обменивающимися информацией. Поскольку сетевой уровень управляет данными, поступающими по нескольким виртуальным каналам, то эти данные могут поступать в неправильной очередности. Для устранения этих издержек сетевой уровень проверяет и при необходимости корректирует порядок передачи пакетов перед отправкой их следующему уровню стека. Также на сетевом уровне пакеты получают сетевые адреса и выполняется форматирование пакетов в соответствии с сетевым протоколом принимающей стороны. Кроме того, обеспечивается передача пакетов с такой скоростью, чтобы принимающий уровень успевал обрабатывать их.

Транспортный уровень подобно канальному и сетевому уровням выполняет функции, обеспечивающие надежную пересылку данных от передающего узла к принимающему. Транспортный уровень гарантирует, что данные на принимающей стороне собираются в правильном порядке, в независимости от порядка поступления составляющих их частей [2]. Кроме этого, по завершении пересылки принимающий узел может послать этому подтверждение.

Когда в сети используются виртуальные каналы, транспортный уровень отслеживает уникальные идентификаторы, назначенные каждому каналу. Эти значения называются портами, идентификаторами соединения или сокетами, они назначаются сеансовым уровнем.

Также транспортный уровень обеспечивает проверку сегментов данных. При этом на самом верхнем уровне контроля гарантируется безошибочная передача пакетов от узла к узлу в заданный промежуток времени.

Таким образом, два этих уровня являются ключевыми в решении задачи безошибочной доставки сообщения. Поскольку на этих уровнях принимаются решения о необходимости:

– повтора пакета данных в случае сбоя при его передаче;

– ограничения числа маршрутов по доставке сообщений;

– обеспечения правильной сборки сообщения после доставки всех его составляющих для передачи более высоким уровням.

На рисунке 2.5 представлена ситуация когда транспортный уровень отправителя разбивает сообщение, передаваемое по сети на три сегмента. На сетевом уровне сегменты упаковываются в пакеты и направляются одновременно по трем разным маршрутам получателю. На стороне получателя сетевой уровень принимает пакеты, распаковывает их и передает транспортному уровню. Транспортный уровень считает и сортирует пакеты, собирает сообщение и передает его дальше.

Для выполнения своих функций протоколы этих двух уровней внедряют дополнительные поля в структуру передаваемых данных, а в некоторых случаях дополнительно порождают служебные пакеты для сбора информации.

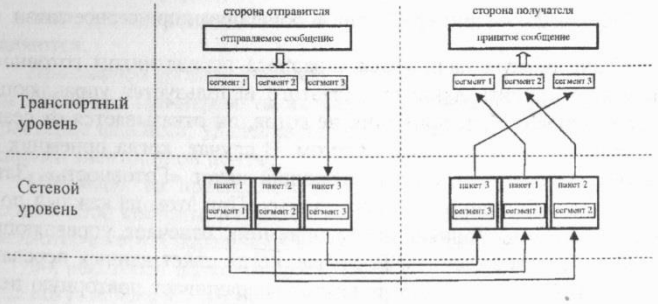


Рисунок 2.5 – Доставка и сборка информации сетевым и транспортным уровнями

2.4 Сеансовый, представительский и прикладной уровни OSI

Сеансовый уровень отвечает за установление и поддержку коммуникационного канала между двумя узлами [2,6,8]. Таким образом, он обеспечивает очередность работы узлов — определяет, какой из узлов первым начинает передачу данных. Сеансовый уровень определяет продолжительность работы узла на передачу, а также способ восстановления информации после ошибок передачи. Если сеанс связи был ошибочно прерван на более низком уровне, сеансовый уровень пытается восстановить передачу данных. По окончанию сеанса связи этот уровень подает команды отключения узлов.

В процессе сеанса обмена информацией по сети между передающим и принимающим абонентами происходит обмен информационными и управляющими сообщениями по установленным правилам. Это позволяет обеспечить надежную передачу информации при любой интенсивности обмена по сети (рисунок 2.6).

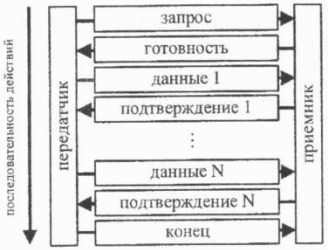


Рисунок 2.6 – Пример обмена сообщениями при сеансе связи

Сеанс обмена начинается с запроса передатчиком готовности приемника принять данные. Для этого используется управляющий пакет «Запрос». Если приемник не готов, он отказывается от сеанса специальным управляющим пакетом. В случае, когда приемник готов, он посылает в ответ управляющий пакет «Готовность». Затем начинается собственно передача данных. При этом на каждый полученный информационный пакет приемник отвечает управляющим пакетом «Подтверждение». В случае, когда пакет данных передан с ошибками, в ответ на него приемник запрашивает повторную передачу. Заканчивается сеанс управляющим пакетом «Конец», которым передатчик сообщает о разрыве связи.

Примером связи на сеансовом уровне может быть подключение рабочей станции к некоторому серверу Internet. Станция и сервер имеют уникальные адреса протокола Internet (IP-адреса), и сеансовый уровень использует эти адреса для установки соединения между узлами. После того, как подключение осуществлено и рабочая станция зарегистрировалась на сервере, на данном уровне устанавливается сеанс передачи данных.

Сеансовый уровень позволяет так выполнять передачу данных по сети, что ее производительность можно увеличить в два раза. Например, устройства, работающие на сеансовом уровне, могут передавать и принимать данные, однако, не одновременно. Для сеансового уровня этот способ передачи называется двусторонним альтернативным режимом для управления диалогом. Но, кроме этого, сеансовый уровень позволяет соединить эти устройства для одновременного приема-передачи, что вдвое увеличивает скорость передачи данных при сеансовом диалоге между двумя узлами.

Представительский уровень управляет форматированием данных, поскольку прикладные программы нередко используют различные способы представления информации. В некотором смысле, он выполняет функции программы проверки синтаксиса. Он гарантирует, что числа и символьные строки передаются именно в том формате, который понятен принимающему узлу. Также он отвечает за шифрование данных. Шифрование – это процесс засекречивания информации, который не позволяет неавторизованным пользователям прочитать данные в случае их перехвата. Еще одна функция – сжатие данных после их формирования, так как между символами и строками может оставаться свободное место. При сжатии эти промежутки удаляются.

Прикладной уровень управляет доступом к приложениям и сетевым службам. Примером таких служб являются передача файлов, управление файлами, удаленный доступ к файлам, управление сообщениями электронной почты.

Например, на прикладном уровне работает редиректор сетевой операционной системы. Редиректор – это служба, позволяющая видеть компьютер в сети и обращаться к нему. Если в сети разрешается общий доступ к некоторой папке, то при помощи редиректора другие компьютеры могут видеть эту папку и использовать ее. Таким образом, локально выполняемое приложение не ощущает разницы между локальным и сетевым диском при своем обращении к файловой системе.

2.5 Понятие и свойства сетевых протоколов

Протоколы (*protocols*) – это набор правил и процедур, регулирующих порядок реализации некоторой связи. В компьютерной среде протоколы – это правила и технические процедуры, позволяющие нескольким компьютерам, объединенным в сеть, общаться друг с другом.

Иерархически организованный набор разноуровневых протоколов, достаточный для организации полноценного взаимодействия узлов в сети, называется *стеком протоколов*. [2]

Многие стеки протоколов разрабатывались задолго до того, как стала широко использоваться модель OSI, поэтому на программном уровне они более соответствуют модели DoD (рисунок 2.7).

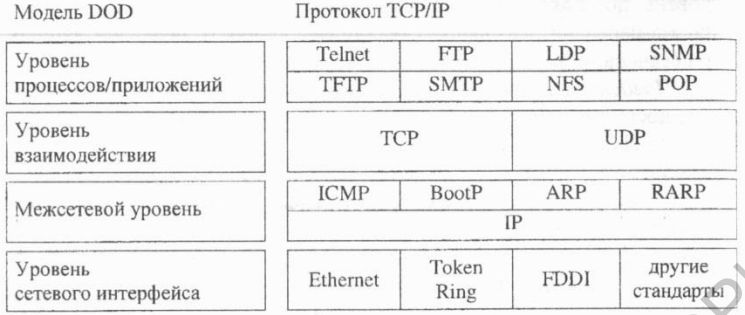


Рисунок 2.7 – Соответствие протоколов Internet уровням модели DoD

Передача данных по сети разбита на ряд последовательных действий, каждому из которых соответствуют свои правила и процедуры, составляющие протокол. В обязательном порядке сохраняется очередность их выполнения: на компьютере-отправителе – в направлении сверху вниз, а на компьютере-получателе – снизу вверх.

Протоколы могут быть двух типов: низкоуровневые и высокоуровневые:

– низкоуровневые протоколы появились достаточно давно и с тех пор не претерпели никаких кардинальных изменений. За длительное время использования таких протоколов в них были найдены и устранены все возможные «дыры» и ошибки.

– что касается высокоуровневых протоколов, то они постоянно разрабатываются и совершенствуются.

Стандарты низкоуровневых протоколов как видно из рисунка 2.7 (уровень сетевого интерфейса) могут быть жестко связаны со стандартами на оборудование, для которых действуют спецификации IEEE 802 (см. п. 2.11). Примерами низкоуровневых протоколов (межсетевого уровня на рисунке 2.7) являются ICMP, BootP, ARP, RARP, IP, а также драйвера сетевых устройств, оболочка NDIS и другие протоколы такого же уровня из других стеков.

Существует множество различных протоколов, каждый из которых имеет свои особенности. Одни протоколы узконаправленные, другие имеют более широкое применение, так как не все протоколы можно использовать в одинаковых условиях. Иногда применение одного протокола выгодно для небольшой группы компьютеров и крайне невыгодно для большого количества компьютеров, с несколькими маршрутизаторами и подключением к Internet.

Многие авторы описывают протоколы опираясь не на модель DoD, а на модель ISO/OSI. В таблице 2.1 – пример такого описания.

Таблица 2.1 – Основные функции, выполняемые протоколами

Модель OSI	Функции	Примеры протоколов
Прикладной уровень	Прикладной уровень отвечает за доступ приложений в сеть. Задачами этого уровня является копирование файлов, обмен почтовыми сообщениями и управление сетью.	FTP - протокол копирования файлов TFTP - упрощенный протокол копирования файлов X.400 - электронная почта Telnet - удаленный доступ в сеть SMTP - простой протокол почтового обмена CMIP - общий протокол управления информацией SNMP - простой протокол управления сетью NFS - сетевая файловая система FTAM - метод доступа для копирования файлов
Представительский уровень	Уровень представления отвечает за возможность диалога между приложениями на разных машинах. Этот уровень обеспечивает преобразование данных (кодирование, компрессия и т.п.) прикладного уровня в поток информации для транспортного уровня.	DNS LDAP NetBIOS/IP
Сеансовый уровень	Сеансовый уровень отвечает за организацию и поддержку соединений между сессиями, администрирование и безопасность сети	
Транспортный уровень	Транспортный уровень определяет протоколы обмена сообщениями и обеспечивает сквозное управление протоколом данных через сеть	TCP - протокол управления передачей NCP - NetWare Core Protocol SPX - упорядоченный обмен пакетами TP4 - протокол передачи класса 4
Сетевой уровень	Сетевой уровень отвечает за деление пользователей на группы (адресацию) и управление сетью. На этом уровне происходит маршрутизация пакетов на основе преобразования MAC-адресов в сетевые адреса. Сетевой уровень обеспечивает передачу пакетов на транспортный уровень.	IP - протокол Internet IPX - протокол межсетевого обмена X.25 (частично этот протокол реализован на канальном уровне) CLNP - сетевой протокол без организации соединений
Канальный уровень	Канальный уровень обеспечивает формирование, передачу и прием кадров данных. Этот уровень обслуживает запросы сетевого уровня и использует сервис физического уровня для приема и передачи пакетов.	HDLC для последовательных соединений Ethernet Token Ring FDDI X.25 Frame relay PPP
Физический уровень	Физический уровень отвечает за подключение к физической среде передачи (медь, оптика, радио). Этот уровень получает кадры данных от канального уровня и преобразует их в оптические или электрические сигналы, соответствующие значениям битов в потоке данных. Эти сигналы посылаются через среду передачи на приемный узел.	

2.6 Прикладные протоколы

Прикладные протоколы выполняют задачу обслуживания сетевых запросов пользовательских программ.

Среди прикладных протоколов наиболее распространены протоколы сети Internet. Например, среда WWW построена по хорошо известной схеме «клиент-сервер». На рисунке 2.8 показано, как разделены функции в этой среде [11].

Программа-клиент выполняет функции интерфейса пользователя и обеспечивает доступ практически ко всем информационным ресурсам Internet. В этом смысле она выходит за обычные рамки работы клиента только с сервером определенного протокола, как это происходит, например в TELNET. Довольно широко распространенное мнение, что WWW-клиенты Mosaic или Netscape – просто элементы графического интерфейса Internet, является лишь отчасти верным. Базовые компоненты WWW-технологии (HTML и URL) играют при доступе к другим ресурсам Mosaic не последнюю роль, и поэтому мультипротокольные клиенты должны быть отнесены именно к World Wide Web, а не к другим информационным технологиям Internet. Фактически, клиент – это интерпретатор HTML. И, как типичный интерпретатор, клиент в зависимости от команд (разметки) выполняет различные функции.

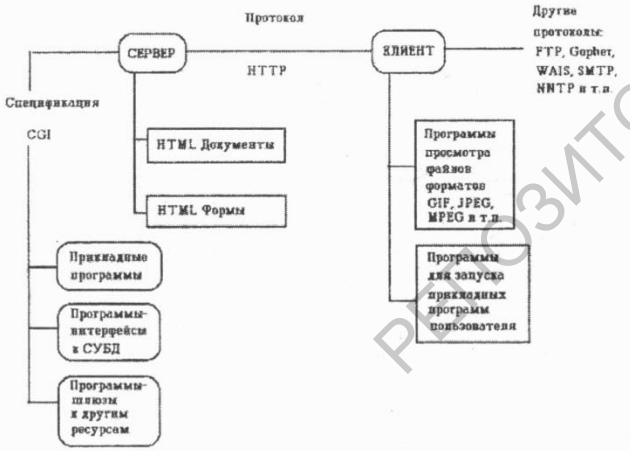


Рисунок 2.8 – Схема структуры «клиент – сервер»

Процесс разработки и выдачи документации протоколов Internet скорее напоминает академический исследовательский проект, чем что-либо другое. Протоколы определяются в документах, называемых Requests for Comments (RFC) (Запросы для Комментария). RFC публикуются, а затем рецензируются и анализируются специалистами по Internet. Уточнения к протоколам публикуются в новых RFC. Взятые вместе, RFC обеспечивают красочную историю людей, компаний и направлений, которые формировали разработку набора протоколов для открытой системы, являющегося на текущий момент самым популярным.

Таким образом, комплекс протоколов Internet охватывает большое семейство протоколов, прикладные программы и саму сеть.

Протоколы Internet можно использовать для передачи сообщений через любой набор объединенных между собой сетей. Они в равной мере пригодны для связи как в локальных, так и в глобальных сетях. Комплект протоколов Internet включает в себя не только спецификации низших уровней (такие, как TCP и IP), но также спецификации для таких общих применений, как почта, эмуляция терминалов и передача файлов. На рисунке 2.9 представлены некоторые из наиболее важных протоколов Internet в составе стека протоколов TCP/IP.

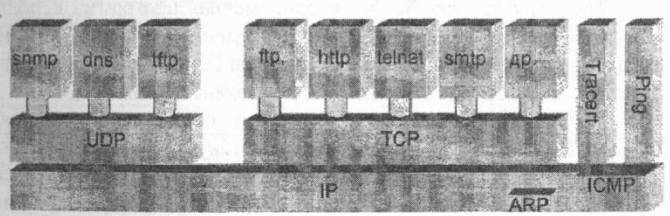


Рисунок 2.9 – Схема структуры «клиент – сервер»

По назначению и реализуемым службам все протоколы Internet удобно разделить на следующие виды:

- протоколы назначения адресов;
- протоколы маршрутизации;
- протоколы файлового обмена;
- почтовые протоколы;
- протоколы удаленного доступа и управления.

Далее в этой главе будут рассмотрены общие признаки и примеры некоторых из перечисленных видов.

2.7 Протоколы файлового обмена

Протокол FTP (File Transfer Protocol – протокол переноса файлов) обеспечивает базовые элементы системы совместного использования файлов хостами сети. Протокол FTP использует TCP для создания виртуальных соединений, обеспечивающих поддержку управления. Для операций переноса файлов организуется отдельное соединение TCP. Управляющие соединения используют образ протокола TELNET для обмена командами и сообщениями между хостами сети.

Управляющие запросы FTP используют обмен TELNET и могут содержать команды TELNET или опции согласования параметров. Однако большинство управляющих запросов FTP является просто текстовыми строками ASCII и может классифицироваться как команды или сообщения FTP.

Сообщения FTP являются откликами на команды FTP и содержат код отклика, за которым следует пояснительный текст.

Протокол TFTP (Trivial File Transfer Protocol – тривиальный протокол переноса файлов) использует дейтаграммы UDP. TFTP поддерживает операции записи и чтения файлов, но не поддерживает службы каталогов и проверки полномочий (авторизации) пользователей.

Протокол Internet Gopher и одноименная программа используют модель клиент-сервер. Этот протокол предполагает использование надежного протокола доставки TCP. Серверы Gopher прослушивают порт 70 (этот номер порта выделен для Gopher комитетом IANA).

Документы Gopher могут располагаться на множестве хостов Internet. Пользователи запускают клиентскую программу на своем компьютере, подключаются к серверу Gopher и посылают ему селектор (строка текста, которая может быть пустой) через соединение TCP с использованием предопределенного порта. Сервер отвечает на запрос текстовым блоком, завершающимся точкой в пустой строке, и разрывает соединение. Первый символ каждой строки говорит о том, что описывает строка – документ, каталог или поисковый сервис. Следующие символы (до знака табуляции) формируют строку вывода на пользовательский экран, служащую для выбора данного документа (или каталога). Первый символ строки реально определяет тип элемента, отображаемого этой строкой.

Почти во всех случаях клиент Gopher предоставляет пользователю некоторое представление о том, чему соответствует данный элемент (выводится пиктограмма, короткий текст и пр.).

Символы после знака табуляции (до следующего символа табуляции) формируют строку селектора, которую клиентская программа должна передать серверу для получения документа (или списка содержимого каталога). Клиент никогда не меняет строку селектора, которая зачастую является маршрутом доступа или другим селектором, используемым сервером для доступа к желаемому элементу. Следующие два символа табуляции обозначают имя домена для хоста и номер порта.

Клиент Gopher решает вопрос доступности объекта для просмотра по первому символу каждой строки в списке содержимого каталога. Увеличение этого списка может расширять протокол.

Протокол HTTP (Hypertext Transfer Protocol – это протокол передачи гипертекста). Он представляет собой протокол уровня приложений, обеспечивающий простой и быстрый способ организации распределенных гиперсред для совместного использования в сети.

Сообщения передаются в формате, похожем на форматы Internet Mail и MIME (Multipurpose Internet Mail Extensions).

Основным назначением протокола HTTP является передача вебстраниц (текстовых файлов с разметкой HTML), хотя с помощью него с успехом передаются и другие файлы, как связанные с вебстраницами (изображения и приложения), так и не связанные с ними (в этом HTTP конкурирует с FTP).

Согласно спецификациям HTTP предполагается, что клиентская программа (веб-браузер) способна отображать гипертекстовые вебстраницы и файлы других типов в удобной для пользователя форме.

Протокол S-HTTP (Secure HTTP) обеспечивает механизм защищенной связи между парами «клиент HTTP» – «сервер HTTP» для того, чтобы можно было выполнять коммерческие транзакции с помощью широкого класса приложений. S-HTTP обеспечивает гибкое решение для поддержки множества ортогональных режимов работы, механизмов управления ключами, моделей доверия, криптографических алгоритмов и форматов инкапсуляции путем согласования опций между участниками каждой транзакции.

Сообщения Secure HTTP синтаксически совпадают с сообщениями HTTP и состоят из строк запроса или состояния, за которыми следует заголовок и текст сообщения. Однако, заголовки S-HTTP отличаются от заголовков HTTP, а тело сообщений обычно зашифровано.

2.8 Почтовые протоколы

Протокол SMTP (Simple Mail Transfer Protocol – простой почтовый протокол, RFC-821, RFC -822) представляет собой почтовый сервис, смоделированный на основе файлового сервиса FTP. SMTP обеспечивает передачу почтовых сообщений между системами и уведомления о входящей почте. SMTP – довольно независимая субсистема, требующая только надежного канала связи. Средой для SMTP может служить отдельная локальная сеть, система сетей или вся сеть Internet.

Протокол SMTP обеспечивает передачу почтового сообщения непосредственно конечному получателю, когда они соединены друг с другом. В противном случае пересылка может выполняться через одну (или более) промежуточную «почтовую станцию».

SMTP-сервера могут вести диалог с несколькими конечными пользователями. Любое почтовое сообщение завершается специальной последовательностью символов. Если получатель успешно завершил прием и обработку почтового сообщения, он посылает положительный отклик.

Протокол POP3 (Post Office Protocol version 3) позволяет рабочим станциям динамически забирать почту с сервера. Для небольших организаций невыгодно держать у себя систему для передачи сообщений (message transport system). Это связано с тем, что в небольших, не специализирующихся на компьютерных технологиях организациях, как правило, рабочие станции клиентов сети не имеют достаточно ресурсов (производительности или дискового пространства) для обеспечения работы полного SMTP-сервера. Кроме того, таким пользователям электронной почты может быть просто невыгодно держать персональный компьютер постоянно подключенным к Internet.

POP3 позволяет только забрать почту из почтового ящика сервера на рабочую станцию клиента и удалить ее из почтового ящика на сервере. Всю дальнейшую обработку почтовое сообщение проходит на компьютере клиента. POP3-сервер не отвечает за отправку почты, он работает только как универсальный почтовый ящик для группы пользователей.

Когда пользователю необходимо отправить сообщение, он должен установить соединение с каким-либо SMTP-сервером и отправить туда свое сообщение по SMTP. Этот SMTP-сервер может быть тем же хостом, где работает POP3-сервер, а может располагаться совсем в другом месте.

Протокол X.400 – обобщенный стандарт управления сообщениями и их обработкой. Система обработки сообщений X.400 построена в соответствии с принципами эталонной модели взаимосвязи открытых систем. СОС может быть построена с использованием любой сети, относящейся к области распространения взаимосвязи открытых систем. Назначение системы обработки сообщений состоит в том, чтобы дать возможность пользователям обмениваться сообщениями на основе их промежуточного накопления.

Сообщение, предоставленное одним отправителем, передаётся через систему передачи сообщений и доставляется одному или нескольким другим получателям. Модель системы приведена на рисунке 2.10.

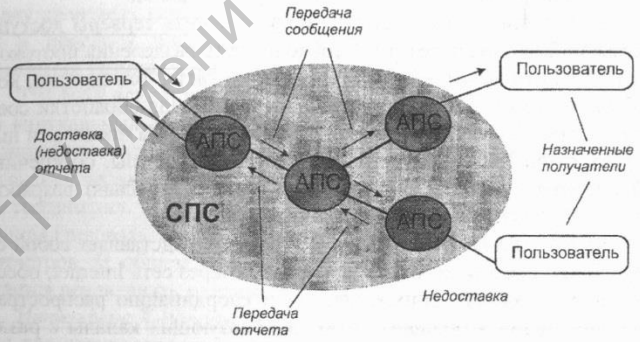


Рисунок 2.10 – Модель системы передачи сообщений

Протокол IMAP4 (Internet Message Access Protocol, Version 4rev1) обеспечивает клиентам доступ и возможность манипуляций с почтовыми сообщениями на сервере. IMAP4 поддерживает операции с удаленными папками сообщений, называемыми почтовыми ящиками (mailbox) как при работе с локальными почтовыми ящиками. Протокол IMAP4 обеспечивает также поддержку offline-клиентов для ресинхронизации с сервером. IMAP4 включает операции создания, удаления и переименования почтовых ящиков, просмотра новых сообщений, удаления сообщений навсегда, установки и снятия флагов, грамматического разбора (parsing), поиска и выборки атрибутов сообщений, текстов и их частей. Сообщения в IMAP4 допускают использование номеров, являющихся порядковыми номерами или уникальными идентификаторами сообщений.

2.9 Протоколы и программы удаленного контроля и управления

DNS (Domain Name Service – служба доменных имен) обеспечивает поиск имен хостов, используя распределенную по сетевым серверам имен базу данных.

Протокол IPDC (IP Device Control – управление устройствами IP) представляет собой семейство протоколов, компоненты которого используются совместно или по отдельности для управления соединениями, средой и передачей сигнализации. Этот протокол решает задачи одного или нескольких протоколов управления шлюзами, расположенными на границе между коммутируемой телефонной сетью и сетью Internet, а также завершающих коммутируемые транки.

Примерами таких устройств могут служить серверы доступа и шлюзы VoIP (голос через IP). Необходимость разделения протоколов управления от системы сигнализации возникает в тех случаях, когда требуется, чтобы логика управления сервисом для обработки соединений полностью или частично была реализована за пределами шлюзов. Протокол IPDC был построен на базе структуры, обеспечиваемой протоколом DIAMETER, который был специально разработан для аутентификации, авторизации и ведения учета.

Протокол NTP (Network Time Protocol) представляет собой систему синхронизации компьютерных часов через сеть Internet, обеспечивающую механизм синхронизации и координацию распространения информации в больших сетях, использующих каналы с различными скоростями.

Протокол использует структуру распространения информации между серверами точного времени, образующими самоорганизующуюся иерархическую структуру «ведущий-ведомый» (master-slave) для синхронизации локальных часов подсети с национальными стандартными часами по проводам или радиоканалу.

Протокол SNMP разработан для того, чтобы различные объекты сетей могли участвовать в глобальной архитектуре управления сетью. Системы сетевого управления могут опрашивать (сканировать) сетевые объекты, реализующие протокол SNMP для получения информации, имеющей отношение к частной реализации системы управления сетью. Система управления сетью узнает о проблемах, получая прерывания (trap) или уведомления об изменениях от сетевых устройств, реализующих SNMP.

Протокол RADIUS представляет собой протокол, управляющий распределенными последовательными линиями для большого числа пользователей.

Обычно RADIUS используется маршрутизаторами CISCO для организации модемных линий, но возможны и варианты связки RADIUS и PPPD. В современных моделях мостов и маршрутизаторов большинство производителей поддерживают этот протокол.

Протокол TELNET представляет собой протокол эмуляции терминала в стеке TCP/IP. Современные варианты TELNET обеспечивают эмуляцию практически всех функций терминалов различных типов, разработанных в течение последних 20 лет.

Набор опций позволяет протоколу TELNET поддерживать передачу двоичных данных, макросы, эмуляцию графических терминалов и передачу информации для поддержки централизованного управления терминалами.

TELNET использует транспортный протокол TCP для организации виртуальных соединений между серверами и клиентами. После организации соединения сервер и клиент TELNET входят в фазу согласования параметров, определяющих режим работы каждой из сторон соединения. В течение сеанса любая из сторон может заново инициализировать старые параметры или согласовать новый набор параметров. В общем случае каждая сторона TELNET-соединения пытается реализовать максимально возможный набор свойств связи.

Интерфейс X-Window обеспечивает удаленный оконный интерфейс для распределенных сетевых приложений. Это программа, использующая в качестве транспортного протокола TCP/IP или DECnet.

X-Window основан на архитектуре клиент-сервер, где сервер представляет собой управляющую программу на рабочей станции пользователя, а клиентские приложения могут размещаться в любом месте сети. Управляющая программа X-сервер на рабочей станции пользователя может одновременно поддерживать множество окон для различных сетевых приложений с асинхронным обновлением содержимого окон в соответствии с информацией X-Window.

Для обеспечения взаимодействия пользователя с удаленными приложениями программа X-сервер на станции пользователя генерирует события в ответ на действия пользователей. В некоторых случаях приложения могут также генерировать события, передаваемые управляющей программе X-сервер.

2.10 Стеки протоколов локальных сетей

Для компьютерной промышленности было разработано множество стеков протоколов, но число стеков, получивших статус стандартных моделей, было и остается ограниченным. Вот наиболее важные из них (рисунок 2.11):

- набор протоколов ISO/OSI;
- IBM System Network Architecture (SNA);
- Digital DECnet;
- AppleTalk;
- Novell NetWare;
- набор протоколов Internet — TCP/IP.

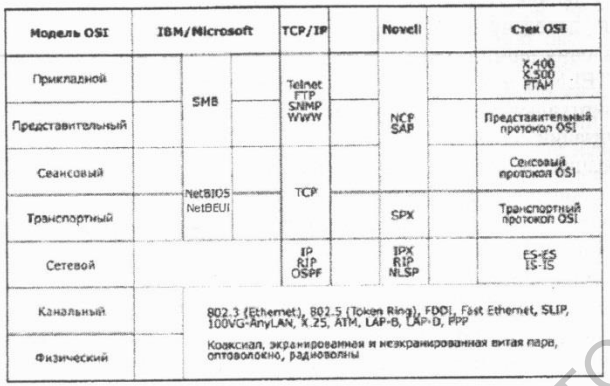


Рисунок 2.11 – Примеры различных протоколов в популярных стеках [7]

Большинство сетевых моделей допускает два основных метода взаимодействия абонентов в сети: взаимодействие без логического соединения или метод дейтаграмм (рисунок 2.12, *а*) и взаимодействие с логическим соединением (рисунок 2.12, *б*) [6].

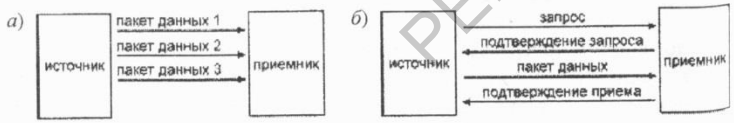


Рисунок 2.12 – Методы взаимодействия абонентов в сети: *а*) метод дейтаграмм; *б*) метод с логическим соединением

Согласно методу дейтаграмм каждый пакет рассматривается как самостоятельный объект. Пакет при этом методе передается без установления логического канала, то есть без предварительного обмена служебными пакетами для выяснения готовности приемника, а также без ликвидации логического канала, то есть без пакета подтверждения окончания передачи. Проверка факта получения переносится на более высокие уровни.

При методе с логическим соединением пакет передается только после того, как будет установлено логическое соединение (канал) между приемником и передатчиком. Каждому информационному пакету сопутствует один или несколько служебных пакетов (установка соединения, подтверждение получения, запрос повторной передачи, разрыв соединения). Логический канал может устанавливаться на время передачи одного или нескольких пакетов. Метод с логическим соединением гораздо надежнее, поскольку, к моменту ликвидации логического канала передатчик уверен, что все его пакеты дошли до места назначения, причем дошли успешно. Не бывает при данном методе и перегрузки сети из-за бесполезных пакетов. Недостаток метода с логическим соединением состоит в том, что довольно сложно разрешить ситуацию, когда принимающий абонент по тем или иным причинам не готов к обмену, например, из-за обрыва кабеля, отключения питания, неисправности сетевого оборудования, сбоя в компьютере. Также этот метод не позволяет передавать широковещательные пакеты, так как нельзя организовать логические каналы сразу со всеми абонентами.

Именно для того, чтобы объединить достоинства обоих методов, многие протоколы используются в виде связанных наборов: TCP/IP и IPX/SPX, в которых протокол более высокого уровня (TCP, SPX), работающий на базе протокола более низкого уровня (IP, IPX), гарантирует правильную доставку пакетов в требуемом порядке.

В качестве примера на рисунке 2.13 показаны стеки протоколов, используемых популярными сетевыми операционными системами [2].

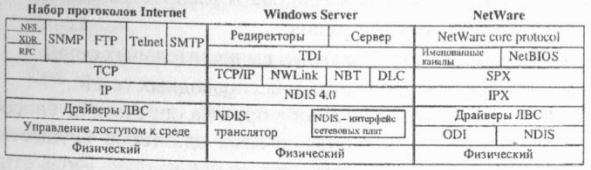


Рисунок 2.13 – Соотношение стеков протоколов с уровнями модели OSI

2.11 Проект IEEE 802.x

Свойства протоколов верхних уровней закреплены спецификациями, описанными в семействе стандартов RFC.

Спецификации протоколов и оборудования, работающих на нижних уровнях сетевых моделей описываются в наборе стандартов проекта IEEE 802. Они охватывают только два нижних уровня модели OSI – физический и канальный. Это связано с тем, что данные уровни составляют основу локальных сетей [3,5]. Такая специфика нашла свое отражение в разделении канального уровня на два подуровня, которые часто называют также уровнями. Канальный уровень (Data Link Layer) делится в локальных сетях на два подуровня:

– управление логическим каналом связи (Logical Link Control, LLC);

– управления доступом к среде (Media Access Control, MAC).

Уровень MAC появился из-за существования в локальных сетях разделяемой среды передачи данных. Именно этот уровень обеспечивает корректное совместное использование общей среды, предоставляя ее в соответствии с определенным алгоритмом в распоряжение той или иной станции сети.

После того, как доступ к среде получен, ею может пользоваться более высокий уровень – уровень LLC. Этот уровень отвечает за передачу кадров данных между узлами с различной степенью надежности, а также реализует функции интерфейса с прилегающим к нему сетевым уровнем. Именно через уровень LLC сетевой протокол запрашивает у канального уровня нужную ему транспортную операцию с нужным качеством. На уровне LLC существует несколько режимов работы, отличающихся наличием или отсутствием на этом уровне процедур восстановления кадров в случае их потери или искажения, то есть отличающихся качеством транспортных услуг этого уровня.

Таким образом, спецификации 802.X распространяются:

– на платы сетевых адаптеров;

– на оборудование глобальных вычислительных сетей;

– на компоненты кабельных и беспроводных сетей.

То есть, спецификации данного проекта определяют способы, в соответствии с которыми платы сетевых адаптеров осуществляют доступ к физической среде и передают по ней данные. Сюда относятся соединение, поддержка и разъединение сетевых устройств.

Список рабочих и исследовательских групп IEEE 802

Активные группы

802.1	Рабочая группа по протоколам верхних уровней локальных сетей.
802.3	Рабочая группа по Ethernet.
802.11	Рабочая группа по беспроводным локальным сетям (Wireless LAN).
802.15	Рабочая группа по беспроводным персональным сетям (Wireless Personal Area Network, WPAN).
802.16	Рабочая группа по системам широкополосного беспроводного доступа (Broadband Wireless Access).
802.17	Рабочая группа по динамическому пакетному кольцу (Resilient Packet Ring).
802.18	Техническая консультативная группа по обязательным требованиям к радио (Radio Regulatory).
802.19	Техническая консультативная группа по смешанным структурам (Coexistence).
802.20	Рабочая группа по мобильным системам широкополосного беспроводного доступа (Mobile Broadband Wireless Access MBWA).
802.21	Рабочая группа по реализации переключения вызова без прерывания соединения (Media Independent Handoff Working Group).
802.22	Рабочая группа по беспроводным региональным сетям (Wireless Regional Area Networks).

Неактивные группы

802.2	Рабочая группа по управлению логическим каналом (Logical Link Control).
802.5	Рабочая группа по сети «маркерное кольцо» (Token Ring).
802.12	Рабочая группа по протоколу «обработка запросов по приоритету» (Demand Priority).

Расформированные группы

802.4	Рабочая группа по сети «маркерная шина» (Token Bus).
802.6	Рабочая группа по городским сетям (Metropolitan Area Network).
802.7	Техническая консультативная группа по широкополосной связи (Broadband).
802.8	Техническая консультативная группа по волоконной оптике (Fiber Optic).
802.9	Рабочая группа по изохронным локальным сетям (Isochronous LAN).
802.10	Рабочая группа по безопасности (Security).
802.14	Рабочая группа по кабельным модемам (Cable Modem).
QOS/FC	Исследовательская группа по контролю качества обслуживания (QoS/Flow Control Study Group).

Вопросы для самоконтроля

1 Зачем нужны модели представления сетевых объектов и устройств?

2 Опишите теоретические модели, оказавшие влияние на сетевые технологии.

3 Какое место в описании компьютерных сетей занимает проект IEEE 802.x?

4 Каковы функции физического уровня модели OSI?

5 Каковы функции канального уровня модели OSI?

6 Каковы функции сетевого уровня модели OSI?

7 Каковы функции транспортного уровня модели OSI?

8 Каковы функции сеансового уровня модели OSI?

9 Каковы функции представительского уровня модели OSI?

10 Каковы функции прикладного уровня модели OSI?

11 Какие альтернативные модели описания компьютерных сетей вы знаете?

12 Каков порядок разработки сетевых стандартов и какие организации в этом участвуют?

13 Как реализуется сетевая архитектура в структуре современных операционных систем?

14 Что такое MAC и каковы его функции?

15 Что такое LLC и каковы его функции?

16 Дайте определение понятия протокола.

17 Какие типы протоколов существуют?

18 Приведите соответствие типов протоколов модели OSI.

19 Какие устройства реализуют протоколы канального уровня?

20 Какие стеки протоколов вы знаете?

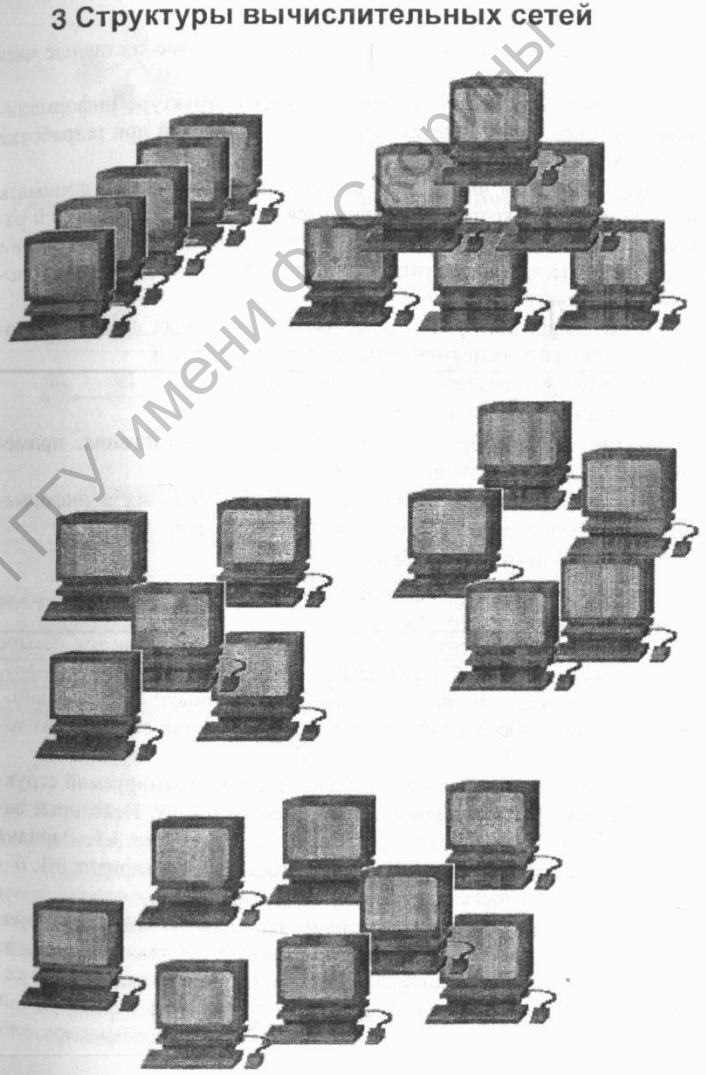
21 Опишите схему структуры «клиент – сервер».

22 Какие протоколы файлового обмена вы знаете?

23 Какие почтовые протоколы вы знаете?

24 Назовите протоколы удаленного контроля и управления.

3 Структуры вычислительных сетей



3.1 Понятие топологии

Структура вычислительной сети делится на две составные части: логическую и физическую.

Логическая структура сети подчинена структуре информационных потоков. Она является первичной и ключевой при разработке физической структуры сети.

Под термином *физическая структура сети* следует понимать базовый принцип, который используется при размещении узлов и рабочих станций, а также активного оборудования сети на территории предприятия (в здании, группе зданий и между ними), то есть *топологию компьютерной сети*.

С точки зрения проектирования компьютерных сетей, топология – это описание основной компоновки сети [3,6,10].

Топология определяет следующие свойства [2]:

– тип кабельной системы;

– тип и характеристики передающего оборудования, применяемого для передачи данных;

– физическое размещение компьютеров, силовых и информационных кабелей, а также других компонентов сети;

– способ прокладки кабеля;

– возможность расширения сети;

– способ управления сетью.

На текущий момент наиболее популярными являются четыре типа базовых топологий, называемых «чистыми»: *«шина», «кольцо», «звезда», «ячейка»*, и два типа комбинированных: *«звезда-шина», «звезда-кольцо»*. Остальные относят к сложным или смешанным топологиям.

Сложные топологии – это топологии с программируемой структурой, которые настраиваются под решаемую задачу. Некоторые варианты сложных топологий представлены на рисунке 3.1. Вариант 3.1, *а* является примером нерегулярной топологии, а вариант 3.1, *б* – иерархический случай связи (древовидная топология).

Если топологии *«шина», «кольцо», «звезда», «ячейка», «звезда-шина», «звезда-кольцо»* чаще применимы для локальных сетей, то более сложные схемы типичны для региональных и глобальных сетей. Некоторые современные вычислительные сети используют и другие сетевые структуры: *«решетки», «кубы», «гипердеревья», «гиперкубы»* и т. д. (рисунок 3.2).

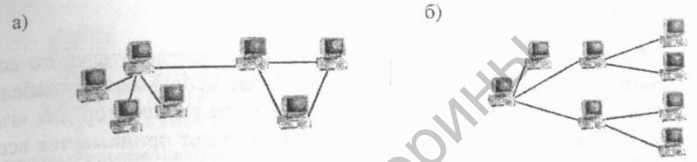


Рисунок 3.1 – Примеры сложных топологий вычислительных сетей

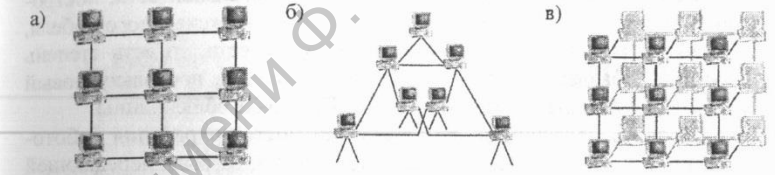


Рисунок 3.2 – Структуры топологий сложных вычислительных систем:
а) топология «решетка»; *б*) топология «гипердерево»;
в) топология «куб»

Топология часто определяет способ взаимодействия компьютеров в сети, в частности – метод доступа к среде.

Выбор топологии локальной или региональной сети существенно сказывается на ее стоимости и рабочих характеристиках. При этом важной характеристикой для однородной сети является среднее число шагов между узлами D.

$$D = \sum_{d=1}^{n} \frac{\alpha \cdot N_d}{n-1},$$

где n – полное число узлов в сети; α – расстояние между крайними узлами сети, N_d – число узлов сети на расстоянии α.

Как правило, обычная локальная сеть, которая проектируется с нуля, подчинена одному из четырех типов «чистых» топологий. После проведения модификации и/или адаптационных работ ее топология становится сложной или смешанной.

Требования топологий компьютерных сетей дополняются положениями, закрепленными в стандартах структурированных кабельных систем.

3.2 Топология «шина»

Шинная топология использует принцип последовательного соединения узлов сети в виде цепочки. В случае использования кабеля к каждому концу сегмента шины подключается терминатор для «гашения» отраженного сигнала. Передаваемый пакет принимается всеми узлами сегмента, и на прохождение всего сегмента требуется некоторое количество времени, называемое задержкой (рисунок 3.3).

В качестве среды передачи в данной топологии часто применяется коаксиальный кабель. Пример реализации локальной сети, построенной по топологии «шина» с использованием коаксиального кабеля, показан на рисунке 3.4. Расширяемость такой сети, то есть степень простоты добавления новых элементов – хорошая, поскольку новый узел можно «врезать» (подключить) в любой точке общей шины.

Уровень надежности, то есть вероятность сохранения работоспособности при выходе из строя узла сети или разрыва передающей среды этой топологии, очень низкий. Обрыв кабеля в любой точке может блокировать весь сетевой обмен.

Наличие терминатора для шинной топологии обязательно, поскольку терминатор указывает на физическое окончание сегмента. На практике терминатор представляет собой электрическое сопротивление, гасящее сигнал, когда тот достигает конца сети. Без терминатора сегмент не соответствовал бы спецификациям IEEE и сигналы могли бы отражаться обратно, возвращаясь в тот же кабель, по которому они были переданы. Отраженный сигнал сбивает синхронизацию сети и может сталкиваться с новыми сигналами, передаваемыми по сети.

В некоторых источниках утверждается, что топология «шина» может быть использована только для устаревших сетей, поскольку она не в состоянии поддерживать скоростные режимы выше 10 Мбит/с. Однако коаксиальный кабель, являющийся основой этой топологии, позволяет передавать данные на гораздо более высокой скорости.

Кроме классических стандартов сетевых архитектур с использованием данной топологии – ArcNet и Ethernet, следует упомянуть и сетевые архитектуры для данной топологии, разработанные в СССР, такие, как FishNet (100 Ом) и Iola (75 Ом). Сети кабельного телевидения и системы CaTV также используют шинную топологию для подключения отдельных пользователей к общей информационной среде или одной из информационных сред. Также следуют упомянуть, что стандарты ИК-сетей часто реализуются по топологии «шина».

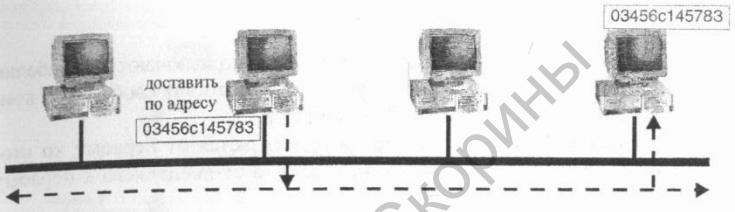


Рисунок 3.3 — Доставка данных адресату в топологии «шина»

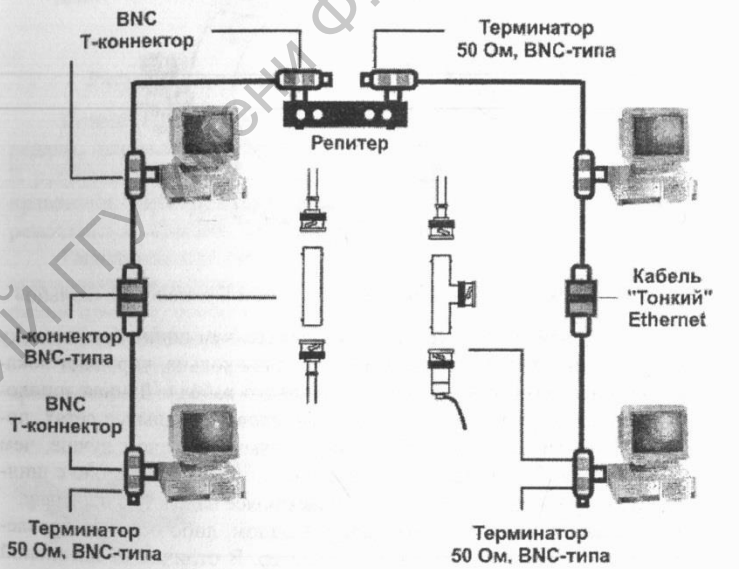


Рисунок 3.4 – Структура сети, построенной по топологии «шина» с использованием тонкого коаксиального кабеля

В целом, данную топологию нельзя списывать с рынка сетевых технологий. Сети и сегменты сетей на ее основе еще довольно долго будут существовать, а также вновь проектироваться и создаваться для решения целого ряда специфичных задач.

3.3 Топология «кольцо»

При топологии «кольцо» компьютеры подключаются к кабелю, замкнутому в кольцо. Поэтому у кабеля просто нет свободного конца, на который надо поставить терминатор.

Продвижение информации осуществляется от первому ко второму, от второго к третьему и так далее, а от последнего к первому (рисунок 3.5).

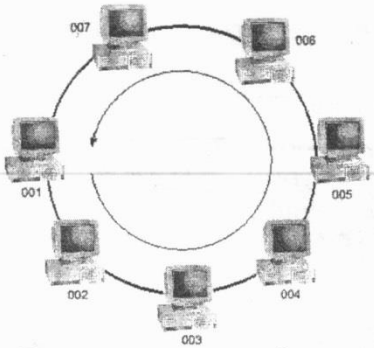


Рисунок 3.5 – Пример сети, построенной топологии «кольцо»

Кольцевой топологией легче управлять, чем шинной, поскольку оборудование, используемое для построения кольца, упрощает локализацию дефектного узла или неисправного кабеля. Данная топология хорошо подходит для передачи сигналов в локальных сетях, поскольку она справляется с большим сетевым трафиком лучше, чем шинная топология. В целом можно сказать, что по сравнению с шинной топологией, кольцевая обеспечивает более надежную передачу.

Сигналы передаются по кольцу в одном, либо обоих направлениях и проходят через каждый компьютер. В отличие от пассивной топологии «шина», здесь каждый компьютер выступает в роли повторителя, усиливая сигналы и передавая их следующему компьютеру. Поэтому, если выйдет из строя один компьютер, прекращает действовать вся сеть. Интерфейс связи может быть реализован в виде внешнего трансивера, либо быть встроенным в сетевой адаптер. Для обеспечения бесперебойной работы он должен быть всегда включен и иметь возможность замыкания кольца при отключении узла сети (рисунок 3.6).

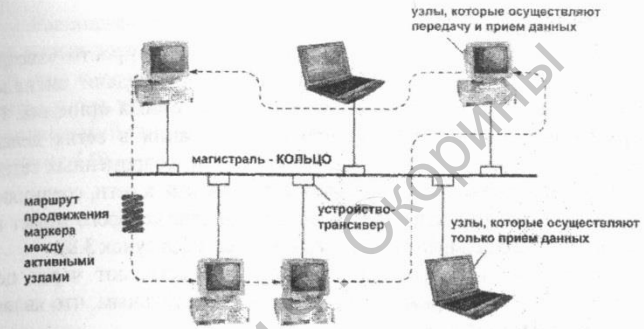


Рисунок 3.6 — Пример работы сети с топологией «кольцо»

Кольца изначально разрабатывались для однонаправленной передачи, позднее были разработаны двунаправленные модификации. В результате этого, если разрывается кольцо передачи в одном направлении, данные все же могут достигнуть пункта назначения, перемещаясь в обратном направлении по другому кольцу.

Расширяемость сети, то есть степень простоты добавления новых элементов, в отличие от топологии «шина», – достаточно трудоемкий процесс, особенно если вновь подключаемый элемент расположен в стороне от уже существующей кабельной проводки.

На текущий момент топологией «кольцо» пользуются сетевые архитектуры Token Ring и FDDI (рисунок 3.7).

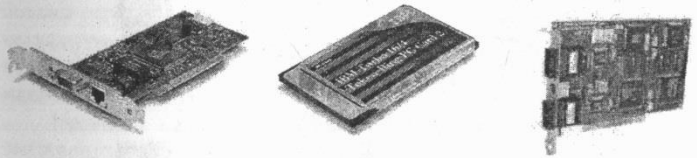


Рисунок 3.7 — Примеры сетевых адаптеров для кольцевых топологий

Перспективы применения этой топологии в чистом виде – довольно туманны (в том числе для FDDI), но ее принципы наследуются в комбинированных схемах топологий.

3.4 Топология «звезда»

Звездообразная топология (star topology), или просто «звезда» (далее звезда), является старейшим способом передачи сигналов, имеющим свое начало в коммутационных телефонных станциях. Несмотря на возраст, достоинства при использовании в сетях делают звездообразную топологию удачным выбором для современных сетей.

В этом случае все компьютеры, подключаемые к сети, соединяются кабелем с «центральным элементом», в качестве которого может использоваться специальный компьютер – узел сети (рисунок 3.8).

Сигналы от передающего компьютера поступают через центральный элемент (например, сервер) ко всем остальным, что является основой терминальных систем.

Звезда является частным случаем дерева, поэтому сети с топологией звезда образуют иерархически подчиненную систему.

Несмотря на большие расходы кабеля, чем у топологии «шина», топология звезда считается дешевой, а поэтому – довольно распространенной. Максимальная скорость передачи ограничена типом центрального элемента и возможностями передающей среды. Надежность центрального элемента является узким местом и основным недостатком сети.

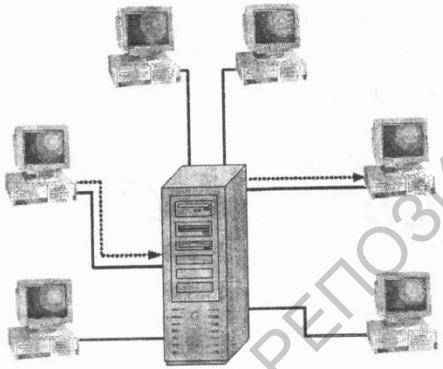


Рисунок 3.8 – Передача информации в топологии «звезда»

С точки зрения организации качественного обслуживания запросов пользователей (например, при организации работы сети терминальных клиентов) данная структура остается актуальной.

Расширяемость такой сети, то есть степень простоты добавления новых элементов, довольно высокая. Достаточно соединить новый узел с центральным элементом сети. Если свободных портов в центральном элементе нет, его можно заменить или установить дополнительный специализированный многопортовый сетевой адаптер (рисунок 3.9).

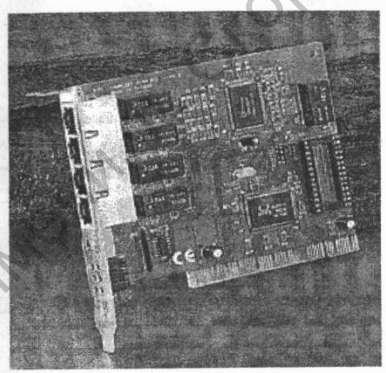


Рисунок 3.9 – Многопортовый сетевой адаптер Ethernet NEXLAN

Недостатком «звезды» является то, что центральный элемент является единственной точкой отказа и при выходе его из строя все подключенные узлы теряют возможность передачи данных.

Другим недостатком является то, что для «звезды» требуется больше кабеля, чем для «шины», но этот недостаток уже считается несущественным, поскольку кабельные системы топологии «звезда», как правило, поддерживают гораздо более высокие скорости информационного обмена.

Несмотря на то, что прямая физическая коммутация «рабочая станция» ⇒ «сервер» позволяет получить пользователю максимальную скорость обслуживания сетевых запросов, сервером на практике такая схема применяется редко. Причиной этого можно считать сложность в обеспечении эффективной связи между клиентами сети, либо одновременную связь рабочих станций с несколькими серверами.

Более дешевой практической реализацией топологии «звезда» стали комбинированные варианты топологий «звезда-шина» и «звезда-кольцо» со специализированным центральным элементом.

3.5 Ячеистая топология

Сеть с ячеистой топологией обладает высокой избыточностью и надежностью, так как каждый компьютер в такой сети соединен с любым возможным участником соединения отдельным кабелем, то есть реализуется принцип «каждый с каждым» (рисунок 3.10).

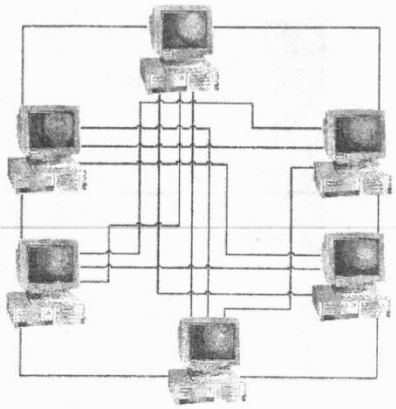


Рисунок 3.10 – Пример сети, построенной по ячеистой топологии

Сигнал от передающего узла к принимающему узлу может проходить по разным маршрутам, поэтому разрыв кабеля не сказывается на работоспособности сети.

Нередко ячеистая топология может быть реализована частично на наиболее важных направлениях в комбинации с остальными топологиями при построении относительно больших сетей (рисунок 3.11).

Высокая скорость доставки сообщений в такой сети обусловлена непосредственной пересылкой от передающего узла к принимающему или по маршруту с минимальным числом пересылок, в случае отсутствия прямого пути.

Такая топология применяется только в тех случаях, когда необходимо обеспечить максимальную надежность и скорость доставки сообщений. Поэтому изначально сети данной топологии проектировались по заказу военных.

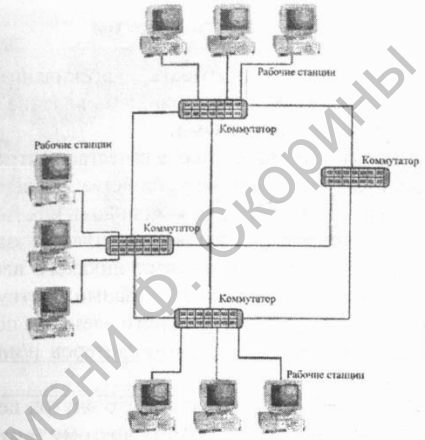


Рисунок 3.11 – Пример сети с элементами ячеистой топологии

Расширяемость сети для такой топологии – очень сложная и дорогостоящая операция, по сравнению с другими топологиями.

Чаще всего отдельные элементы этой топологии реализованы в глобальных сетях, для чего используются линии связи общего доступа. Большие затраты на прокладку кабеля компенсируются высокой надежностью и простотой обслуживания.

Ячеистая топология является весьма перспективной. Сейчас она постепенно вытесняет топологию «кольцо» в структуре сетей SONET (рисунок 3.12).

Рисунок 3.12 – Ячеистая структура, наложенная поверх кольца SONET

3.6 Комбинированные топологии

Уровень надежности и стоимость обслуживания кабельной системы в топологии «звезда» обусловили появление ее популярных комбинаций с другими топологиями.

В комбинированных топологиях в качестве центрального элемента используются специализированные устройства: концентраторы, коммутаторы, мосты, маршрутизаторы, их комбинации или гибриды.

Поскольку физически реализована топология «звезда», выход из строя одного компьютера не оказывает никакого влияния на сеть – остальные компьютеры по-прежнему взаимодействуют друг с другом, и лишь выход из строя центрального элемента повлечет за собой остановку подключенных к нему компьютеров и/или подчиненных центральных элементов.

Логическое управление сетью скрыто внутри центрального элемента и может соответствовать любому другому типу топологии.

К наиболее распространенным видам комбинированных топологий относятся следующие:

– топология *«звезда-шина» (star-bus)* – это комбинация топологий «шина» и «звезда» (рисунок 3.13). Логически это выглядит так: несколько сетей и даже отдельных узлов с топологией «звезда» объединяются при помощи магистральной линейной шины «начинкой» центрального элемента — HUB. Физически такое объединение осуществляется по топологии «звезда»;

– топология *«звезда-кольцо» (star-ring)* кажется очень похожей на «звезду-шину». Отличие в том, что в «звезде-кольце» объединяемые элементы (подсети или отдельные узлы сети) на основе центрального элемента – MAU образуют логическое кольцо (рисунок 3.13).

Другие образцы современного активного сетевого оборудования, используемые в качестве центрального элемента, – коммутаторы, реализуют одновременную передачу нескольких информационных сигналов, что соответствует принципу топологии *«звезда-ячейка» (star-mesh)*.

Применение в качестве центрального элемента активного устройства, рассчитанного на объединение с себе подобными в плоскостные или иерархические структуры (рисунок 3.14), серьезно удешевляет стоимость сети по сравнению с первоначальной топологией «звезда». Этот факт позволил комбинированным топологиям серьезно потеснить применение последней при проектировании локальных сетей.

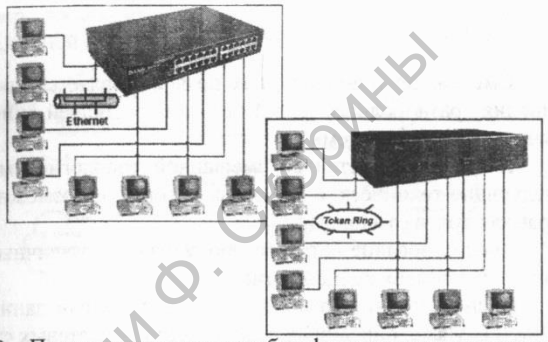


Рисунок 3.13 – Пример внешнего подобия физических структур сетей с комбинированными топологиями «звезда-шина» и «звезда-кольцо»

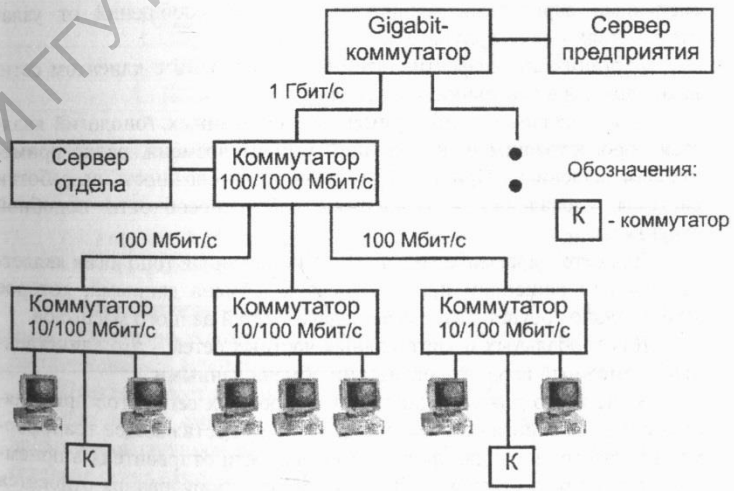


Рисунок 3.14 – Каскадное объединение центральных элементов для увеличения масштаба сети

3.7 Смешанные топологии

Смешанная топология, как правило, является продуктом объединения разнородных сетей в рамках общей информационно-вычислительной системы.

К свойствам сетей со смешанной топологией можно отнести следующие технические моменты, которые невозможно реализовать в рамках других топологий:

- использование сетевого оборудования различных сетевых архитектур в рамках единой сети;
- использование разнородных сред передачи данных (за исключением случаев, описанных спецификациями сетевых стандартов);
- возможность объединения в одну информационно-вычислительную систему архитектурно несовместимых вычислительных комплексов и машин;
- организация эффективного обмена информацией в сетях с несколькими вариантами маршрутов доставки сообщений от узла-отправителя к узлу-получателю;
- организация эффективного обмена данными с клиентом сети, находящимся в состоянии движения.

Для локальных сетей применение смешанных топологий является дорогостоящим и, на текущий момент времени, редко применяемым решением. Причиной этого является сложность разработки системы управления и поддержки работоспособности подобной структуры.

Для сетей масштаба города (SAN) смешанная топология является удобным решением при организации обмена данными, которое максимально соответствует всем задачам сетей данного масштаба.

Для глобальных и виртуальных частных сетей – это единственный возможный вариант реализации обмена данными.

Чаще всего для объединения разнородных сегментов применяется специализированное оборудование, осуществляющее трансформацию пакетов из вида, приемлемого для сети отправителя в приемлемый для сети назначения. К числу такого оборудования относятся мосты, маршрутизаторы, шлюзы и их гибриды.

При использовании иерархических схем объединения сетевых сегментов, одна из используемых топологий будет считаться сетеобразующей, а остальные будут выступать в качестве расширения.

Например, топология «звезда» является сетеобразующей для следующей сложной сети (рисунок 3.15).

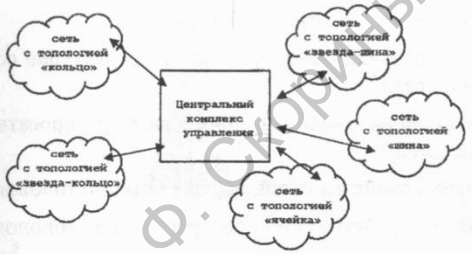


Рисунок 3.15 – Иерархическая сеть

В других случаях сеть верхнего уровня не считается сетеобразующей, а выполняет только функцию общей информационной магистрали (рисунок 3.16).

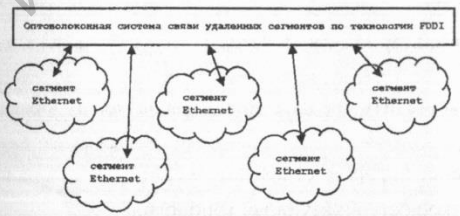


Рисунок 3.16 – Локальная сеть Ethernet с использованием скоростной магистрали дальнего действия FDDI

Таким образом, можно видеть, что смешанные топологии могут быть изначально заложены в проект сети, чтобы иметь возможность воспользоваться лучшими из их характеристик.

Практика построения и эксплуатации сетевых технологий показала, что иногда смешанная топология может также стать средством применения специализированного оборудования, несовместимого с сетевым стандартом основной сети. Например, в банковских сетях, построенных по стандарту Ethernet, до сих пор могут применяться быстродействующие системы матричной печати, которые подключаются к сети по стандарту Xerox Network System. Промежуточным звеном объединения сетей в этом случае может служить дополнительный узел сети, выполняющий функции шлюза.

Вопросы для самоконтроля

1 Определите понятие топология сети.

2 В чем разница между физической структурой сети и логической структурой сети?

3 Какие виды топологий применяют при проектировании компьютерных сетей?

4 Каковы свойства сетей, построенных по топологии «шина»?

5 Каковы свойства сетей, построенных по топологии «кольцо»?

6 Каковы свойства сетей, построенных по топологии «звезда»?

7 Каковы свойства сетей, построенных по топологии «ячейка»?

8 Каковы свойства сетей с комбинированными топологиями?

9 Изобразите схематично некоторые примеры смешанных топологий.

10 Какие альтернативные сетевые структуры вы можете назвать и описать?

11 Как вычислить среднее число шагов между узлами в топологии сети?

12 Что такое иерархическая топология?

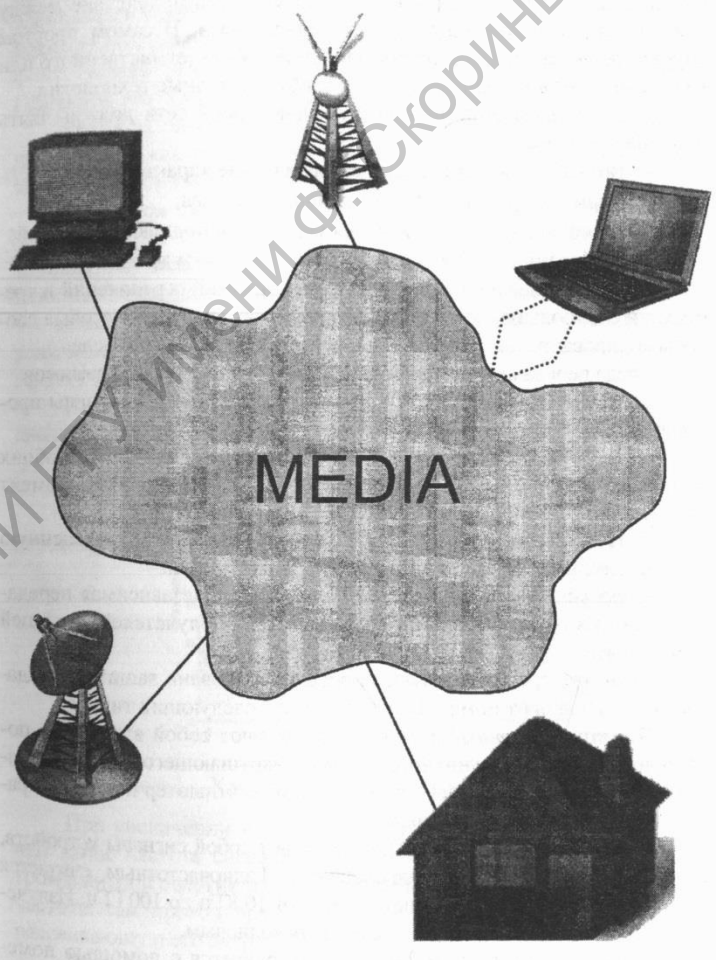
13 Что такое сетеобразующая топология?

14 Какие кабельные системы применяются в различных сетевых топологиях?

15 Можно ли сравнивать надежностные характеристики сетей, построенных по различным топологиям?

16 Каково стоимостное соотношение различных сетевых топологий?

4 Среда передачи данных



4.1 Понятие среды передачи данных

Под средой передачи данных следует понимать набор оборудования, с помощью которого осуществляется взаимодействие между участниками соединения в рамках сеанса связи. В самом простом случае среда передачи реализована в виде кабеля (единственного или в составе группы) и/или задействуются беспроводные технологии.

Для использования кабеля в компьютерной сети должны быть однозначно описаны:

- тип кабельной системы и ее физические характеристики;
- формы и уровни информационного сигнала;
- способы разветвления среды передачи и подключения к ней;
- требования, выставляемые к сетевому оборудованию.

При использовании беспроводных технологий ограничений и требований еще больше, поскольку каждая из этих сред имеет особые способы кодирования, декодирования и применения сигнала в среде.

Среда передачи может работать в одном из следующих режимов:

Симплексная передача. Однонаправленный канал, сигналы проходят по нему всегда только в одном направлении.

Полудуплексная передача. Сигналы могут передаваться в обоих направлениях по единственному каналу связи, но в каждый момент времени сигналы передаются только в одну сторону.

Дуплексная передача. Данный способ реализует полноценную двустороннюю связь по единственному каналу связи.

Многоканальная передача. Одновременная независимая передача от многих отправителей к такому же числу получателей по общей линии связи.

Свойства среды передачи определяют уровень защиты передаваемых сигналов от помех. Помехи бывают следующих типов:

Электромагнитные помехи представляют собой вторжение постороннего электромагнитного сигнала, нарушающего форму полезного сигнала. В этом случае принимающий компьютер не может правильно интерпретировать сигнал.

Радиочастотные помехи представляют собой сигналы устройств, излучающих сигналы на радиочастотах. Радиочастотным считается электромагнитное излучение на частотах от 10 КГц до 100 ГГц. Излучение от 2 до 10 ГГц называется также микроволновым.

Влияние радиочастотных помех устраняется с помощью помехозащитных фильтров, применяемых в различных типах сетей.

Перекрестные помехи. К этому типу помех относятся сигналы проводов, расположенных на расстоянии нескольких миллиметров друг от друга. Протекающий по проводу электрический ток создает электромагнитное поле, которое генерирует сигналы в другом проводе, расположенном рядом. Довольно часто, разговаривая по телефону, можно услышать приглушенные разговоры других людей. Причиной этого являются перекрестные помехи.

Перекрестные помехи значительно уменьшаются, если скрутить два провода, как это сделано в витой паре. Чем больше витков приходится на единицу длины, тем меньше влияние помех.

Затухание сигналов. Проходя по кабелю, электрические и оптические сигналы становятся все слабее. Чем больше расстояние до источника, тем слабее сигнал. Такое ослабление сигнала с расстоянием называется затуханием сигнала. Затухание является причиной того, что в спецификациях различных сетевых архитектур указывается ограничение на длину кабеля. Если это ограничение соблюдается, то эффект затухания не повлияет на нормальную работу канала связи.

Различные среды передачи данных имеют различные допуски по диапазону рабочих частот и скорости затухания сигнала (рисунок 4.1).

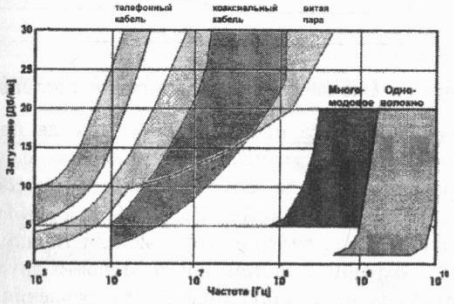


Рисунок 4.1 – Характеристики кабельных сред передачи данных

При увеличении частоты затухание увеличивается, потому что, чем выше частота сигнала, тем интенсивнее рассеивание его электромагнитной энергии в окружающее пространство. При увеличении частоты сам провод превращается из носителя сигнала в антенну, рассеивающую его энергию в пространство.

Все стандарты, относящиеся к среде передачи данных, описываются на физическом уровне модели OSI.

4.2 Простейшие схемы соединения компьютеров в сеть

Для того чтобы организовать сетевое взаимодействие или сеанс связи между двумя компьютерами, можно использовать один из двух методов:

- использование стандартных портов ввода-вывода;
- использование специализированных устройств связи.

Практически любой внешний информационный порт компьютера можно применять для организации сеанса связи. К их числу относятся: COM, LPT, USB, IEEE 1394. Данный вид связи поддерживается на уровне операционной системы, может быть интегрирован в оболочку управления файлами или реализован в виде отдельного программного модуля.

Связать два компьютера через последовательный порт – задача достаточно простая. Для этого необходимо соединить COM-порты компьютеров по схеме, указанной на рисунке 4.2. Соединение получило название null-modem и позволяет получить скорость информационного обмена до 115 000 бит/с.

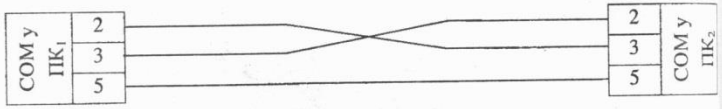


Рисунок 4.2 – Схема соединения контактов последовательного порта

Широкая полоса пропускания и высокая производительность шины IEEE 1394 обеспечивают одновременное функционирование в сети (рисунок 4.3) видеомагнитофонов, видеокамер, DVD/CD-проигрывателей, аудио-комплексов, телевизоров HDTV, кабельного и спутникового телевидения, спутниковых терминалов связи, модемов xDSL, охранных систем, компьютеров и других устройств [4]. Скорость передачи до 1 600 Мбит/с. Для сравнения, скорость передачи Hi-Speed USB – 480 Мбит/с.

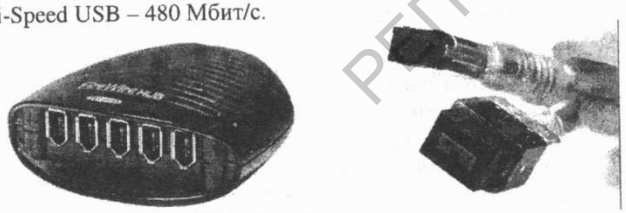


Рисунок 4.3 – FireWire-коммутатор и кабельные разъемы

В качестве специализированного оборудования средств организации связи также могут быть использованы модемы через соединение «null-modem», оборудование сотовых операторов (рисунок 4.4), сетевые адаптеры через cross-кабель [10,12], свитчеры.

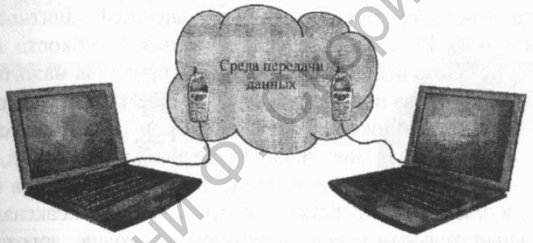


Рисунок 4.4 – Соединение через сети операторов сотовой связи

В беспроводных сетях всегда необходима установка дополнительного оборудования. Исключение составляют типы компьютеров, в которых оно установлено по умолчанию, например мобильные и портативные системы. Примером такой связи является технология Bluetooth (рисунок 4.5), которая, являясь стандартом для беспроводного подключения различных устройств, включает в себя поддержку многих функций (передача голоса, синхронизация данных, передача файлов, использование факса и модема и других) на скорости до 11 Мбит/с.

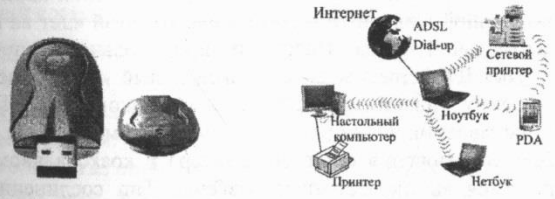


Рисунок 4.5 – Внешний вид Bluetooth-модуля и способ его применения

В Bluetooth адаптеры выступают не в качестве сетевых плат, а в роли последовательных портов, через которые средствами операционной системы организуется прямое подключение. При этом одна сторона выступает в качестве сервера доступа, а вторая – удаленного клиента. Хотя возможна работа одного сервера одновременно с несколькими клиентами (до 7), но два клиента, подключенных к одному серверу, друг друга не видят.

4.3 Коаксиальный кабель

Коаксиальный кабель (COAX) применяется для передачи электрических импульсов. Он состоит из центральной медной жилы в диэлектрической оболочке, поверх которой нанесена металлическая оплетка, и вся конструкция защищена внешней защитной оболочкой (рисунок 4.6). [6] Для обеспечения большей гибкости центральная жила может быть набрана из нескольких проводов малого сечения.

Различают два вида коаксиального кабеля: толстый (около 1 см в диаметре) и тонкий (около 5 мм в диаметре). Тонкий коаксиальный кабель применяется для монтажа во внутренних помещениях, а толстый – для магистральных линий внутри зданий и между ними (в шахтах, тоннелях и в пленумных полостях). Встречаются виды коаксиального кабеля с дополнительным внешним экраном. Он толще, дороже и сложнее при монтаже, а потому сфера его применения ограничена.

Коаксиальный кабель для прокладки между зданиями должен удовлетворять дополнительным требованиям. Различают два вида кабеля для этих работ:

– для прокладки в туннелях, шахтах или коробах;

– для воздушного монтажа (в этом случае кабель сращивают со специальным тонким металлическим тросом).

Коаксиальный кабель используется в топологии «шина», где обязательно использование оконечных терминаторов. Эффективная длина сегмента зависит от удельного сопротивления кабеля, толщины центральной жилы и типа материала, который идет на изготовление центральной жилы. Например, при удельном сопротивлении 50 Ом (Novell/Ethernet) медный коаксиальный кабель имеет эффективную длину: тонкий около 200 м, толстый около 500 м. При удельном сопротивлении 93 Ом (ArcNet) – более 610 м.

Для подключения сетевого адаптера к коаксиальному кабелю используются высокочастотные разъемы. Тип соединения зависит от типа кабеля: тонкий подключается «в разрыв» с помощью Т-коннектора (рисунок 4.7, а), а для толстого применяется контактная врезка (на кабель устанавливается разъем типа «вампир» или «зуб», который в свою очередь подключается к сетевому адаптеру с помощью внешнего трансивера) (рисунок 4.7, б).

Возможности коаксиального кабеля пока не исчерпаны современными сетевыми технологиями, таким образом, его использование в обозримом будущем будет продолжаться.

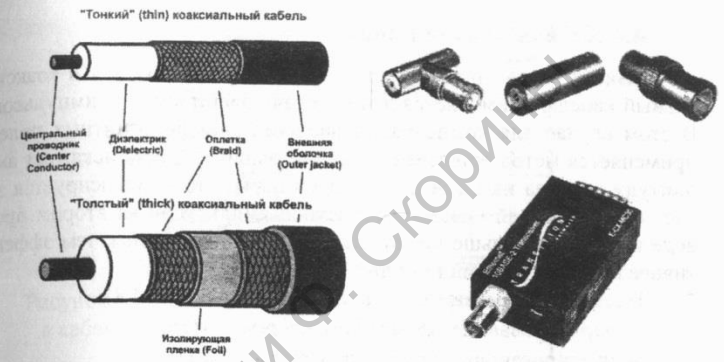


Рисунок 4.6 – Структура коаксиального кабеля

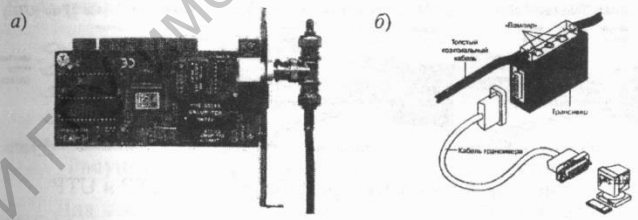


Рисунок 4.7 – Примеры подключения к коаксиальному кабелю: *а*) тонкий коаксиальный кабель; *б*) толстый коаксиальный кабель [2]

Для того, чтобы сеть Ethernet, состоящая из сегментов различной физической природы (например, сочетание «толстый»-«тонкий» Ethernet), работала корректно, необходимо, чтобы выполнялись три основных условия:

– количество станций в сети не превышает 1024;

– удвоенная задержка распространения сигнала (Path Delay Value, PDV) между двумя самыми удаленными друг от друга станциями сети не превышает 575 битовых интервалов;

– сокращение межкадрового расстояния IGS (Interpacket Gap Shrinkage) при прохождении последовательности кадров через все повторители не более, чем на 49 битовых интервалов (начальное межкадровое расстояние – 96 битовых интервалов). Суммарную величину уменьшения межкадрового интервала при прохождении всех повторителей в спецификациях обозначают – PVV (Path Variability Value).

4.4 Кабель «витая пара»

«Витая пара» (далее просто – витая пара), также как и коаксиальный кабель, применяется для передачи электрических импульсов. В этом случае для компенсации внешних электромагнитных полей применяется метод естественной компенсации. Помеха искажает амплитуду сигнала на один из проводов пары, что компенсируется за счет симметричной наводки с обратной амплитудой на втором проводе пары. Чем больше число витков на единицу длины, тем эффективнее работает данный принцип.

Витые пары бывают следующих типов (рисунок 4.8):

- экранированная (*shielded twisted pair – STP*);
- изолированная (*screened twisted pair – ScTP*);
- неэкранированная (*unshielded twisted pair – UTP*).

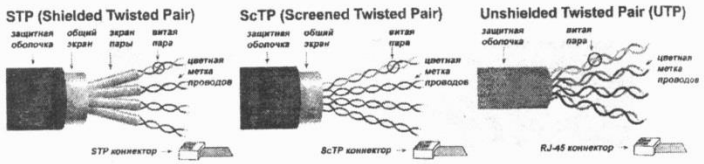


Рисунок 4.8 – Структура кабелей STP, ScTP и UTP

Экранированная витая пара (STP) и изолированная витая пара (ScTP) дороже при производстве, поэтому для проектирования сетей чаще применяется неэкранированная витая пара (UTP).

Витую пару UTP принято классифицировать по категориям. В качестве UTP категории 0 может быть использован двойной провод в жесткой оболочке, применяемый в аналоговых сетях, например, телефонных. Начиная с UTP категории 3, витая пара включает 4 попарно свитых проводника. Сравнительно недавно, одновременно с разработкой стандартов для гигабитных технологий передачи данных, производители стали предлагать кабели с улучшенными частотными свойствами, которые стали позиционироваться как кабели UTP категорий 6 и 7. Электрические характеристики этих витых пар намного превосходят аналогичные характеристики кабелей UTP старого образца (рисунок 4.9).

Витую пару применяют в сетях с топологиями: «*кольцо*», «*звезда*», «*ячейка*». Максимальный скоростной режим для современных локальных сетей с использованием UTP ограничен 1 Гбит/с.

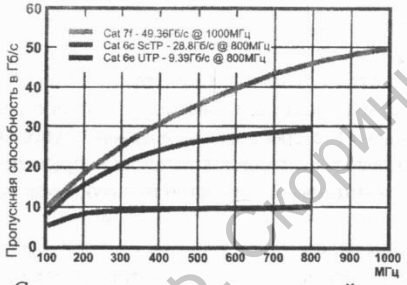


Рисунок 4.9 – Сравнение допустимых скоростей передачи данных в кабеле UTP категорий 6 и 7 при увеличении частоты сигнала

Для коммуникации применяется комбинация настенных розеток, в том числе pach-панели, и соединительные штекеры RJ-45 (рисунок 4.10), в устаревших системах (например, ArcNet) – RJ-11.

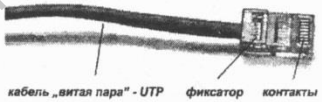


Рисунок 4.10 – Кабель «витая пара» с коннектором RJ-45

Для соединения настенной розетки с сетевым адаптером или pach-панели с хабом применяются кабели patch-cord (прямая расшивка). Для соединения сетевых устройств или напрямую двух сетевых адаптеров применяются кабели cross-cord (cross-кабель). Разводка проводов cross-кабеля показана на рисунке 4.11.

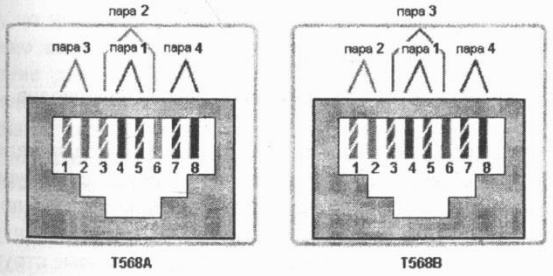


Рисунок 4.11 – Схема «расшивки» cross-кабеля Ethernet (согласно стандартам EIA/TIA 568A–568B)

4.5 Волноводы

Если частота передачи достаточно высока, то электрическая и магнитная составляющие сигнала могут распространяться в свободном пространстве (не требуется сплошной проводник). [4] Для того чтобы сигнал распространялся в нужном направлении с наименьшими помехами и потерями, иногда используют такую среду, как волновод.

Виды волноводов:

– *металлический волновод* – металлический волновод представляет собой полую металлическую трубку круглого (рисунок 4.12) или прямоугольного сечения. Электромагнитные волны могут распространяться по волноводу, отражаясь от стенок.

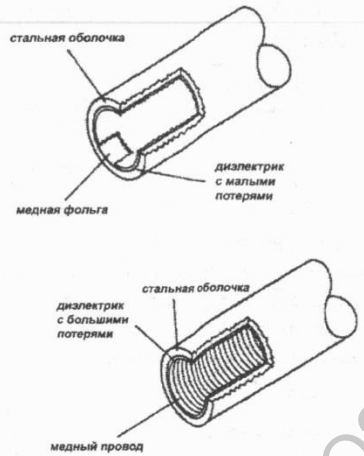


Рисунок 4.12 – Структура строения волноводов

В результате интерференции отраженных под определенными углами волн образуются направляемые волновые структуры с синусоидальным или близким к нему распределением поля в поперечном сечении. При этом амплитуды направляемых волн описываются функциями от поперечных координат. Такие волновые структуры называются модами (от англ. *mode*). В кабеле эти моды являются мешающими, паразитными.

В волноводе же, при отсутствии центрального провода уже не может распространяться «кабельная» волна, но одна из мод может быть использована для передачи сигнала.

Металлические волноводы получили применение в качестве линий передачи сантиметровых и миллиметровых волн. При уменьшении длины волны уменьшаются поперечные размеры волновода и возрастают потери мощности волны в стенках. Поэтому для волн с длинами порядка миллиметра и короче волноводы применяются лишь на очень короткие расстояния.

Металлические волноводы применяют на частотах от 2 до 110 ГГц для соединения сверхвысокочастотных передатчиков и приемников с антеннами. В волноводы под повышенным давлением закачивается сухой воздух или чистый азот. Это делается с целью снижения влажности, поскольку в сверхвысокочастотном диапазоне она существенно увеличивает затухания. Прокладка волноводной линии при условиях, которые требуется выполнить (прямолинейность трассы и др.), оказывается очень дорогостоящей, поэтому их применение не стало массовым;

– *диэлектрический волновод* – диэлектрический волновод – это стержень из диэлектрического материала, в котором могут распространяться электромагнитные волны с малыми потерями. Для волн миллиметрового диапазона это полистирол и полиэтилен (фторопласт), малопоглощающие, так называемые неполярные диэлектрики. Электромагнитная волна может распространяться внутри стержня, отражаясь от его границ под углом полного внутреннего отражения. Как и в металлическом волноводе, при интерференции образуются направляемые волны – моды. При этом нет потерь мощности в металле, но имеют место потери в диэлектрике. Эти потери все же достаточно велики, поэтому диэлектрические волноводы получили применение для передачи сигнала на миллиметровых волнах на сравнительно короткие расстояния (метры, десятки метров).

Однако диэлектрические волноводы оказались чрезвычайно перспективными для применения в диапазоне световых волн, точнее, в диапазоне инфракрасных волн с длиной волны порядка микрометра. Они представляют собой волокна из стекла, поэтому получили название оптических волокон или волоконных *световодов*.

В современных высокоскоростных сетях используется *волоконно-оптический кабель*, по сути являющийся диэлектрическим волноводом.

4.6 Оптоволокно

Оптоволокно используется для передачи информационного сигнала в виде оптического импульса и допускает использование одного световода для организации нескольких сеансов связи одновременно в обоих направлениях. Если это реализовано, то кабельная система называется многомодовой, если нет – одномодовой.

Во многомодовом оптоволокне есть два варианта организации одновременного двустороннего обмена несколькими участниками соединения через один световод:

– со сдвигом фаз одной длины световой волны;

– с использованием разных длин световых волн.

Пример распространения оптического сигнала в кабеле показан на рисунках 4.13 – 4.15, структура и способ соединения оптоволокна – на рисунке 4.16.

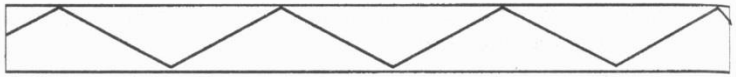


Рисунок 4.13 – Траектория световых импульсов в одномодовом оптоволоконном кабеле

Рисунок 4.14 – Траектория световых импульсов во многомодовом оптоволоконном кабеле с использованием сдвига фаз

Рисунок 4.15 – Траектория световых импульсов во многомодовом оптоволоконном кабеле с использованием сдвига длины волны

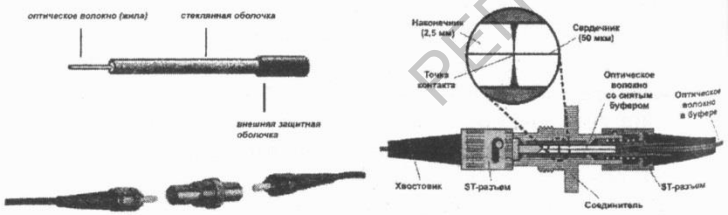


Рисунок 4.16 – Структура оптоволокна и способ его соединения

Оптоволокно состоит из одной или нескольких стеклянных или пластиковых жил (световодов), покрытых слоем стекла, которое, в свою очередь, заключено в поливинхлоридную оболочку. Для генерации световых импульсов используется один из двух источников света:

– *светодиоды* обычно используются в одномодовом режиме, интенсивность импульсов невелика;

– *полупроводниковые лазеры* генерируют интенсивный, хорошо сфокусированный световой импульс заданного цвета. Они используются в многомодовом режиме.

Технология изготовления оптических кабелей такова, что механические характеристики их значительно превосходят медные кабели на витой паре UTP. Для сравнения можно привести допустимые усилия на разрыв при прокладке кабеля, которые для оптоволокна составляют 100 кг, а для витой пары – 15 кг (согласно спецификации кабелей). Такая прочность оптоволокна достигается за счет применения современных высокопрочных полимерных нитей (например, арамидных нитей) и центральной упрочняющей жилы, в качестве которой иногда используется стальной трос малого сечения.

Важное свойство оптического волокна – долговечность. «Время жизни» волокна, то есть сохранение им своих свойств в допустимых пределах, достигает 25 лет для пластиковых световодов и гораздо дольше при использовании стеклянных световодов, что позволяет проложить оптико-волоконный кабель во время монтажа сети и, впоследствии, наращивать пропускную способность сети путем замены активного оборудования на более современные образцы.

Оптоволокно применяют в топологиях: «звезда», «кольцо», «ячейка» или их комбинации. Максимальная скорость передачи данных в этой среде, полученная в экспериментальных условиях, достигает 3 Тбит/с.

4.7 Структурированные кабельные системы

В настоящее время по мере того, как все большее количество пользователей переходят к применению открытых систем, выпускаемое активное оборудование проектируется на основе положения, что кабельная часть информационной инфраструктуры соответствует требованиям стандартов, то есть является гарантированно надежной и способной обеспечивать определенные рабочие характеристики.

К различным рискам, являющимся следствием нестандартных кабельных систем, можно отнести следующие: сетевые рабочие характеристики ниже определенных стандартами, повышенная стоимость внесения изменений в систему и неспособность системы поддерживать новые технологии. По мере распространения принципов структурированного кабелирования стоимость устанавливаемого сетевого оборудования падает, а эффективность передачи данных растет с экспоненциальной зависимостью. [13]

Проектирование структурированной кабельной системы (СКС) разделяется на две основные стадии: *архитектурную* и *телекоммуникационную*. Основной задачей архитектурной стадии является определение общей структуры СКС, оптимальной по комплексу технико-экономических характеристик в процессе создания и последующей эксплуатации. Телекоммуникационная стадия чаще всего начинается после окончания архитектурной, а иногда и после завершения капитальных строительно-монтажных работ. В этот период уточняется конкретная структура СКС, составляется перечень необходимого оборудования, планы его размещения и т. д.

В самом общем случае СКС включает в себя три подсистемы:

– подсистема внешних магистралей (первичная) – является основой для построения сети связи между компактно расположенными на одной территории зданиями (кампус);

– подсистема внутренних магистралей (вторичная или вертикальная) связывает между собой отдельные этажи здания и/или пространственно разнесенные помещения в пределах одного здания;

– горизонтальная (третичная) подсистема образована внутренними информационными кабелями между сетевым оборудованием и информационными розетками рабочих мест, самими информационными розетками, коммутационным оборудованием и соединительными кабелями.

Для размещения оборудования используется стандарт, включающий в себя способы коммутации, энергообеспечения и защиты оборудования от несанкционированного доступа. Одним из центральных элементов этого стандарта (как с точки зрения топологии сетей, так и с точки зрения организации энергоснабжения, коммутации и защиты) являются коммуникационные шкафы.

Коммуникационные шкафы (рисунок 4.17) в общем случае рассматриваются как конструкции, предназначенные для обслуживания горизонтальной распределительной системы. Кроме этой основной функции, они могут выполнять и дополнительные – в них допускается размещение промежуточных и главных кроссов.

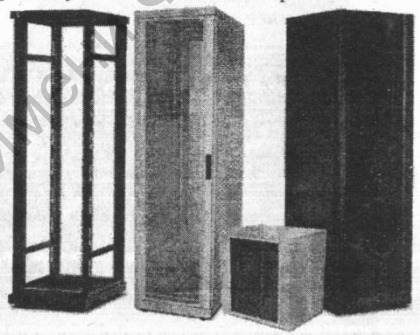


Рисунок 4.17 – Примеры коммуникационных шкафов и стоек

Для успешного размещения оборудования в коммуникационных шкафах требуется организация высокого уровня совместимости по геометрическим параметрам крепежных элементов.

Стандартный размер коммуникационных шкафов предписывает размер ~ 465 мм по горизонтали и шаг (межосевое расстояние для крепежных отверстий) ~ 17 мм по вертикали. Габарит такого шкафа определяется как 19". Существует и «расширенный» стандарт на 23".

По высоте шкафы измеряются в юнитах (количестве единиц оборудования) «U»: 4U (280 мм), 6U (345 мм), 9U (478 мм), 12U (612 мм), 15U (746 мм), 18U (878 мм), 21U (1012 мм) и выше.

Системы энергоснабжения оборудования и источники бесперебойного питания размещаются внутри коммуникационных шкафов, так что следует учитывать этот факт при выборе размеров коммуникационного шкафа для конкретного проекта сети.

4.8 Коммуникация в структурированных системах

Кабельные системы являются лишь носителем (средством передачи) данных в сети. Основой сети является сетевое оборудование. Большая его часть собирается в коммуникационных стойках или шкафах, и его объединение в сеть представляет серьезную проблему, которая может быть сформулирована следующим образом: *чем больше структуризация системы, тем меньше задокументирована и систематизирована сама структура связей между оборудованием.*

Внутри коммуникационной стойки образуется хаотически переплетенный жгут проводов (рисунок 4.18), и процесс поиска нужного кабеля занимает существенное время.

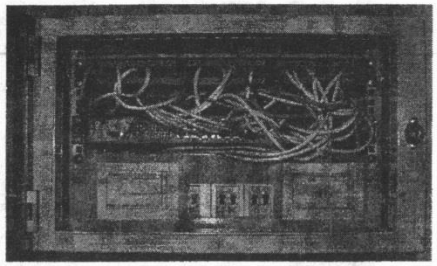


Рисунок 4.18 – Пример коммутации сети для учебного класса

В качестве решения данной проблемы были разработаны системы комбинированной коммутации, применяемые для серверных решений типа «Blade». В этом случае система коммутации базируется на внутренних шинах специального серверного шасси (рисунок 4.19).

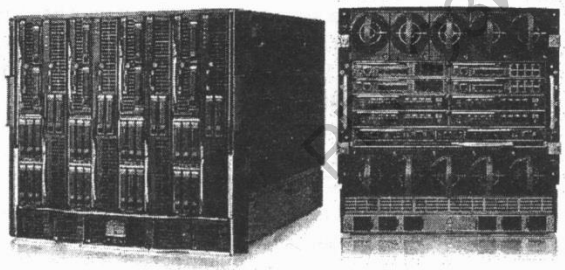


Рисунок 4.19 – Шасси HP BladeSystem c7000 (виды спереди и сзади)

Коммутационное оборудование имеет порты подключения на передней и задней (магистральной) панели, при этом последние имеют программное управление и могут быть настроены для работы в любой комбинации коммутационных каналов (рисунки 4.20, 4.21).

Рисунок 4.20 – Модуль коммутатора FC для организации SAN

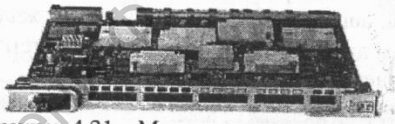


Рисунок 4.21 – Модуль маршрутизатора

Серверные «лезвия» могут иметь различные физический размер, компоновку и состав оборудования. Единственное и обязательное требование – совместимость с шасси Blade-системы (рисунок 4.22).

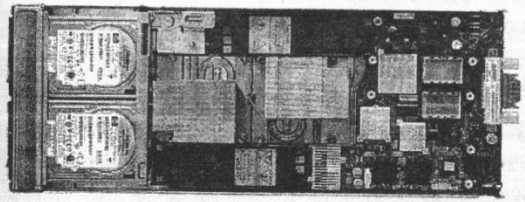


Рисунок 4.22 – Серверное лезвие HP ProLiant BL465c

Все модули, устанавливаемые в шасси современного Blade-сервера, используют общие системы питания и охлаждения, единую коммуникационную среду и средства управления. Все элементы этой системы дублируются. Современные Blade-серверы поддерживают горячую замену всех своих модулей: вычислительных, коммуникационных, блоков питания, вентиляторов.

Использование Blade-серверов позволяет обеспечить свободный доступ к каждому вычислительному или сетевому модулю, отсутствие нагромождения кабелей значительно облегчают задачи установки и замены отдельных устройств, поддержку и эксплуатацию всей системы в целом. Blade-серверы потребляют существенно меньше электроэнергии и занимают гораздо меньше места.

4.9 Оформление кабельных систем

Для укладки информационных и силовых кабелей различного назначения, а также установки розеток и других элементов кабельных систем используются шахты, полости, отверстия в стенах либо декоративные настенные/напольные кабельные короба.

Декоративные короба используются в тех случаях, когда:

– прокладка кабелей другими способами невозможна;

– возникает потребность в защите кабелей от механических повреждений, попаданий брызг воды и других жидкостей;

– необходимо обеспечение высоких эстетических характеристик внутренней отделки офисных помещений.

Кабельные короба представляют собой полые закрытые желоба различных сечений, обязательно имеющие съемную или, по меньшей мере, откидную крышку и предназначенные для монтажа на любой плоской капитальной или декоративной вертикальной поверхности. [13] Наиболее популярны прямоугольные сечения, кроме них производятся трапециевидные, треугольные и полукруглые в сечении короба и декоративные плинтусы.

Короб может быть:

– цельным, т. е. в этом случае он состоит из единого куска пластика, свернутого в короб, и по одному из его ребер имеется разрез с пазами для крепления. С противоположной стороны стенка короба в зоне перегиба имеет меньшую толщину и за счет этого обладает повышенной гибкостью (рисунок 4.23, *а*);

– составным, то есть состоящим из двух компонентов: основания и крышки. Крышки выполняются как П-образными (рисунок 4.23, *б*), так и плоскими (рисунок 4.23, *а*);

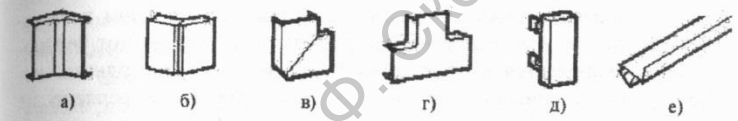
– сборными с поворотной крышкой (рисунок 4.23, *г*);

– других конфигураций.

а) б) в) г) д)

Рисунок 4.23 – Конструкции прямоугольных коробов:
а) цельный; *б*) составной с П-образной крышкой;
в) составной с плоской крышкой; *г*) сборный с поворотной крышкой;
д) напольный короб

Для каждого из типоразмеров короба производители предлагают более или менее полный ряд стандартных комплектующих элементов (рисунки 4.24 и 4.25). Эти элементы существенно расширяют возможности прикладки и монтажа, а также улучшают эстетические характеристики смонтированных коробов.



а) б) в) г) д) е)

Рисунок 4.24 – Дополнительные элементы для кабельных коробов:
а) внутренний угол; *б*) внешний угол; *в*) плоский угол;
г) отвод; *д*) торцевая заглушка; *е*) разделительная стенка

Внедрение структурированной кабельной системы всегда положительно сказывается на характеристиках качества и надежности функционирования оборудования физического уровня.

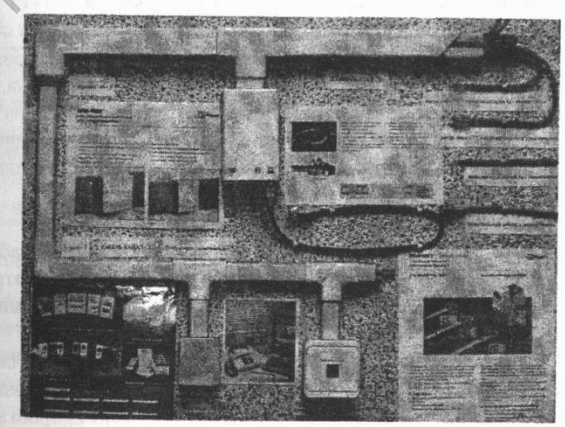


Рисунок 4.25 – Вариант оформления кабельных систем

Основными материалами, из которых изготавливаются декоративные короба, являются ударопрочные полимеры и металлы (например, алюминий или сталь оцинкованная или нержавеющая).

4.10 Беспроводные сети

Технология беспроводных сетей WLAN (Wireless LAN) развивается довольно быстро. Эти сети удобны для подвижных средств, в первую очередь, но находят применение и в других областях (сети с мобильными клиентами, больницы, спортивные состязания и т. д.). [2]

Беспроводные сети имеют три варианта реализации:

– *локальные вычислительные сети* (на беспроводном принципе) – в этом случае единственная разница обычной сети от беспроводной заключается в отсутствии кабельной системы, однако, используемое соединение точка-точка, как правило, закреплено не только за помещением, но и за местоположением самого помещения. В этом случае используется бесперебойная связь. Фиксированный приемопередатчик соединяется кабелем с рабочей станцией. Прием передачи может называться точкой доступа;

– *расширенные локальные вычислительные сети* – в этом случае часть сети реализуется с помощью кабельной сети, а отдельные ее участники обладают большим уровнем мобильности. В некоторых случаях беспроводным соединением может быть радиомост между сегментами кабельной сети. Обратным примером может служить беспроводная сеть, в которой кабелем соединяется система серверов;

– *мобильные сети* – это сети мобильных компьютеров. В более общем случае – это система вычислительных комплексов, объединенная в сеть с помощью любого вида беспроводной технологии.

На текущий момент более популярными являются следующие виды беспроводных технологий:

– *радиосоединение:*

а) узкополосное – одна радиочастота на всех;

б) широкополосное – набор частот – наиболее проработанный и традиционный тип носителя беспроводной связи, несмотря на то, что технология дает плохой уровень защиты от электромагнитных излучений;

– *лазерное излучение* – можно использовать только в случае наличия прямой видимости приемника и передатчика между двумя зданиями. Можно обеспечить достаточно высокую скорость передачи, но надежность связи – низкая из-за того, что луч может рассеиваться или отклоняться (из-за особенностей изготовления оборудования, многие авторы объединяют с инфракрасной связью);

– *инфракрасное излучение* – здесь используется и прямой сигнал, и отраженный; из-за этого поддерживается достаточно низкая скорость распространения сигнала, но обеспечивается высокая надежность передачи;

– *микроволновое соединение* – используется как разновидность радиосоединения – на текущий момент является достаточно дешевой технологией. Недостатки – низкая скорость передачи данных и малый радиус действия;

– *использование сотовых сетей общего доступа* – наиболее удобен для реализации удаленного подключения мобильной станции пользователя к сети предприятия, осуществляющего данную услугу;

– *спутниковые системы* – самая глобальная из беспроводных систем по охвату территории. Недостатки – высокая стоимость передающего оборудования и арендная плата за трафик через спутник.

В последние годы было принято большое количество стандартов, регламентирующих параметры различных видов беспроводных соединений (рисунок 4.26). Это дало толчок к разработке и широкому применению мобильных устройств связи и сопутствующих устройств.

Рисунок 4.26 – Сферы использования беспроводных соединений

К сожалению, беспроводные, особенно мобильные каналы, крайне ненадежны. Потери пакетов в таких каналах весьма вероятны. Понижение скорости передачи, как правило, не приводит к понижению вероятности потери. Кроме того, маршруты между отправителем и получателем неоднородны и могут включать в себя сегменты с различными методами передачи данных (проводные и беспроводные).

!!! Влияние излучений некоторых типов беспроводных передающих устройств на здоровье пользователей сети также вызывает серьезную озабоченность.

Вопросы для самоконтроля

1 Дайте определение среды передачи данных.

2 В каких режимах может работать среда передачи данных?

3 Каким образом можно соединить компьютеры в сеть?

4 Какие характеристики имеет коаксиальный кабель?

5 Какие существуют типы «витых пар»?

6 Назовите основные категории «витой пары» и их характеристики.

7 Объясните физический смысл волновода.

8 Опишите физические явления, протекающие в оптоволоконном кабеле.

9 Дайте понятие мультиплексирования каналов.

10 Опишите возможные коммуникации структурированных кабельных систем.

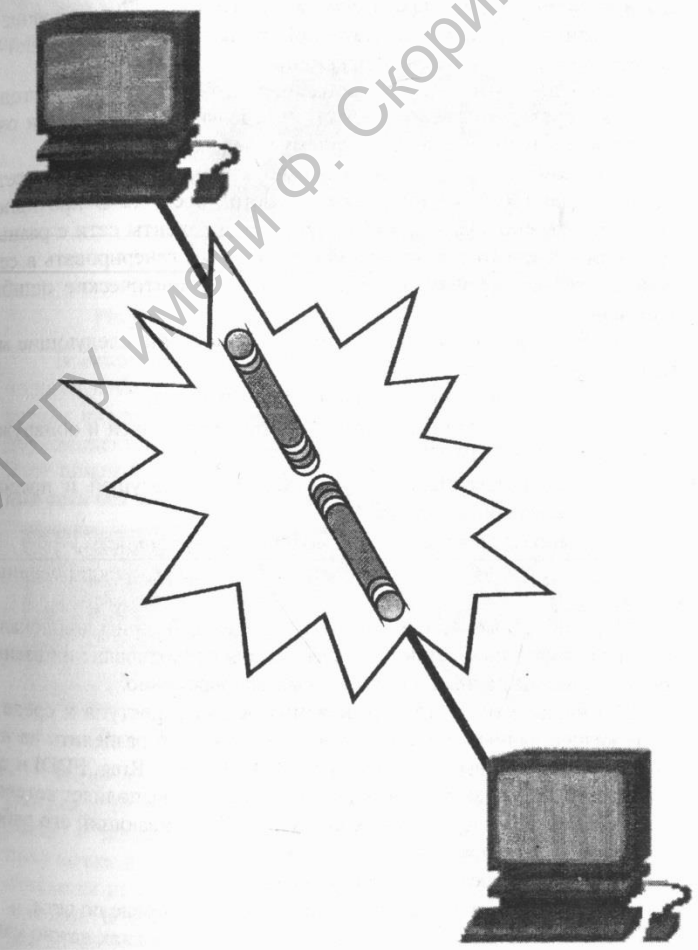
11 Каким образом осуществляется декорирование кабельных систем?

12 Приведите основные виды беспроводных сетей.

13 Раскройте понятие «затухание сигнала».

14 Как происходит одновременная передача информационных сигналов во многомодовом оптоволокне?

5 Методы доступа к среде



5.1 Назначение методов доступа к среде

Передача данных по сети состоит из решения двух задач:

– передать новые данные через кабель без «столкновения» с другими данными, уже передаваемыми по нему;

– принять данные с достаточной степенью уверенности в том, что при передаче они не были искажены.

Эти задачи решаются соблюдением наборов правил (методов доступа к среде), согласно которым определяются приоритет и очередность между узлами сети по приему и передаче сообщений.

Все компьютеры, подключенные к одному сегменту сети, должны использовать один и тот же метод доступа. В противном случае неизбежно возникнет ситуация, когда клиенты сети с разным доступом к среде будут одновременно пытаться генерировать в сеть свой служебный трафик, порождая взаимные критические ошибки передачи.

Наиболее распространены и просты в описании следующие методы доступа к среде:

– метод доступа с использованием маркера;

– множественный доступ с контролем несущей и обнаружением коллизий (CSMA/CD);

– множественный доступ с контролем несущей и предотвращением коллизий (CSMA/CA);

– множественный доступ по приоритету запроса;

– доступ через выделенные каналы связи (фиксированные слоты).

Перечисленные методы доступа к среде характерны для локальных вычислительных сетей. Они служат для предотвращения взаимного разрушения данных, передаваемых одновременно.

В зависимости от поддерживаемых методов доступа к среде и типов кадров данных сетевое оборудование можно разделить на несколько групп (сетевых технологий): Ethernet, Token Ring, FDDI и др. Обработку кадров данных, передаваемых по сети, выполняет сетевой адаптер и драйвер операционной системы, обслуживающий его работу. Совместно они реализуют следующие функции:

– поддерживают метод доступа в сети;

– формируют и анализируют кадры, передаваемые по сети.

Помимо указанных различий в сетевых технологиях важно учитывать и различия в используемых стеках сетевых протоколов.

Важное требование при определении необходимых методов доступа к среде определяется видом среды передачи и количеством таких сред, которые необходимо использовать в рамках сети.

Например, для обеспечения большей универсальности в условиях большого спектра сред передачи разрабатывались сетевые адаптеры и другие виды устройств типа Combo (рисунок 5.1).

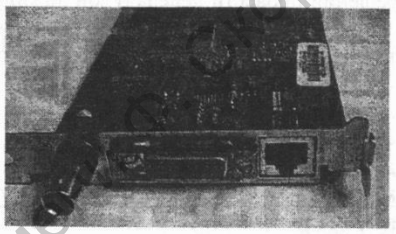


Рисунок 5.1 – Сетевой адаптер Ethernet типа Combo

В некоторых случаях сетевое оборудование не комплектуется полным набором разработанных для него аппаратных модулей для разных видов передающих сред. Пользователь получает возможность доукомплектовать оборудование под требования конкретной сети. Этот прием часто оставляет возможность для частичной модернизации сети без замены оборудования (рисунок 5.2).

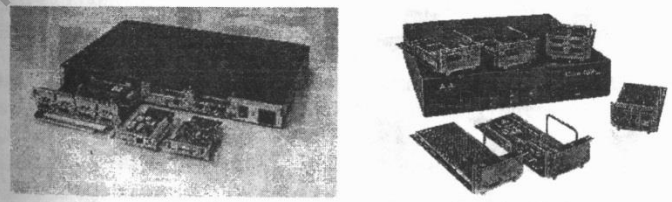


Рисунок 5.2 – Пример модульных маршрутизаторов

В случае выбора конкретной среды передачи и сетевой технологии для всей сети можно реализовать доступ к среде на разной скорости, в зависимости от возможностей оборудования отправителя, получателя и ретранслирующих устройств. Такая поддержка осуществляется на программном уровне производителями сетевого оборудования. В этом случае в характеристиках сетевого оборудования всегда указывается его совместимость по спецификациям IEEE 802.

5.2 Доступ к среде с использованием маркера

Метод с передачей маркера неконкурентный – в нем два компьютера не могут начать передавать сигнал одновременно. В этом случае специальный служебный кадр (*маркер*) курсирует по строго определенной траектории. Если какой-либо из компьютеров нуждается в разрешении провести передачу, он дожидается момента, когда этот маркер приходит к нему, дополняет или заменяет его информацией и отправляет дальше. Получившийся кадр следует дальше, пока не достигнет пункта назначения или не вернется к отправителю.

Когда кадр достигает компьютера, адрес которого указан в заголовке, сетевой адаптер компьютера копирует данные, добавляет к пакету подтверждение об успешном приеме и передает дальше по кругу. Компьютер, передавший эти данные, получает кадр с подтверждением, после чего освобождает маркер, т. е. возвращает его к исходному виду. Этот процесс показан на рисунке 5.3.

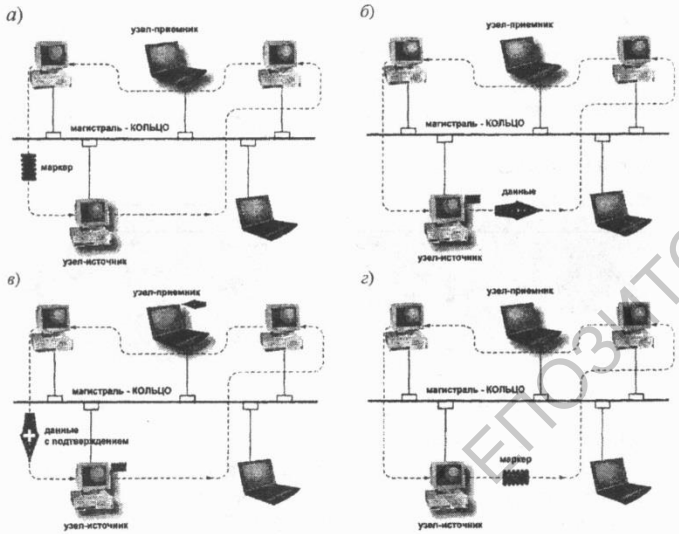


Рисунок 5.3 – Принцип действия маркерного доступа:
а) ожидание маркера; б) передача кадра;
в) возврат кадра; г) освобождение маркера.

Время удержания одной станцией маркера ограничивается *тайм-аутом удержания маркера,* после истечения которого станция обязана передать маркер далее по кольцу. В сетях Token Ring 16 Мб/с используется также несколько другой алгоритм доступа к кольцу, называемый алгоритмом *раннего освобождения маркера (Early Token Release).* В соответствии с ним станция передает маркер доступа следующей станции сразу же после окончания передачи последнего бита кадра, не дожидаясь возвращения по кольцу этого кадра с битом подтверждения приема.

Каждая станция применяет механизмы обнаружения и устранения неисправностей сети, возникающих в результате ошибок передачи или переходных явлений (например, при подключении и отключении станции).

Не все станции в кольце равны. Одна из станций обозначается как *активный монитор,* что означает дополнительную ответственность по управлению кольцом. Активный монитор осуществляет управление тайм-аутом в кольце, порождает новые маркеры (если необходимо), чтобы сохранить рабочее состояние, и генерирует диагностические кадры при определенных обстоятельствах. Активный монитор выбирается, когда кольцо инициализируется, и в этом качестве может выступить любая станция сети. Если монитор отказал по какой-либо причине, существует механизм, с помощью которого другие станции (резервные мониторы) могут договориться, какая из них будет новым активным монитором.

Для различных видов сообщений передаваемым данным могут назначаться различные *приоритеты.* Каждый кадр или маркер получает приоритет, устанавливаемый битами приоритета (от 0 до 7). Станция может воспользоваться маркером, если только она получила маркер с приоритетом, меньшим или равным, чем ее собственный. Сетевой адаптер станции, если ему не удалось захватить маркер, помещает свой приоритет в резервные биты маркера, но только в том случае, если записанный в резервных битах приоритет ниже его собственного. Эта станция будет иметь преимущественный доступ при последующем поступлении к ней маркера.

Чаще всего методы с использованием маркера применяются в сетях с *кольцевой топологией* (например, Token Ring и FDDI), однако ничто не мешает передавать маркер и в сетях с другими видами топологий (например, ArcNet – маркерная шина).

5.3 Метод доступа к среде CSMA/CD

Carrier Sense Multiple Access with Collision Detection — множественный доступ с контролем несущей и обнаружением коллизий.

Несущая (*Carrier*) – это информационный сигнал, транслируемый любым сетевым устройством во время передачи данных. Если узел, готовящийся начать передачу, опознает несущую (*Carrier-Sense, CS*), то он откладывает передачу своего кадра данных до окончания чужой передачи.

Компьютеры постоянно конкурируют за право передачи. Для этого все сетевые адаптеры, независимо от того, собираются они передавать информацию или нет, «прослушивают» среду передачи, стремясь обнаружить передаваемые данные.

Это позволяет решить следующие задачи:

– любой компьютер сети находится в постоянной готовности принять информацию, адресованную ему;

– производится поиск момента, когда среда передачи освобождается, ведется только отправителем.

Все данные, передаваемые по сети, помещаются в кадры определенной структуры и снабжаются уникальным адресом станции назначения. Затем кадр передается по кабелю. Все станции, подключенные к кабелю, могут распознать факт передачи кадра, и та станция, которая узнает собственный адрес в заголовках кадра, записывает его содержимое в свой внутренний буфер, обрабатывает полученные данные и посылает по кабелю кадр-ответ. Адрес станции-источника также включен в исходный кадр, поэтому станция-получатель знает, кому нужно послать ответ. Между двумя последовательно передаваемыми по общей шине кадрами информации должна выдерживаться пауза в 9,6 мкс. Эта пауза нужна для приведения в исходное состояние сетевых адаптеров узлов, а также для предотвращения монопольного захвата среды передачи данных одной станцией.

Основная ошибка в конкурентных методах доступа к среде – это *коллизия* (*collision, столкновение кадров*). Она возникает в случае одновременной попытки передачи информационных кадров от двух и более компьютеров одновременно, что обусловлено особенностями распространения сигнала в сетях передачи данных, построенных по шинной топологии. В этом случае передаваемые данные взаимно разрушаются.

Вероятность возникновения коллизии тем выше, чем дальше находятся друг от друга участники соединения и чем большее число компьютеров подключено к сегменту сети. Вероятность возникновения повторной коллизии выше, чем у первичной коллизии.

Обнаружение коллизии может осуществляться по увеличению амплитуды при взаимном наложении сигнала (рисунок 5.4). Направление движения пакетов на рисунке показано стрелочками.

Чтобы корректно обработать коллизию, все станции одновременно наблюдают за возникающими на кабеле сигналами. Если передаваемые и наблюдаемые сигналы отличаются, то фиксируется обнаружение коллизии (*Collision Detection, CD*). Для увеличения вероятности немедленного обнаружения коллизии всеми станциями сети, ситуация коллизии усиливается посылкой в сеть станциями, начавшими передачу своих кадров, специальной последовательности битов, называемой jam-последовательностью.

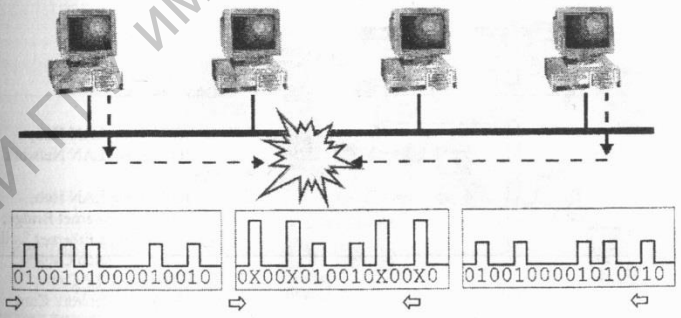


Рисунок 5.4 – Возникновение коллизии в сети с общей шиной

После обнаружения коллизии передающая станция обязана прекратить передачу и ожидать в течение случайного интервала времени, а затем может снова сделать попытку передачи кадра. Узел делает максимально 16 попыток передачи этого кадра информации, после чего отказывается от его передачи. Величина задержки выбирается как равномерно распределенное случайное число из интервала, длина которого экспоненциально увеличивается с каждой попыткой – такой выбор величины задержки снижает вероятность коллизий и уменьшает интенсивность выдачи кадров в сеть.

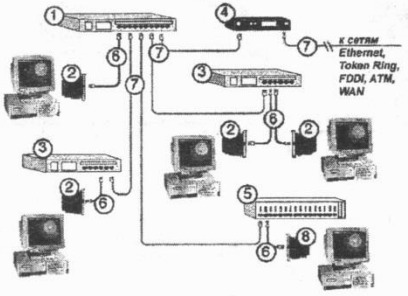
Метод доступа CSMA/CD применяется в стандарте сетевой технологии Ethernet, что определяет его широкую популярность.

5.4 Доступ к среде с использованием приоритетов

Метод доступа с использованием приоритетов – Demand Priority – разрабатывался как способ повышения пропускной способности сети по сравнению с методом доступа CSMA/CD. Применялся в сетях Fast Ethernet – 100 Anylan Voice Guide с использованием UTP Cat 3 или оптоволокна.

При использовании UTP Cat 3 все четыре пары кабеля используются для передачи данных. Каждая пара поддерживает скорость передачи 30 Мбит/с. Используется схема кодирования 5B/6B. Содержимое MAC-кадра сегментируется на квинтеты и сопровождается битом четности. После кодирования передача идет по 4 каналам в круговом порядке.

Совместимость 100 Anylan VG с сетями Ethernet и Token Ring осуществляется на уровне форматов данных. Пример такой смешанной сети показан на рисунке 5.5.



Обозначения:

1 – 100VG AnyLAN Hub;
2 – 100VG AnyLAN Network Card;
3 – 100VG AnyLAN Hub;
4 – 100VG to Ethernet Bridge;
5 – 10/100 Mbps Ethernet Switch;
6 – UTP Cat5 Patch Cables;
7 – UTP Cat5 UTP Cable;
8 – 10 Base-T Network Card.

Рисунок 5.5 – Процедура переопределения приоритетов

Передачи не являются широковещательными на все другие компьютеры сети. Компьютеры не борются самостоятельно за доступ к среде, но работают под централизованным управлением. Для этого необходима сеть с организацией кабельной системы по топологии «звезда». Центральным узлом сетевой архитектуры может быть компьютер, мост, маршрутизатор или коммутатор.

Каждому компьютеру – участнику сетевого соединения присваивается характеристика, называемая приоритетом передачи данных. Эти приоритеты бывают статические и динамические. В одних сетях предполагалось, что они будут назначаться администратором, а в других – сетевыми менеджерами.

Как и в CSMA/CD в Demand Priority компьютеры тоже прослушивают несущую, и когда она освобождается – начинают передачу. При использовании сложных устройств в качестве центрального элемента связь осуществляется только между компьютером-отправителем, центральным элементом и компьютером-получателем, а для всех остальных узлов сети несущая остается свободной. Поэтому, чтобы узлы не пытались передавать свои данные в этот момент, предполагается возможность центрального элемента сообщать о своей занятости. Например, «псевдозаполнением» несущей.

В случае, если два компьютера одновременно отправляют свои данные, центральный элемент сравнивает приоритеты и осуществляет передачу лишь тех данных, которые имеют более высокий приоритет. Данные второго компьютера отбрасываются (рисунок 5.6) [2]. При равном приоритете передаваемых данных сохраняемый блок данных выбирается случайным образом.

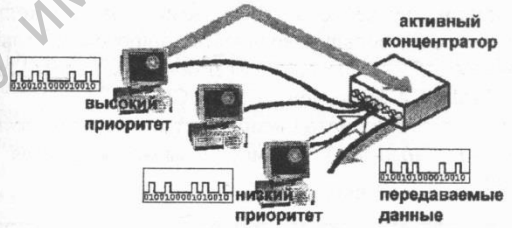


Рисунок 5.6 – Предотвращение коллизии в сетях Demand Priority

Статическое распределение приоритетов может заключаться в закреплении приоритета за номером порта центрального элемента с последовательным уменьшением или увеличением.

При динамическом назначении приоритетов центральный элемент автоматически управляет доступом к сети, делая циклические опросы всех узлов сети, проверяя их работоспособность и переопределяя приоритеты. При этом, если компьютер долгое время не участвует в сетевом обмене, его приоритет можно повысить.

В спецификации IEEE 802.12 для сети 100 Anylan VG предписывается, что выбор приоритетов построен на принципе голосования.

Технические решения, разработанные в рамках этой технологии можно найти в современных сетевых стандартах.

5.5 Метод доступа к среде CSMA/CA

Метод доступа *Carrier Sense Multiple Access with Collision Avoidance* – множественный доступ с контролем несущей и предотвращением коллизий практически аналогичен CSMA/CD. В нем компьютеры также конкурируют за право передачи, и для этого постоянно ведется контроль несущей. Отличие заключается в том, что для разрешения передачи информации отправитель запрашивает подтверждение от всех компьютеров в сети, для этого он формирует и передает в сеть сигнал запроса на передачу – RTS (*Request to Send*). Получив пакет RTS, компьютер, который не собирается сам передавать информацию, сразу отправляет разрешение.

Если компьютер сам собирается передавать информацию и уже отправил свой RTS, то он сравнивает временные отметки своего RTS и полученного, после чего решает: высылать разрешение или поставить пришедший RTS в очередь.

В таком случае вероятность возникновения коллизии минимальна, но в сети большое количество широковещательных сообщений (рисунок 5.7). Поэтому эффективность использования канала связи у CSMA/CA ниже, чем у CSMA/CD.

Чаще всего этот метод используется в *иерархических топологиях* (*«звезда», «дерево»*), примером является сетевая архитектура AppleTalk.

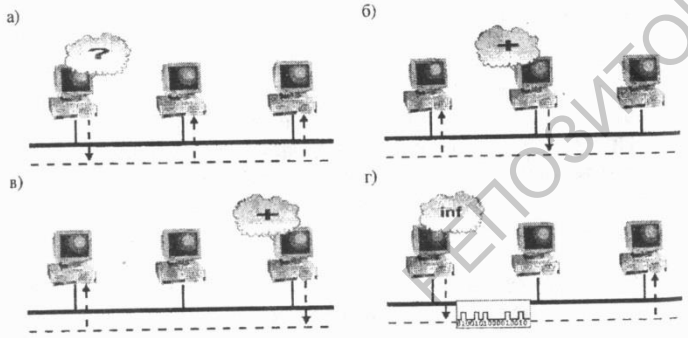


Рисунок 5.7 – Процесс сетевого обмена в сетях CSMA/CA:
а) запрос на право доступа к среде; б) и в) подтверждение на доступ к среде от всех участников сетевого обмена; г) передача данных.

Обновленная версия CSMA/CA, которая также называется функцией распределенной координации (*distributed coordination function*), применяется в беспроводных сетях.

В этом случае станция, ожидающая возможности передачи, прослушивает частоту коммуникаций и определяет ее занятость, проверяя уровень индикатора мощности сигнала в приемнике (Receiver Signal Strength Indicator, RSSI). В тот момент, когда передающая частота свободна, наиболее вероятно возникновение конфликтов между двумя станциями, которые одновременно захотят начать передачу. Когда передающая частота освобождается, каждая станция ждет несколько секунд (их число определяется параметром DIFS), чтобы убедиться в том, что частота остается незанятой.

DIFS – это аббревиатура от термина *Distributed coordination function's Intra Frame Space* – интервал между фреймами функции распределенной координации, который определяет заранее установленное время обязательного ожидания (задержки).

Если станции ожидают в течение времени, определенного интервалом DIFS, вероятность возникновения конфликта между станциями уменьшается, поскольку для каждой станции, требующей передачи, вычисляется разное значение времени задержки (отсрочки), по истечении которого станция снова будет проверять занятость передающей частоты.

Если на момент истечения интервала DIFS:

– частота остается незанятой, то передачу начинает станция, имеющая минимальное время отсрочки;

– частота оказывается занятой, то станция, требующая передачи, ждет, пока частота не освободится, после чего простаивает еще в течение индивидуального времени отсрочки.

При определении времени отсрочки длительность заранее заданного интервала времени умножается на случайное число. Временной интервал – это некоторое значение, хранящееся в базе управляющей информации, имеющейся на каждой станции. Значение случайного числа лежит в диапазоне от нуля до величины максимального размера окна конфликтов. Размер окна конфликтов также хранится в базе управляющей информации станции. Таким образом, для каждой станции, ожидающей передачи, определяется уникальное время отсрочки, что позволяет станциям избегать конфликтов.

Вопросы для самоконтроля

1 Как организуется очередность приема и передачи информации в сетевой среде?

2 На каком уровне модели OSI действуют методы доступа к среде?

3 Какие методы доступа к среде чаще всего применяются в компьютерных сетях?

4 Как можно ограничить доступ к среде передачи на физическом уровне модели OSI?

5 Каковы свойства сети, построенной с использованием маркерного доступа к сети?

6 Каковы свойства сети, построенной с использованием метода доступа к сети CSMA/CD?

7 Каковы свойства сети, построенной с использованием метода доступа к сети CSMA/CA?

8 Каковы свойства сети, построенной с использованием метода доступа к сети по приоритету запроса?

9 Какие ошибки передачи данных обусловлены выбором метода доступа к среде?

10 Что такое коллизия?

11 Что происходит в сети после возникновения коллизии?

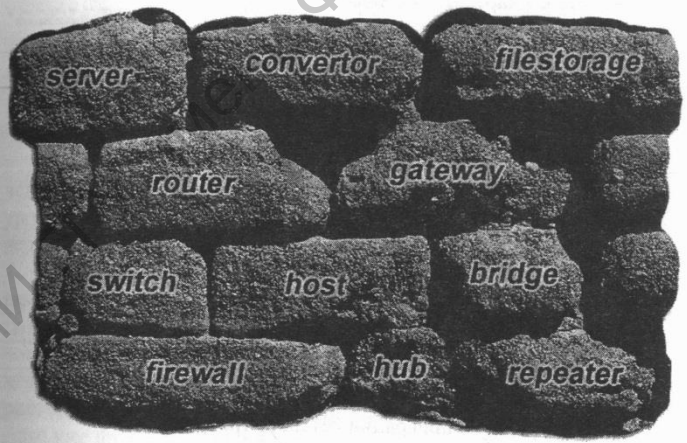
12 Какие методы борьбы с коллизиями применяют в современных сетях?

13 Какие способы повышения надежности передачи данных с использованием методов доступа к среде вы знаете?

14 Как объединяются сети с различным методом доступа к среде?

15 Каковы перспективы развития методов доступа к среде передачи данных?

6 Активное оборудование сетей



6.1 Виды активного оборудования сетей

К активному оборудованию сетей относятся все виды оборудования, используемые для поддержки формы сигнала, ретрансляции, выбора или изменения маршрута продвижения пакета, преобразования формата передаваемых данных, а также специализированное оборудование объединения и обслуживания сетей.

Разные авторы к активному оборудованию сетей относят различный набор устройств. Вот приблизительный их перечень:

- трансивер (*TRANSIEVER*);
- сетевая карта (*NETCARD*);
- модем (*MODEM*);
- повторитель (*REPEATER*);
- конвертор (*CONVERTOR*);
- концентратор (*HUB, MAU*);
- коммутатор (*SWITCH*);
- мост (*BRIDGE*);
- маршрутизатор *(ROUTER);*
- канал *(CHANNEL);*
- шлюз (*GATEWAY, BRANDMAUER*);
- дополнительные сетевые устройства:
  а) принт-сервер;
  б) сетевое хранилище;
  в) антивирусный сетевой экран;
  г) антиспамовый сетевой экран;
  д) устройство шифрации сетевого трафика;
  е) точка доступа;
- комбинированные и гибридные виды устройств:
  а) коммутатор-маршрутизатор;
  б) мост-маршрутизатор.

Лучшим способом для понимания отличий между сетевыми адаптерами, повторителями, мостами, коммутаторами, маршрутизаторами и другими активными сетевыми устройствами является рассмотрение их работы относительно модели OSI. Соотношение между собой функций этих устройств достаточно хорошо видно на рисунке 6.1.

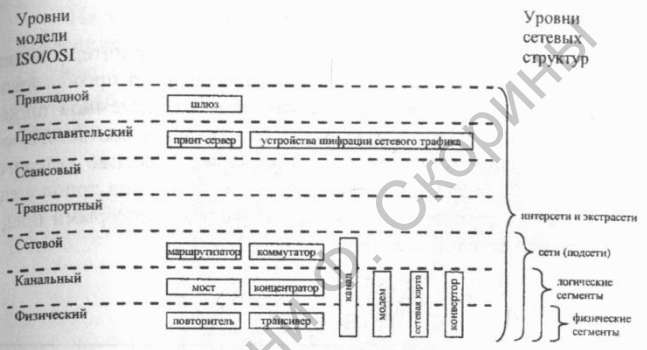


Рисунок 6.1 – Соответствие функций коммуникационного оборудования уровням модели OSI

Например, повторитель, который регенерирует сигналы, за счет чего позволяет увеличивать длину сети, работает на физическом уровне. А самое сложное устройство – шлюз работает на самом верхнем прикладном уровне.

Функции большинства других устройств могут не умещаться в рамках одного уровня модели OSI. Например, сетевой адаптер работает на физическом и канальном уровнях. К физическому уровню относится та часть функций сетевого адаптера, которая связана с приемом и передачей сигналов по линии связи, а получение доступа к разделяемой среде передачи, распознавание MAC-адреса компьютера – это уже функция канального уровня.

Многие из упомянутых сложных, комбинированных и гибридных сетевых устройств не отражены на данной схеме по причине их многочисленности и продолжающегося роста их разнообразия.

Следует знать, что чем ниже устройство находится по уровню модели OSI, тем больше его производительность или ошибки в работе сильнее сказываются на производительности сети.

Самая экономная по количеству элементов активного сетевого оборудования локальная сеть – соединение точка-точка. Применяются лишь сетевые адаптеры и непосредственно соединительный кабель (оптоволокно, витая пара или коаксиальный кабель), либо беспроводное соединение.

6.2 Применение сетевых адаптеров

Сетевой адаптер или сетевая карта (*netcard*) – это интерфейсная карта ввода-вывода информации, которая обеспечивает преобразование информационных сигналов, поступающих от системной шины компьютера в форму, пригодную для ретрансляции в соответствующей среде передачи (рисунок 6.2). Внутреннее строение сетевого адаптера и его физические интерфейсы зависят от типа топологии, среды передачи и сетевого стандарта, для работы с которыми предназначен данный сетевой адаптер.

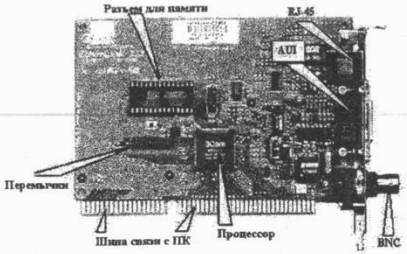


Рисунок 6.2 – Функциональные блоки сетевого адаптера Ethernet

Современные мини – и суперминикомпьютеры, а также большие ЭВМ (Mainframes), все еще могут иметь встроенные адаптеры с AUI-разъемами. Ряд современных системных плат персональных компьютеров тяготеет ко встроенным адаптерам с разъемом RJ-45.

Сетевые адаптеры или сетевые интерфейсные карты (Network Interface Card, NIC) для PC, выпускаемые многими производителями в широком ассортименте, различаются поддерживаемыми средами передачи, типом системной шины (ISA, EISA, MCA, PCI, реже VLB), архитектурой и производительностью. Для ноутбуков существуют адаптеры Ethernet в стандарте PCMCIA (PC CARD). Выпускаются также адаптеры, подключаемые к стандартному LPT-порту (Paraport) или к USB. Примеры показаны на рисунке 6.3.

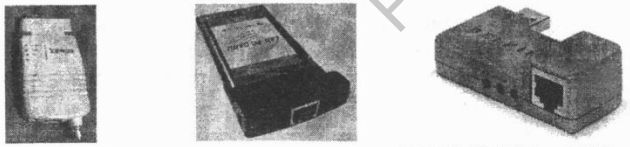


Рисунок 6.3 – Сетевые адаптеры для портов LPT, PCMCIA и USB

На текущий момент широко распространены сетевые карты с интерфейсом 100Base-TX на шину PCI (рисунок 6.4, *а*). Применяются также сетевые карты с оптическим интерфейсом (рисунок 6.4, *б*). Например, 100Base-FX – с основным оптическим разъемом SC на многомодовое волокно.

а) *б*)

Рисунок 6.4 – Внешний вид сетевого адаптера:
а) сетевой адаптер 100Base-TX; *б*) сетевые адаптеры 100Base-FX

Настройка сетевого адаптера заключается в первую очередь в настройке операционной системы, которая может быть успешно осуществлена только при условии отсутствия конфликтов по оборудованию между сетевым адаптером и любым другим устройством системы.

Конфликт может быть по прерыванию, по диапазону адресов ввода-вывода, а в некоторых случаях по каналу DMA. Учитывая все это, производители перевели все современные модели сетевых адаптеров в режим PnP.

Этапы настройки сетевого адаптера можно изложить в следующей последовательности.

1 Физически установить устройство в соответствующий порт.

2 Назначить прерывания и адреса ввода-вывода, если нет режима PNP.

3 Протестировать систему на возможные конфликты по параметрам с уже установленным оборудованием.

4 Установить драйвера для сетевого устройства в состав операционной системы.

5 Установить программы, обслуживающие сетевой обмен.

6 Проверить работоспособность системы.

Важными функциями современных сетевых карт являются автоконфигурирование скорости сетевого обмена 10/100/1000 Мбит/с и возможности поддержки дуплексного режима передачи.

6.3 Применение модемов

Модем (модулятор-демодулятор) служит для передачи информации на большие расстояния, недоступные локальным сетям. Передача осуществляется через выделенные или коммутируемые телефонные линии.

Ранние модели модемов передавали данные асинхронно, работая на скоростях до 18000 бит/с с FSK-модуляцией (frequency shift keying – манипуляция сдвигом частоты), используя две частоты для передачи и две для приёма. Асинхронная передача не сопровождается сигналами таймера, и модемы ориентируются на номинальную скорость передачи. Для предотвращения потерь данных они группируются в очень короткие блоки (символы) с ограничительными битами (биты start и stop). Наиболее распространённая система для этого – ASCII–кодировка с контролем по чётности. Синхронные модемы требуют две выделенные пары проводов для синхронизации данных и установки в слот системной шины специального контроллера.

Синхронные модемы работают на скоростях до 56 Кбит/с на аналоговых линиях. Данные при синхронной передаче сопровождаются сигналами таймера и почти всегда сгруппированы в блоки. Передающее устройство собирает данные в блоки и сопровождает их дополнительными кодами, необходимыми для обнаружения и/или коррекции ошибок в соответствии с одним из протоколов (BISYNC, SDLC, HDLC и т. д.). Программа-источник и программа-получатель данных полагают, что модем прозрачен для этих типов данных, соответственно модем может игнорировать группирование данных. Обычными методами модуляции являются фазовая модуляция и интегрированная фаза с амплитудой.

Тип модема также зависит от числа функций, реализованных в нем либо только аппаратно, либо совместно с программным способом (*софт-модемы*).

Факс-модемы позволяют передавать и принимать факсимильные изображения, совместимые с обычными факс-машинами.

Голосовые модемы (Voice Modem) преобразуют звуковое сообщение в файл данных, аудиосигнал сжимается по методу ADPCM (Adaptive Differential Pulse Code Modulation). Сообщение может передаваться по электронной почте или в режиме реального времени. Звук воспроизводится через внутренний динамик самого модема или через мультимедийные средства компьютера.

DSL-модемы (Digital Subscriber Line – цифровая линия подписки) разработаны телефонными компаниями для предоставления услуг кабельного телевидения. Популярность завоевал асимметричный подвид стандарта – ADSL.

ADSL-модем передаёт данные одновременно с голосом, используя обычную пару медных телефонных проводов. Для этого создаются три раздельных частотных канала. Первый набор частот передаёт обычный телефонный сигнал. Второй канал передаёт (upstream) данные на скорости от 64 Кбит/с до 640 Кбит/с в зависимости от качества линии, расстояния и диаметра провода. Третий канал – высокоскоростной принимающий (downstream) канал, работающий на скоростях от 1,5 Мбит/с до 6,3 Мбит/с. Каждый канал работает только в одном направлении. Схема работы с ADSL-модемом приведена на рисунке 6.5.

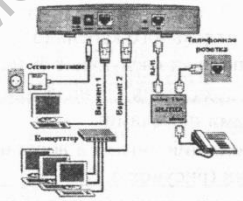


Рисунок 6.5 – Применение оборудования ADSL

Скоростные параметры модемов имеют следующие характеристики:

- *cps* – скорость передачи символов, байт/с;
- *bps* – скорость передачи, бит/с;
- *baud* – количество изменений сигнала в линии за 1 секунду.

Для повышения эффективной скорости работы при ограниченной полосе линии применяют различные методы кодирования и модуляции, при которых *bps* превышает *baud*.

Конструктивно модемы выпускаются в двух вариантах исполнения: внутренние – Internal и внешние – External (рисунок 6.6).

а) *б)*

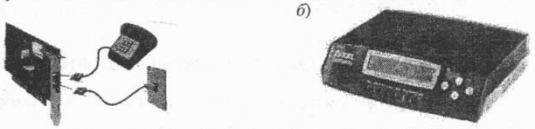


Рисунок 6.6 – Внешний вид Internal (*а*) и External (*б*) модемов

6.4 Применение репитеров

Повторитель (репитер, repeater) соединяет два или несколько кабельных сегментов и ретранслирует любой входящий сигнал на все другие сегменты.

Сегмент кабеля – это один отрезок кабеля, удовлетворяющий спецификациям IEEE (например, отрезок кабеля 10Base2 длиной 185 м, к которому подключено не более 30 узлов, включая терминаторы и сетевое оборудование).

Повторитель – это устройство физического уровня, чаще всего упоминаемое при описании топологии «шина», но и другие топологии применяют схожие устройства. При этом стоит сказать, что для каждой кабельной системы разрабатывается свой тип повторителя.

Повторители позволяют соединять пользователей, находящихся в удаленных концах здания на расстояниях, не отвечающих требованиям IEEE, на длину отдельного кабельного сегмента.

Повторитель выполняет следующие функции физического уровня:

– фильтровать искажения сигнала или шум, вызванный радио или электромагнитными помехами;

– усиливать входящий сигнал и восстанавливать его форму для более точной передачи (рисунок 6.7);

– синхронизировать сигнал (в сетях Ethernet);

– воспроизводить сигнал на всех кабельных сегментах.

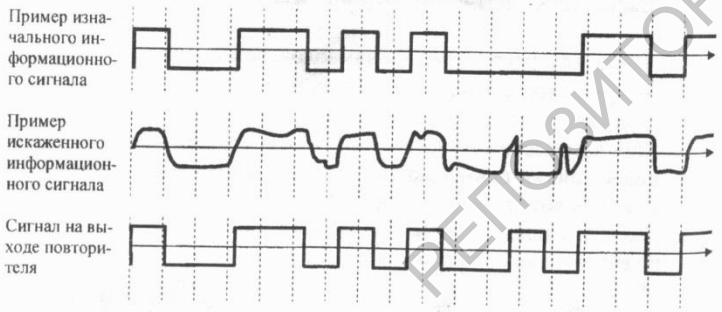


Рисунок 6.7 – Обработка сигналов повторителем

Синхронизация сигнала, например, позволяет избежать коллизий в сети Ethernet, когда сигнал передается в кабель.

Таким образом, повторители могут решить следующие вопросы:

– удлинить кабельную систему (например, на расстояние более 185 м для сегмента 10Base2 и свыше 500 м – для 10Base5);

– увеличить количество подключенных узлов и обойти ограничения, налагаемые на отдельный сегмент (например, подключить свыше 30 узлов в сети Ethernet);

– распознать сетевую ошибку и отключить сегмент кабеля;

– подключиться к компонентам в других сетевых устройствах, таких как концентраторы и коммутаторы, а также усилить и синхронизировать сигналы;

– соединить сегменты, работающие с разной кабельной системой;

– удлинить сегменты магистрального кабеля в локальных и глобальных сетях;

– удлинить сегменты оптоволоконного кабеля;

– увеличить рабочее расстояние для каналов связи.

Если повторитель ретранслирует сигнал в два и более кабельных сегмента, он называется многопортовым повторителем. Например, повторитель может иметь порты для 2–8 дополнительных сегментов. Такой повторитель сети 10Base2 (рисунок 6.8) может передавать сигнал в несколько кабельных сегментов длиной 185 м. Каждый кабель может иметь до 29 подключенных узлов, включая терминаторы на обоих концах.

В случае ошибки повторитель перестает передавать данные в неисправный сегмент. Такой способ отключения сегмента называется изолированием или секционированием (partitioning).

Применение многопортового повторителя меняет шинную топологию сети на топологию «звезда-шина».

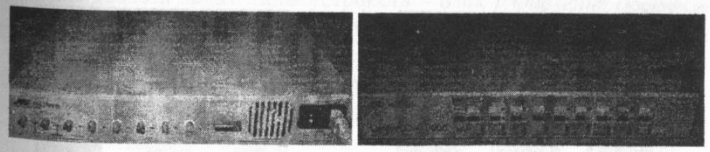


Рисунок 6.8 – Восьмипортовый Ethernet Repeater 10base2

По своей сути многопортовый повторитель практически уже мало чем отличается от устройств, называемых концентраторами.

6.5 Применение концентраторов

Концентратор *(HUB, MAU)* – это активный многопортовый повторитель с функцией автосегментации.

Автосегментация (аналог partitioning) необходима для повышения надежности сети. Обработка ошибок и текущий контроль состояния каналов связи осуществляется самим концентратором.

Концентраторы можно *каскадировать*, т. е. соединять друг с другом, увеличивая тем самым размер сети и создавая сложные топологии. Недостатком такой технологии является то, что трафик получаемой системы будет общим, т. е. увеличивается вероятность возникновения ошибок. Ограничение на число подключенных узлов может распространяться на всю объединенную систему.

Все порты концентратора равноправны. Получив сигнал от одной из подключенных к нему станций, концентратор транслирует его на все свои активные порты. При этом, если на каком-либо из портов обнаружена неисправность, то этот порт автоматически отключается (сегментируется), а после ее устранения снова делается активным.

Концентраторы могут быть активными и пассивными, то есть без функции восстановления формы сигнала.

Простейшие концентраторы представляют собой единую точку подключения к сети, позволяющую физически реализовать в виде звезды логическую шинную сеть Ethernet или маркерное кольцо. Такие концентраторы также называются неуправляемыми и предназначены они для очень маленьких сетей, содержащих до 12 узлов.

Концентраторы применяются в сетевых топологиях «звезда», «звезда-шина», «звезда-кольцо». В зависимости от конкретной топологии внутренняя логическая начинка, а значит, и механизм работы устройства будут разными (рисунок 6.9).

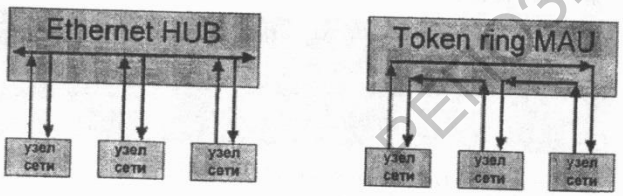


Рисунок 6.9 – Примеры внутренней структуры концентраторов

Концентраторы топологии «звезда-шина», применяемые в Ethernet (*HUB*), работают по принципу «один ко многим», то есть:

– являются центральным устройством, через которое соединяется множество узлов сети;

– позволяют большое количество компьютеров соединять в одну или несколько локальных сетей;

– соединяют вместе сегменты сетевой магистрали;

– обеспечивают соединение между различными типами передающей среды;

– позволяют централизовать сетевое управление и структуру.

Модель, применяемая в топологии «звезда-кольцо» имеет внутреннюю логическую организацию – кольцо, которую можно сравнить с эстафетой. Т. е. информация передвигается последовательно от одного порта к другому по кольцу. Принцип используется в сети Token Ring, концентратор называется *модуль множественного доступа* (*multistation access unit, MAU*), также встречается термин *интеллектуальный модуль множественного доступа* (*smart multistation access unit, SMAU*). Последний применяется, если модуль обладает возможностью находить неисправности в соединениях с рабочими станциями и изолировать неисправные станции от сети.

Модуль MAU также может выполнять функции *пассивного* или *активного* концентратора. Активный концентратор работает как повторитель, что более чем в два раза увеличивает количество поддерживаемых узлов.

В иерархических схемах допускается применение сложных и гибридных устройств (на уровнях объединения сегмента), что расширяет число функций сети.

Например, усовершенствование технологии модулей MAU позволило создать новые типы устройств – *блок управления доступом* (*Controlled Access Unit, CAU*), который позволяет несколько соединенных между собой наращиваемых блоков рассматривать как единый модуль MAU сети с маркерным кольцом. Блоки CAU также имеют возможность сбора информации, необходимой для управления производительностью сети.

Большинство концентраторов были выпущены для сетей со скоростью обмена 10 Мбит/с (HUB Ethernet), либо 20 Мбит/с (MAU TokenRing). Сейчас концентраторы практически полностью исчезли с рынка.

6.6 Применение коммутаторов

Ключевой проблемой проектирования и эксплуатации локальных сетей является распределение пропускной способности кабеля между всеми станциями, подключенными к сети. Например, в сети 10BASE-T при подключении 100 рабочих станций каждая из них получает возможность передавать данные в среднем со скоростью:

$$\frac{10 Мбит/с}{100} = 0{,}1 Мбит/с.$$

Иначе говоря, пропускная способность канала для одной станции в такой сети составляет 100 Кбит/с. С развитием мультимедийных приложений, позволяющих передавать звук, видео и статические изображения высокого качества, значительно возросли требования к параметрам локальных сетей.

Коммутатор позволяет уплотнить передачу (рисунок 6.10).

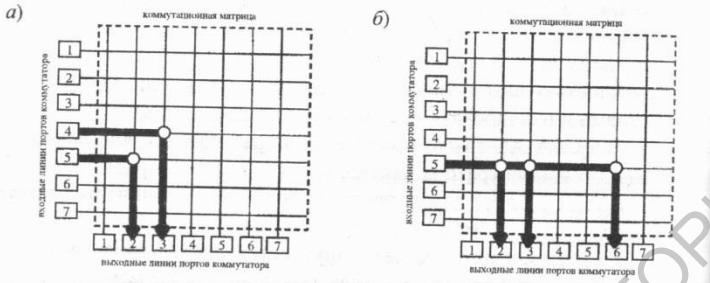


Рисунок 6.10 – Логическая структура коммутатора:
а) одновременная передача по двум каналам;
б) широковещательная рассылка

Обратите внимание, что подключение двух файловых серверов (Data) к отдельным портам коммутатора позволяет одновременно устанавливать два канала связи между рабочими станциями и файловыми серверами, что увеличивает максимальную скорость доступа к данным в сети вдвое.

Другими словами, в коммутаторе выполняется функция трансляции сигнала конкретному порту назначения (виртуальный канал или коммутируемая линия), а при наличии более одной коммутируемой линии – организации несколько одновременных сеансов обмена.

Ключевым звеном коммутатора является архитектура защиты магистрали от блокирования (*non-blocking*), которая позволяет установить множественные связи между разными парами портов одновременно, причем кадры не теряются в процессе коммутации. При этом параллельный трафик между взаимодействующими сетевыми устройствами остается локализованным. Локализация осуществляется с помощью адресных таблиц, устанавливающих связь каждого порта с адресами сетевых устройств, относящихся к сегменту этого порта. Таблица заполняется в процессе анализа коммутатором адресов станций отправителей в передаваемых ими кадрах.

Кадр передается через коммутатор локально в соответствующий порт только тогда, когда адрес станции назначения, указанный в поле кадра, уже содержится в адресной таблице этого порта. В случае отсутствия в таблице адреса станции назначения, кадр рассылается во все остальные сегменты. Если коммутатор обнаруживает, что MAC-адрес станции назначения приходящего кадра находится в таблице MAC-адресов, приписанной за портом, то этот кадр сбрасывается – его получит станция назначения, находящаяся в исходном сегменте.

Если приходящий кадр является широковещательным (*broadcast*), то есть если все биты поля MAC-адреса получателя в кадре задаются равными единице, то такой кадр будет размножен коммутатором (подобно концентратору), т. е. направлен во все остальные порты.

Внешний вид коммутаторов представлен на рисунке 6.11.

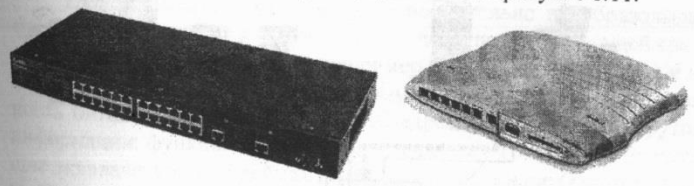


Рисунок 6.11 – Примеры коммутаторов

Максимальное количество коммутируемых линий в коммутаторе можно рассчитать по формуле: $m = div\ (n/2)$, где m – число коммутируемых линий, а n – число портов коммутатора.

Именно технология коммутации позволила увеличить скорость передачи данных в сетях до стабильного значения в 10 Гбит/с.

6.7 Применение мостов

Мост (bridge) – это сетевое устройство, соединяющее между собой сегменты локальной сети или целые сети (рисунок 6.12).

Мосты являются устройствами канального уровня и позволяют решать следующие задачи:

– расширить локальную сеть в случае, когда достигнут лимит на максимальное количество соединений (например, если сегмент Ethernet имеет 30 узлов);

– объединить две однородные сети через промежуточный канал другого типа связи (например, модемный мост между сегментами сети);

– расширить локальную сеть и обойти ограничения на длину сегментов (например, если нужно нарастить сегмент Ethernet на тонком кабеле, который уже имеет длину 185 м);

– сегментировать локальную сеть для ликвидации узких мест в сетевом трафике;

– объединять две сети разных сетевых архитектур (например, сеть с топологией «кольцо» можно объединить с сетью с топологией «шина»);

– предотвратить неавторизованный доступ к сети.

Часто мосты применяют для объединения более двух сетей одновременно.

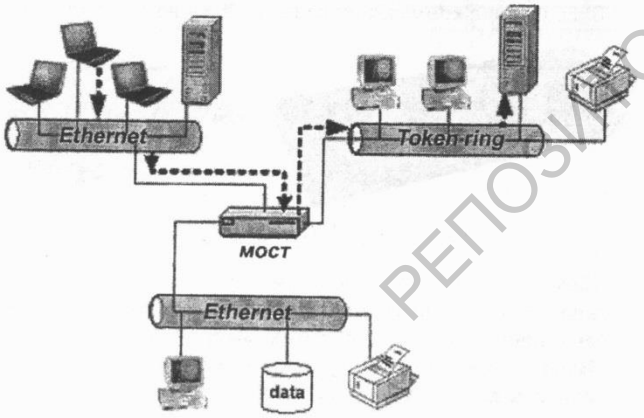


Рисунок 6.12 – Объединение сетей с помощью моста

Мосты функционируют в так называемом беспорядочном режиме (*promiscuous mode*), что подразумевает просмотр физического целевого адреса каждого фрейма перед его пересылкой. Этим мосты отличаются от повторителей и концентраторов.

Чаще всего используются два типа мостов.

Прозрачные мосты – считывают исходный и целевой физические адреса фрейма. Для этого они перехватывают весь сетевой трафик и анализируют целевой адрес каждого фрейма, определяя, следует ли пересылать данный фрейм в следующую сеть. Для этого мост просматривает MAC-адреса передаваемых через него фреймов и строит *таблицу целевых адресов*.

Если мост знает, что фрейм предназначен для узла, который находится в том же сегменте, что и отправитель фрейма, он отбрасывает сегмент, поскольку тот не нуждается в дальнейшей пересылке. Если мост знает, что целевой адрес располагается в другом сегменте, он транслирует фрейм только в нужный сегмент. Если мосту не известен целевой сегмент, он передает фрейм во все сегменты, за исключением исходного сегмента, и этот процесс называется *лавинной маршрутизацией* (*лавинной адресацией*) (*flooding*). Главным достоинством мостов является то, что они сосредотачивают трафик в конкретных сетевых сегментах. Мост может выполнять фильтрацию и пересылку с довольно высокой скоростью, поскольку он просматривает информацию только на канальном уровне и игнорирует информацию на более высоких уровнях.

Транслирующие мосты могут дополнительно преобразовывать фреймы, относящиеся к одному методу доступа и передающей среде, во фреймы другого стандарта (например, Ethernet – Token Ring) и наоборот. Такой мост должен уметь изменять или добавлять: очередность битов в адресах; формат MAC-адреса; элементы маршрутной информации; функции, имеющиеся во фреймах Token Ring, не имеющие эквивалентов во фреймах Ethernet; зондирующие (*explorer*) пакеты Token Ring, которых нет в сетях Ethernet.

К достоинству мостов относится то, что они могут использоваться еще и как низкоуровневые брандмауэры (сетевые экраны).

Важно знать что, если в сети присутствует более одного моста, может возникнуть ситуация, когда они не смогут правильно опознать, какой компьютер к какой из сетей относится, т. к. механизм регистрации узлов сети в таблице маршрутизации не лишен некоторых недостатков.

6.8 Применение маршрутизаторов

Маршрутизатор (*router*) – это устройство, предназначенное для определения и назначения наиболее оптимального маршрута продвижения пакетов при их перемещении по сети с несколькими вариантами маршрутов доставки.

Маршрутизатор выполняет некоторые функции моста, такие как анализ топологии, фильтрация и пересылка пакетов. Однако, в отличие от мостов, маршрутизаторы могут направлять пакеты в конкретные сети, анализировать сетевой трафик и быстро адаптироваться к изменениям сети.

Маршрутизаторы относятся к сетевому уровню модели OSI, что позволяет им анализировать в пакетах больше информации, чем это возможно для мостов. Его структуру отражает рисунок 6.13.

Маршрутизаторы подразделяются на два основных типа:

– *статические* (*static*) – здесь необходимо, чтобы администратор вручную создал и сконфигурировал таблицу маршрутизации, а также указал каждый маршрут для передачи данных через сеть;

– *динамические (dynamic)* – автоматически определяют маршруты и поэтому требуют минимальной настройки. Они сложнее статических, так как анализируют информацию от других маршрутизаторов и для каждого пакета принимают отдельное решение о маршруте передачи данных в сети.

Рисунок 6.13 – Функциональная схема блоков маршрутизатора

Процедура создания маршрута состоит в оценке и сравнении между собой нескольких вариантов путей прохождения информации через сеть, вычисленных согласно «метрикам» маршрутизации, значения которых хранятся в таблицах маршрутизации. Таблицы маршрутизации этих устройств намного сложнее, чем таблицы маршрутизации мостов.

Метрика маршрутизации – это свойство каналов связи, согласно которому в числовом эквиваленте определяется оптимальность данного маршрута в текущий момент времени. К примерам таких метрик можно отнести: цену аренды канала связи за единицу времени, скорость пропускания канала связи, длину сегмента, число заявок в единицу времени, длину очереди на обслуживание в текущий момент времени и пр. Часть характеристик может быть статическими, но некоторые могут измениться и потребуют обновления. Обновление осуществляется широковещательными пакетами, что отрицательно сказывается на сетевом трафике.

Положительный момент в применении маршрутизаторов – локализация трафиков, т. е. в соседней части сети будут транслироваться только те пакеты, которые не могут быть обслужены в пределах данного сегмента сети.

Отрицательным моментом является возможность организации «адресной петли». Например, в сети есть 6 узлов маршрутизации (рисунок 6.14). Необходимо доставить пакет от первого к шестому.

Рисунок 6.14 – Пример маршрутизации пакетов в сложных сетях

В этой сети от маршрутизатора 1 к маршрутизатору 6 есть два маршрута продвижения данных: «1–3–5–6» и «1–2–4–5–6».

При оценке маршрутизатором 1 может быть выбран оптимальным маршрутом первый путь – «1–3–5–6». Пакет пересылается маршрутизатору 3, а на самом маршрутизаторе 3 после анализа может сложиться ситуация, когда оптимальным маршрутом доставки пакета маршрутизатору 6 будет выбран маршрут «3–1–2–4–5–6». Таким образом, пакет возвращается на исходный маршрутизатор и может блуждать по кольцу, пока не истечет срок его жизни.

6.9 Применение шлюзов

Шлюз (*gateway*) обеспечивает связь между различными архитектурами и сетевыми средами.

Шлюзы распаковывают и преобразуют данные, передаваемые из одной среды в другую, чтобы каждая среда могла понимать сообщения других сред. В частности, шлюз изменяет формат данных, иначе прикладная программа на принимающей стороне не сможет их распознать. Например, шлюзы электронной почты (такие, как X.400) принимают сообщение в одном формате, транслируют его и пересылают в формате X.400, используемом получателем, и наоборот.

Шлюз связывает две системы, которые применяют разные:

- коммуникационные протоколы;
- структуры и форматы данных;
- языки;
- архитектуры.

Шлюзы – это самые сложные устройства, они включают в себя функции прикладного уровня модели ISO и поэтому являются самыми медленными, зато позволяют реализовать любую обработку и преобразование передаваемой информации.

Например, обеспечение безопасности информации, шифрование данных на входе и выходе, антивирусная профилактика, объединение трафика нескольких пользователей «Proxy».

Шлюзы связывают разные сети, например Microsoft Windows NT Server с SNA (Systems Network Architecture фирмы IBM). Шлюзы создаются для выполнения определенного типа задач, то есть для конкретного типа преобразования данных. Часто их и называют в соответствии со специализацией (например, Windows NT Server To SNA Gateway).

Некоторые шлюзы используют все семь уровней модели OSI, но обычно шлюзы выполняют преобразование протоколов только на прикладном уровне.

Шлюз принимает данные из одной среды, удаляет старый протокольный стек и переупаковывает их в протокольный стек системы назначения. Для этой работы необходимо ведение расширенных таблиц адресации и маршрутизации.

Обычно в качестве шлюза используют выделенный сервер.

Если шлюз используется в качестве коммуникационного центра гетерогенной сети, то он должен выполнять функции переводчика (транслятора протоколов) и/или конвертора (преобразователя сигналов).

Обрабатывая данные, шлюз выполняет следующие операции (рисунок 6.15):

– извлекает данные из приходящих пакетов, пропуская их снизу вверх через полный стек протоколов передающей сети;

– заново упаковывает полученные данные, пропуская их сверху вниз через стек протоколов сети назначения.

Самая актуальная задача, решаемая современными шлюзами – это защита информации, в частности, функция брандмауэра (сетевого экрана, межсетевого фильтра).

Еще одно назначение шлюзов – связывать локальную сеть персональных компьютеров и среду мэйнфреймов или миникомпьютеров, которые непосредственно взаимодействовать с персональными компьютерами в пределах однородной сети не могут.

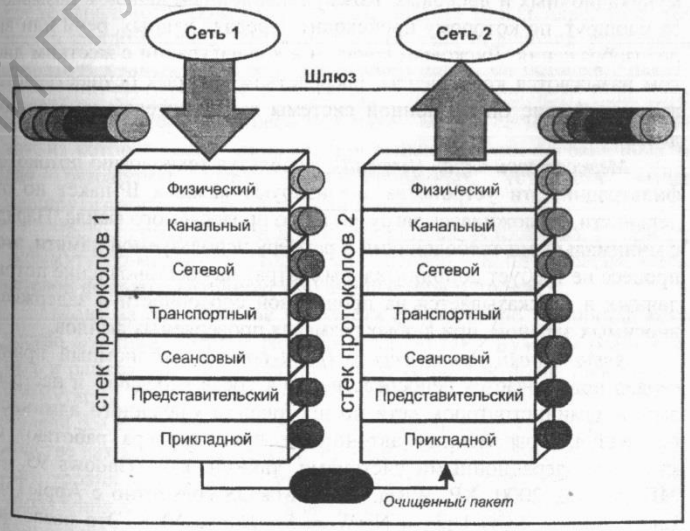


Рисунок 6.15 – Преобразование пакета данных шлюзом

6.10 Другие примеры активного оборудования сетей

Кроме вышеописанных сетевых устройств широко применяются другие специализированные и многофункциональные их разновидности. Число таких устройств непрерывно растет по причине удобства в эксплуатации, простоты настройки, высоких характеристик по скорости и качеству обслуживания запросов пользователей.

Ниже кратко описаны функции некоторых из этих устройств.

Конвертор (convertor, медиа-конвертор). Конвертор – двухпортовое устройство, оба порта которого представляют средозависимые интерфейсы. Конверторы, в отличие от повторителей, могут работать в дуплексном режиме. Распространены конверторы 100Base-TX/100Base-FX. Применение конвертора позволяет подбирать для сети любые образцы активного сетевого оборудования, не учитывая их совместимости со средой передачи.

Канал (channel). Каналом называется физический или логический путь для передачи сигналов. В литературе о компьютерных сетях чаще всего встречаются упоминания о каналах двух типов: коммуникационных и дисковых. Коммуникационным каналом называется маршрут, по которому происходит передача данных, речи или видеоизображения. Дисковым каналом в конфигурации с жестким диском называются компоненты, посредством которых осуществляется взаимодействие операционной системы с накопителем на жестком диске.

Межсетевой экран (firewall). Используя технологию потоковой фильтрации, эти устройства анализируют каждый IP-пакет по отдельности, не дожидаясь загрузки всего проверяемого файла. Наряду с минимальными требованиями к размеру используемой памяти, этот процесс не требует дополнительных затрат на восстановление потока данных и не сказывается на пропускной способности и задержках, вносимых экраном, при любых размерах проверяемых файлов.

Автономный принт-сервер (print-server). Автономный принт-сервер подключается непосредственно к среде передачи и настраивается администратором сети по протоколам удаленного администрирования. Современные автономные принт-сервера работают со многими операционными системами, такими, как Windows 95, 98, ME, NT 4.0, 2000, XP, Wista, Apple MacOS совместно с AppleTalk, Linux, Solaris, SCO Unix и NetWare 5.x Native NDS. Это позволяет гибко настроить принт-сервер под требования сетевой среды.

Сетевое хранилище (file-server). Это компактное устройство позволяет хранить десятки тысяч изображений и документов для совместного использования их в сети, при этом не занимая много места в офисе. Кроме того, оно обеспечивает защиту данных при помощи базы данных пользователей, а совместный доступ к папке осуществляется на основе учетной записи пользователя или группы пользователей.

Современные образцы поддерживают возможность «горячей» замены, поэтому их можно подключать и отключать от сети в любой момент времени. Строго соответствуя стандарту Universal Plug-and-Play, они могут напрямую взаимодействовать с другими сетевыми устройствами, совместимыми с UPnP.

Гибридные устройства. Сетевые администраторы часто сомневаются, что надо использовать при объединении сетей – мост или маршрутизатор. Ведь эти устройства реализуют похожие функции:

– передают пакеты между сетями;

– передают данные по каналам глобальных сетей.

Однако мост, работающий на подуровне управления доступом к среде канального уровня модели OSI, «видит» только адрес узла, точнее, в каждом пакете мост ищет адрес узла подуровня управления доступом к среде. Если мост распознает адрес, он оставляет пакет в локальном сегменте или передает его в нужный сегмент. Если адрес мосту неизвестен, он пересылает пакет во все сегменты, исключая тот, из которого пакет прибыл. Для решения таких пограничных задач разработан класс комбинированных устройств «мост-маршрутизатор» (*bridge-router* или *brouter).*

Часто применяются и другие гибридные устройства. Например, «коммутатор-маршрутизатор», «файл-сервер – принт-сервер», «межсетевой фильтр – антивирусный анализатор» и прочие.

Мода на объединение устройств существенно увеличила количество функций, которое разработчики считают нужным реализовывать в рамках устройств негибридного типа. Так появились понятия коммутации второго, третьего и четвертого уровней относительно модели ISO/OSI. Все эти устройства позиционируются при производстве как коммутаторы. Причем относительно коммутации четвертого уровня до сих пор не утихают споры. Поэтому данный уровень управления коммутацией сейчас называется «в зависимости от типа запроса приложений».

Вопросы для самоконтроля

1 Какие виды активного оборудования сетей вы знаете? Перечислите их.

2 Что относится к дополнительным и комбинированным сетевым устройствам?

3 Проведите соответствие функций коммуникационного оборудования уровням модели OSI.

4 Что скрывается за понятием односегментная шина?

5 Дайте определение сетевого адаптера или сетевой карты (netcard).

6 Какими параметрами обладают современные сетевые адаптеры?

7 Приведите классификацию сетевых адаптеров.

8 Как осуществляется настройка сетевого адаптера?

9 Что такое модем?

10 Что такое синхронный и асинхронный обмен данными ?

11 Дайте классификацию типов современных модемов.

12 Опишите функции и принцип работы сетевого устройства «повторитель» (repeater).

13 Опишите функции и принцип работы сетевого устройства «концентратор» (hub, mau).

14 Опишите функции и принцип работы сетевого устройства «коммутатор» (switch).

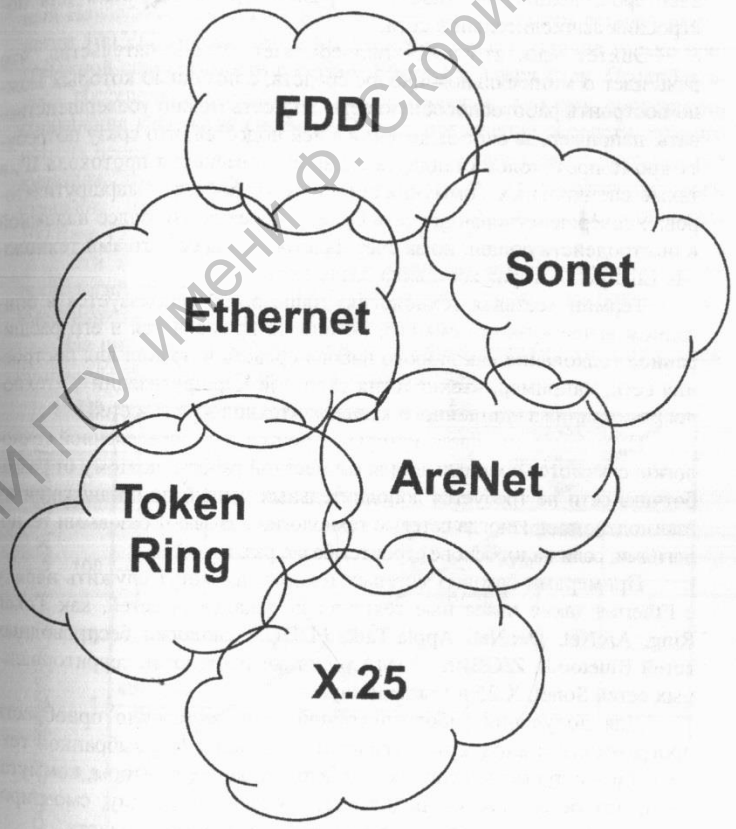
15 Опишите функции и принцип работы сетевого устройства «мост» (bridge).

16 Опишите функции и принцип работы сетевого устройства «трансивер».

17 Опишите функции и принцип работы сетевого устройства «маршрутизатор» (router).

18 Опишите функции и принцип работы сетевого устройства «шлюз».

7 Технологии локальных сетей



7.1 Понятие сетевой технологии

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

Эпитет «достаточный» подчеркивает то обстоятельство, что речь идет о минимальном наборе средств, с помощью которых можно построить работоспособную сеть. Эту сеть можно усовершенствовать, например, за счет выделения в ней подсетей, что сразу потребует кроме протоколов стандарта Ethernet применения протокола IP, а также специальных коммуникационных устройств – маршрутизаторов. Усовершенствованная сеть будет, скорее всего, более надежной и быстродействующей, но за счет надстроек над средствами технологии Ethernet, которая составила базис сети.

Термин «сетевая технология» чаще всего используется в описанном выше «узком» смысле, но иногда применяется и его расширенное толкование как любого набора средств и правил для построения сети, например, «технология сквозной маршрутизации», «технология создания защищенного канала», «технология IP-сетей».

Протоколы, на основе которых строится сеть определенной технологии, создаются специально для совместной работы, поэтому от разработчика сети не требуется дополнительных усилий по организации их взаимодействия. Иногда сетевые технологии называют базовыми технологиями, если на их основе строится базис разных сетей.

Примерами базовых сетевых технологий могут служить наряду с Ethernet такие известные технологии локальных сетей, как Token Ring, ArcNet, DecNet, Apple Talk, FDDI, технологии беспроводных сетей Bluetooth, ZIGBEE, WiMAX или же технологии территориальных сетей Sonet, X.25 и Frame Relay.

Для получения работоспособной сети достаточно приобрести программные и аппаратные средства, относящиеся к выбранной технологии – сетевые адаптеры с драйверами, концентраторы, коммутаторы, другое сетевое оборудование, кабельную систему, смонтировать и соединить их в соответствии с требованиями стандарта.

С экономической точки зрения сетевая технология является аналогом *брэнда* (торговой марки). Удачная комбинация параметров оборудования и программной части обеспечивает рост популярности сетевой технологии и наоборот, просчет в любой из составных частей может оказать весьма негативное влияние.

Известны случаи, когда задержки с выходом на рынок становились причиной прекращения разработки перспективных сетевых технологий.

Ошибки этого типа случались и у больших компаний. Предложенный Hewlett-Packard, AT&T и IBM в 1995 году стандарт сетевой технологии 100 VG AnyLan (IEEE 802.12) поддерживал наличие только программной совместимости с сетями Ethernet и Token Ring. Предполагалось постепенное вытеснение этих технологий, поэтому допускалось сохранение кабельной системы. Однако повышение скорости сетевого обмена ценой замены всего сетевого оборудования не поддержали покупатели. Этим воспользовались конкуренты, которые модифицировали стандарт 10 Base T (IEEE 802.3). Были предложены стандарты 100 Base T2, 100 Base T4 и 100 Base TX (IEEE 802.3u).

Эти и все дальнейшие разработки по модернизации сетевых технологий среди прочих требований удовлетворяют требованию совместимости оборудования «сверху–вниз».

На рисунке 7.1 можно увидеть, какими темпами увеличивалась производительность сетевых технологий.

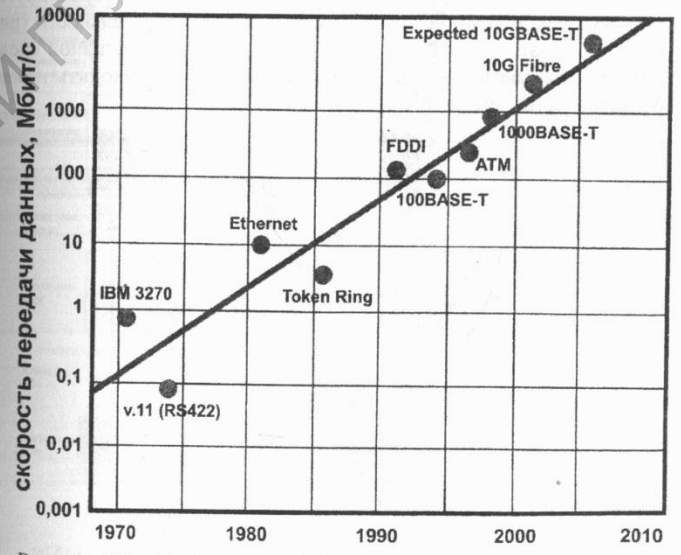


Рисунок 7.1 – График развития популярных сетевых технологий

7.2 Локальные сети ArcNet

Среда ArcNet (*Attached resource computer Network* – вычислительная сеть с присоединенными ресурсами) была разработана Datapoint Corporation в 1977 г. Это простая, гибкая и недорогая сетевая архитектура для сети масштаба рабочей группы.

Первые платы ArcNet были выпущены в 1983 г. Технология ArcNet – предшественница стандартов IEEE Project 802, но в целом она соответствует категории IEEE 802.4. В ней определяются стандарты для сетей с топологией «шина» с методом доступа с передачей маркера, построенные на основе кабеля для модулированной передачи. Сеть ArcNet может строиться только на основе топологий «звезда» или «шина».

Сети ArcNet используют метод доступа с передачей маркера, топологию «звезда», а также «шина» и работают на скорости 2,5 Мбит/с. Преемница сети ArcNet – ArcNet Plus работала на скорости 20 Мбит/с.

В сетях ArcNet маркер проходит не по физическому пути на основе расположения компьютеров, а от одного компьютера к другому согласно закрепленной по их нумерации последовательности (рисунок 7.2). Поэтому ArcNet является довольно неэффективной средой, так как для достижения адресата данные могут проходить намного больший путь, чем необходимо.

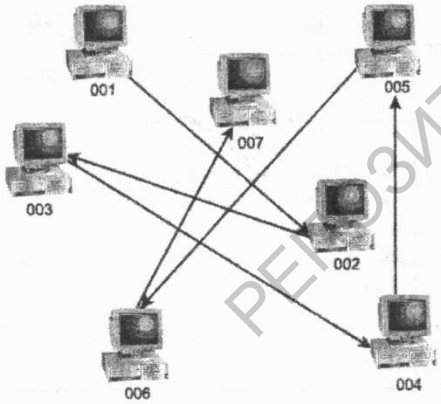


Рисунок 7.2 – Маршрут движения маркера в сети ArcNet

Стандартным для ArcNet считается коаксиальный кабель с полным сопротивлением 93 Ом. ArcNet поддерживает также витую пару и оптоволоконный кабель. Расстояние между компьютерами зависит от используемой кабельной системы. При использовании коаксиального кабеля с BNC-коннекторами и активными концентраторами максимальная длина кабеля от компьютера до концентратора 610 м (2000 футов), если сеть построена по топологии «звезда», и 305 м (1000 футов), если сеть построена по топологии «шина». При использовании неэкранированной витой пары с соединителями длина кабеля между устройствами не более 244 м (800 футов) как при топологии «звезда», так и при топологии «шина».

Каждый компьютер соединяется с концентратором кабелем. Концентраторы бывают пассивными, активными и интеллектуальными (smart). Пассивные концентраторы осуществляют лишь физическую коммутацию проводов. Активные концентраторы способны восстанавливать и ретранслировать сигналы. Интеллектуальные – это активные концентраторы, обладающие диагностическими средствами.

Стандартный кадр ArcNet (рисунок 7.3) поддерживает до 512 байт данных (в ArcNet Plus – до 4096 байт данных).

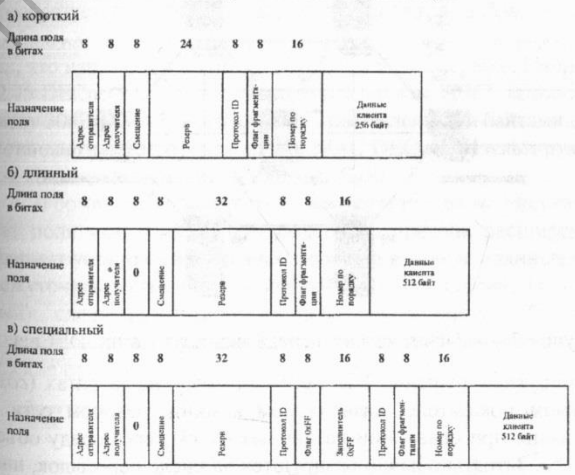


Рисунок 7.3 – Форматы кадров в сетях ArcNet

Сейчас сети ArcNet практически не применяются.

7.4 Локальные сети TokenRing

Сетевая технология *TokenRing* была предложена IBM в 1984 г. для объединения IBM-совместных компьютеров, в том числе:

- персональных станций;
- малых и средних ЭВМ;
- майнфреймов и сред SNA.

Топология сети «кольцо» или «звезда-кольцо» (рисунок 7.6). TokenRing в качестве метода управления доступом станций к передающей среде использует маркерное кольцо.

Кабельная система – коаксиальный кабель, экранированная или неэкранированная витая пара (UPT или SPT) или оптоволокно. Максимальная длина кабеля сегмента зависит от типа кабеля и находится в пределах от 45 до 200 метров.

Данная технология описывается стандартом IEEE 802.5.

Скорость передачи данных от 4 до 16 Мбит/с.

Каждый компьютер сети, получающий кадр, проверяет по адресу назначения – копировать данные в буфер сетевого адаптера или не делать этого. Если пакет предназначен ему, проводится операция копирования и выполняется проверка. После этого состояние фрейма изменяется на «доставлено». Пакет следует дальше по кольцу, пока не достигнет станции отправителя. Тот по состоянию фрейма решает, что делать дальше:

- прекратить передачу и выпустить маркер из-за успешной доставки сообщения;
- прекратить передачу из-за отсутствия адресата;
- повторить передачу.

Сетевая технология TokenRing – это физическое кольцо, реализованное с помощью кабеля либо внутри концентратора MAU. Все сетевые адреса базируются на MAC-адресах. MAC-адреса закреплены фирмой-изготовителем.

В IBM Token Ring используются три основных типа кадров:

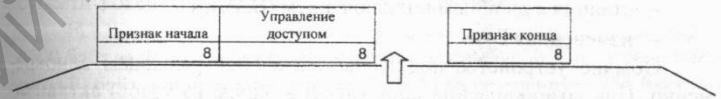
- кадр «Управление/Данные» (Data/Command Frame). С помощью такого пакета выполняется передача данных или команд управления работой сети;
- кадр «Маркер» (Token). Станция может начать передачу данных только после получения такого кадра;
- кадр «Сброс» (Abort). Посылка такого кадра вызывает прекращение любых передач.

Рисунок 7.6 – Алгоритм информационного обмена в сети TokenRing

Для сетей Token Ring характерны высокая надежность и устойчивость, однако вследствие более высокой стоимости и меньшей пропускной способности они менее популярны, чем Ethernet. Существует также стандарт IBM High Speed Token Ring 100 – 155 Мбит/с.

В настоящее время разрабатываются спецификации для Gigabit TokenRing, эта архитектура считается перспективной.

Формат кадра/маркера и описание полей представлены на рисунке 7.7.



Управление фреймом	Адрес назначения	Адрес источника	RIF	DSAP	SSAP	CTRL	Данные	FCS	Состояние фрейма
8	16 или 48	16 или 48	144	8	8	8 или 16	>0	32	8

Стартовый разграничитель	В кадре Token Ring играет ту же роль, что и преамбула в кадре Ethernet
Поле управления доступом	Указывает, является ли кадр маркером или кадром данных. Определяет также приоритет кадра
Поле управления кадром	Содержит информацию об управлении доступом
Адрес назначения	Адрес компьютера, на который передается этот кадр
Адрес источника	Адрес передающего компьютера
Данные	Передаваемая информация (например, содержимое передаваемого файла)
FCS	Frame Check Sequence. Проверочное поле с битами CRC
Конечный разграничитель	Отмечает конец кадра
Поле состояния кадра	Указывает, был ли адрес распознан, а кадр скопирован (заполняется принимающим компьютером перед отправкой кадра обратно в кольцо)

Рисунок 7.7 – Формат кадра TokenRing

7.5 Локальные сети FDDI

Сетевая технология *FDDI* (*Fiber Distributed Data Interface – распределенный интерфейс передачи данных по волоконно-оптическим кабелям*) считается наследником TokenRing. Она разработана в национальном институте стандартизации США в 1988 г. и позволила использовать оптоволоконные среды передачи на скорости 100 Мбит/с.

Метод доступа к среде – маркерный, с возможностью одновременного циркулирования множества кадров в кольце.

Сеть FDDI строится на основе двух оптоволоконных колец, которые образуют основной и резервный пути передачи данных между узлами сети. В нормальном режиме работы сети данные проходят через все узлы и все участки кабеля первичного (Primary) кольца, поэтому этот режим назван режимом Thru – «сквозным» или «транзитным». Второе кольцо (Secondary) в этом режиме не используется.

В некоторых случаях вторичное кольцо используется для повышения пропускной способности потенциально до 200 Мбит/с. Пакеты по этим кольцам движутся в противоположных направлениях.

Сетью FDDI поддерживается 3 типа станций:

- станция с одинарным подключением (SAS);
- станция с двойным подключением (DAS);
- измененная DAS.

Обычно устройства подключаются к обоим кольцам одновременно. При возникновении сбоя (отказ в одном из узлов) активизируется и второе кольцо, что заметно повышает надежность системы, позволяя обойти неисправный участок (рисунок 7.8). Этот режим работы сети называется Wrap, то есть «сворачивание» колец.

а) б)

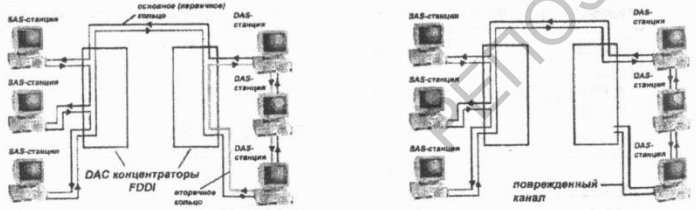


Рисунок 7.8 – Сворачивание FDDI при отказе соединения:
а) нормальный режим работы; *б*) режим работы Warp

В оригинальном варианте технологии FDDI поддерживается до 1000 клиентов со скоростью передачи данных 100 Мбит/сек. Рабочие станции могут располагаться на расстоянии 2 км друг от друга для многомодового оптоволокна и до 4,5 км для одномодового, а вся сеть может простираться на расстояние до 200 км.

Нетрадиционным для других сетей является концентратор, используемый в сетях FDDI. Он позволяет подключить несколько приборов SAS-типа к стандартному FDDI-кольцу, создавая структуры типа дерева. Но такие структуры несут в себе определенные ограничения на длины сетевых элементов, так как при использовании повторителя удаление не должно превышать 1,5 км, а в случае моста 2,5 км (одномодовый вариант).

Концентраторы также бывают двух типов: двойного (DAS) и одинарного (SAS) подключения. Такие приборы повышают надежность сети, так как не вынуждают сеть при отключении отдельного прибора переходить в аварийный режим обхода. Применение концентраторов снижает и стоимость подключения к FDDI. Концентраторы могут помочь при создании небольших групповых субсетей, предназначенных для решения специфических задач, то есть локализовать трафик. К кольцу FDDI могут также легко подключаться и субсети Token Ring (через мост или маршрутизатор).

FDDI позволяет работать с кадрами (рисунок 7.9) размером 4500 байт за вычетом места, занимаемого преамбулой. При этом остается 4470 байт для передачи данных. RFC-1188 резервирует 256 байт для заголовков, оставляя для данных 4096 байт. Маршрутизатор, поддерживающий протокол FDDI, должен быть способен принимать такие длинные пакеты. Посылаться же должны дейтограммы не длиннее 576 байт, если не ясно, сможет ли адресат принимать длинные кадры.

Длина поля в битах	16	1	1	6(2)	6(2)		4(8)	2(4)
Назначение поля	Преамбула	Стартовый разделитель	Управление	Адрес отправителя	Адрес получателя	Данные клиента	Контрольная сумма CRC	Конечный разделитель

Рисунок 7.9 – Формат кадра протокола FDDI

На текущий момент эта технология вытесняется с рынка сетями с ячеистой топологией и более высокоскоростными сетевыми технологиями (например, Gigabit Ethernet), также использующими оптоволоконный кабель в качестве среды передачи данных.

7.6 Локальные сети Apple Talk

Сетевая архитектура *AppleTalk* предложена компанией Apple Computer в 1983 г. для небольших рабочих групп. Сетевая топология сетей AppleTalk «шина» или «дерево». Стандартная рабочая группа AppleTalk состояла из двух рабочих станций и принтера. Метод доступа в данной сетевой архитектуре – CSMA/CA. В сети AppleTalk чаще всего используются экранированные витые пары, однако возможно также использование волоконно-оптических кабелей и неэкранированных витых пар. Формат кадра показан на рисунке 7.10.

Число шагов (1)	Длина дейтограммы (1)
DDP контрольная сумма (2)	
Сеть адресат (2)	
Сеть отправитель (2)	
Идентификатор узла назначения (1)	Идентификатор узла отправителя (1)
Socket узла назначения (1)	Socket узла отправителя (1)
Тип DDP (1)	Данные от 0 до 586 октетов

Рисунок 7.10 – Формат кадров Apple Talk Phase II (размеры в байтах)

Каждый компьютер, подключаемый к сети, ищет хранимый адрес, который он использовал в предыдущем сеансе. Если компьютер находит этот адрес, то использует его. В противном случае он присваивает себе адрес, случайно выбранный из набора предлагаемых адресов. Затем компьютер сообщает этот адрес всем другим компьютерам, чтобы определить, использует ли его еще кто-нибудь. Если да, то процесс поиска адреса повторяется. Если нет, то компьютер сохраняет этот адрес для использования в следующих сеансах.

Программная модель данной сети (стек протоколов) позволяет наиболее гибко реагировать на взаимодействие с другими сетями:

– сеть AppleTalk делится на «зоны» (рисунок 7.11), в каждой зоне может присутствовать до 32 устройств, в модификации – до 254;

– сервер программной части стека протокола – AppleShare;

– клиенты имеют произвольный выбор для подключения к сетевым серверам одной из следующих частей стека протокола:

а) для работы с AppleShare – LocalTalk;

б) для подключения к Ethernet – EtherTalk;

в) для подключения к TokenRing – TokenTalk.

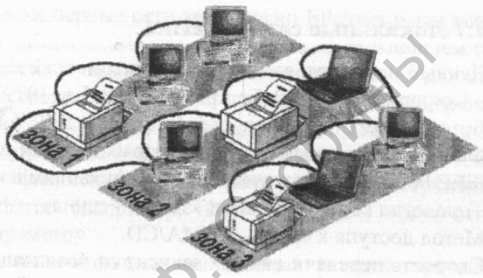


Рисунок 7.11 – Пример сети AppleTalk

Сеть AppleTalk типа Phase 1 являлась изначальной архитектурой протокола AppleTalk, разработанной для поддержки сетей для небольших рабочих групп. Тип Phase 1 поддерживает только одну физическую сеть, с одним сетевым номером и одной зоной.

Большие сети AppleTalk не являются едиными физическими сетями, в которых все компьютеры подключены к одной и той же физической линии связи. Вместо этого они представляют собой объединенные сети, которые являются многочисленными маленькими сетями, соединенными между собой посредством *маршрутизаторов*.

В сети AppleTalk типа Phase 2 усовершенствованы службы маршрутизации и имен AppleTalk. Это приводит к снижению сетевой нагрузки и упрощению выбора маршрутизаторов. Благодаря этому стало возможным создание сетей AppleTalk, поддерживающих более 254 узлов и включающих множество зон.

Любая сеть LocalTalk должна принадлежать одной зоне, а для сетей EtherTalk и TokenTalk можно назначить несколько зон. Отдельные узлы сети можно включить в одну из этих зон.

Каждый компьютер клиента, принтер, сервер и маршрутизатор является узлом сети AppleTalk. Теоретически в сети AppleTalk типа Phase 2 может быть до 254 узлов, но на самом деле их количество ограничено 32 или меньшим числом, что определяется производительностью сетевых сред. Сети EtherTalk и TokenTalk могут иметь по 253 узла на каждый номер в диапазоне номеров сети, но не больше 16,5 миллионов узлов.

Согласно спецификациям пропускная способность сети AppleTalk, по сравнению с другими видами сетей, невелика – 230,4 Кбит/с, поэтому в ней невозможно реализовать высокоскоростные приложения.

7.7 Локальные сети Ethernet

Данный стандарт является продуктом совместной разработки Xerox Corporation, Digital Equipment и Intel в 1979 году на основе разработок Xerox Corporation, сделанных еще в 1975 году.

Фактически данный стандарт разрабатывался параллельно проекту IEEE 802 и соответствует его спецификациям в части IEEE802.3.

Топология сети – «шина» и «звезда – шина».

Метод доступа к среде – CSMA/CD.

Скорость передачи данных зависит от реализации (1, 5, 10, 100, 1000, 10000 Мбит/с).

Физическая среда передачи – коаксиальный кабель, оптоволокно, витая пара и другие виды кабельных и беспроводных связей.

На физическом уровне Ethernet используют кодирование сигнала, которое для соблюдения технологии совместимости осуществляется «сверху-вниз» практически во всех стандартах одинаково. Это манчестерское кодирование сигнала. Исключением является стандарт – 10 BROAD 36, в котором используется кодирование сигнала DPSK.

Эффективная длина сегмента зависит от используемой среды передачи и колеблется от 100 м для витой пары до 2,5 км при использовании оптоволокна.

Формат кадра для сети Ethernet также меняется в зависимости от стандарта, но не значительно. При этом в различных вариантах длина пакета может быть фиксированной или изменяющейся (рисунок 7.12).

Длина поля в байтах	8	6	6	2	46-1500	4
Тип поля	Преамбула	Адрес получателя	Адрес отправителя	Тип протокола	Данные клиента	CRC

Рисунок 7.12 — Пример формата кадра Ethernet

Второй подход («сжатие») заключается в группировке пакетов в большие блоки. Современные скоростные сети (1 Гбит/с и выше) используют механизм группировки пакетов и увеличения частоты генерации сигналов, что накладывает дополнительные требования на среду передачи. Таким образом, среда передачи в Ethernet может использоваться следующим образом: коаксиальный кабель – до 10 Мбит/с, витая пара – до 1 Гбит/с, более высокоскоростные режимы реализуются на оптоволокне.

В беспроводных сетях скорость регулируется возможностями оборудования.

Исторически первые сети технологии Ethernet были созданы на коаксиальном кабеле диаметром 0,4 дюйма. В дальнейшем были определены и другие спецификации физического уровня для стандарта Ethernet, позволяющие использовать различные среды передачи данных в качестве общей шины. Метод доступа CSMA/CD и все временные параметры Ethernet остаются одними и теми же для любой спецификации физической среды, хотя малораспространенные модификации Ethernet (например, 100 VG AnyLAN) могут отличаться по данному параметру.

Наименование модификации Ethernet расшифровывается так, как показано на рисунке 7.13.

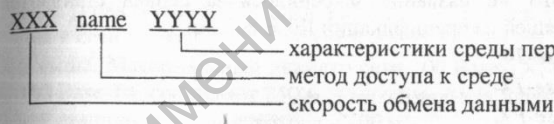


Рисунок 7.13 – Формирование названия стандарта Ethernet

Так например, 10 Base-T – это сеть Ethernet на витой паре UTP-3, методом доступа CSMA/CD и скоростью обмена данных 10 Мбит/с.

Самая распространенная ошибка в сетях Ethernet – возникновение *коллизии*. *Домен коллизий* – это часть сети Ethernet, все узлы которой распознают коллизию, вне зависимости от того, в какой части сети эта коллизия возникла.

Для того, чтобы сеть Ethernet, состоящая из сегментов различной физической природы, работала корректно, необходимо выполнение трех основных условий:

– количество станций в сети не должно превышать 1024 (с учетом ограничений для коаксиальных сегментов);

– удвоенная задержка распространения сигнала (Path Delay Value, PDV) между двумя самыми удаленными друг от друга станциями сети не должна превышать 575 битовых интервалов;

– сокращение межкадрового расстояния (Interpacket Gap Shrinkage) при прохождении последовательности кадров через все повторители не более, чем в два раза (при отправке кадров начальное межкадровое расстояние 96 битовых интервалов).

Поскольку сети этого стандарта широко распространены на территории нашей страны, рассмотрим более современные его модификации.

7.8 Локальные сети Ethernet 100 Мбит/с

Локальные сети Ethernet со скоростью передачи 100 Мбит/с принято называть сети Fast Ethernet. Впервые это название было присвоено стандарту 100 VG AnyLAN, который был совместим с существующим тогда стандартом Ethernet 10 Base-T по среде передачи (витая пара категории 3), но абсолютно несовместим по оборудованию, в том числе из-за метода доступа к среде с использованием приоритетов. Большинство пользователей отказались от перспективы замены такого количества элементов своих локальных сетей, в результате чего стандарт не прижился.

Сейчас это же название закрепилось за серией стандартов Ethernet, состоящей из спецификаций IEEE 802.3u:

- *100 Base-T4;*
- *100 Base-TX*;
- *100 Base-FX.*

Такое разделение необходимо для обеспечения поддержки стандартом трех типов среды передачи: неэкранированной витой пары, экранированной витой пары и оптоволокна.

В этих сетях решена задача совместимости по оборудованию с предыдущими сетевыми стандартами, поскольку в каждой из них применен метод доступа к среде CSMA/CD, т. е. поддерживается связь между любыми сетевыми адаптерами Ethernet со скоростью передачи данных от 10 до 100 Мбит/с.

Сети *100 Base-T4* в качестве среды передачи используют кабель с четырьмя неэкранированными или экранированными витыми парами категории 3, 4 или 5. Для своевременного обнаружения коллизий диаметр сети был уменьшен до 250 м, а максимальное расстояние между узлом сети и портом концентратора до 100 м.

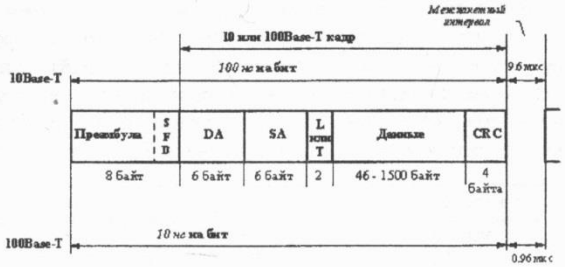
С целью повышения скорости передачи для передачи сигналов задействованы три витые пары (плюс одна витая пара для обнаружения коллизий), что позволило втрое увеличить скорость по сравнению с сетью 10 Base-T. Вместо манчестерского кодирования применили схему кодирования 8B6T, в которой 8 входных бит преобразовываются в уникальную кодовую группу из 6 троичных символов, что увеличило пропускную способность еще в 2,65 раза. Повышение тактовой частоты с 20 до 25 МГц, обеспечило увеличение пропускной способности еще в 1,25 раза. В результате всех перечисленных изменений 100 Base-T4 работает в 10 раз быстрее, чем 10 Base-T.

Сети 100 *Base-TX* также ориентированы на витую пару, но, в отличие от вышеописанной спецификации, из четырех пар перевитых проводов кабеля UTP категории 5 используются только две. Одна из витых пар используется для передачи, другая служит для обнаружения коллизий и приема данных.

Применение двух витых пар вместо четырех, как в стандарте 100 Base-T4, требует изменения тактовой частоты и метода кодирования. В сетях 100 Base-TX используется тактовая частота 125 МГц и схема кодирования 4B5B, в которой каждые 4 бита данных кодируются с помощью 5 бит. Таким образом, для представления данных необходимо только 16 символов, оставшиеся символы служат в качестве управляющих. Тактовая частота 125 МГц предъявляет требования к сети передачи – это может быть только кабель UTP категории 5 и выше. Максимальный диаметр сети 100 Base-TX, равно как и сети 100 Base-T4, составляет 250 м, а максимальная длина кабеля от рабочей станции до концентратора – 100 м.

Сети 100 *Base-FX* ориентированы на использование двужильного многомодового волоконно-оптического кабеля диаметром 62,5 или 125 мкм. Передача сигналов производится в световом диапазоне 1350 нм, а длина сегмента в стандарте 100 Base-FX может достигать 412 м. Передача и прием данных разведены по отдельным жилам, которые обрабатываются одним сетевым адаптером. Схема кодирования в 100 Base-FX та же, что и в стандарте 100 Base-TX.

На рисунке 7.14 показано соотношение кадров данных в сети 100 Base-TX.



SFD (Start of Frame Delimiter) – ограничитель начала кадра
DA, SA – адреса назначения и источника соответственно
L – длина поля данных (для кадра 802.3)
T – тип протокола в поле данных (для Ethernet II)

Рисунок 7.14 – Организация совместимости кадров Ethernet

7.9 Гигабитные сети Ethernet

Разработка стандарта Gigabit Ethernet началась в марте 1996 года, когда комитет IEEE 802.3 одобрил проект стандарта Ethernet для сетей, которые способны работать со скоростью 1 Гбит/с. Группа разработчиков предложила проект стандартизации IEEE 802.3z Gigabit Ethernet. В июле 1997 года был создан предварительный стандарт передачи сигналов в сети с волоконно-оптическими каналами и сегментами, находящимися на небольших расстояниях и соединенными посредством медных проводов, который утвердили в 1999 году. Параллельно шла работа специального комитета (802.3ab) для разработки стандарта передачи сигналов в медной витой паре, совместимого с Gigabit Ethernet.

При разработке учитывался тот факт, что в сети Ethernet с протоколом CSMA/CD временная задержка, зависящая от максимальной длины кабеля, влияет на минимальный размер кадра.

В сетях Ethernet со скоростью передачи 10 Мбит/с максимальная дистанция между узлами одной сети составляла 2,5 км. В Ethernet со скоростью передачи 100 Мбит/с для сохранения масштаба кадра максимальная длина кабеля между двумя узлами была уменьшена до 250 м, а максимальное расстояние от станции до концентратора – до 100 м.

Если размер кадра не изменяется, максимальное расстояние передачи по медному проводу между двумя узлами в сети Gigabit Ethernet не должно превышать 25 м, чего недостаточно для эффективного использования данной технологии.

С целью обеспечения совместимости с предыдущими версиями Ethernet, в которых расстояние передачи 100 м, в стандарте Gigabit Ethernet все кадры, длина которых меньше 512 байт, заполняются специальными дополнительными символами, что необходимо для функционирования механизма обнаружения коллизий. Такой метод называется *расширением носителя* (рисунок 7.15).

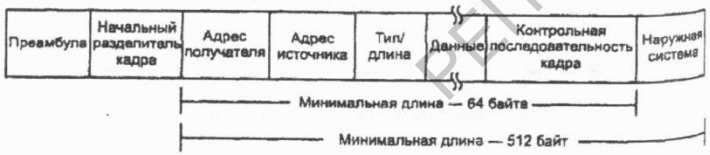


Рисунок 7.15 – Формирование кадров по методу расширения носителя

Очевидно, что когда фактическое количество передаваемых данных меньше или равно 512 байт, подобная передача малоэффективна, а производительность сети ненамного выше производительности Fast Ethernet.

Другой метод, предназначенный для повышения производительности, известен как *передача пакетов блоками*.

При передаче кадров блоками станция, имеющая два и больше пакетов для передачи, отправляет первый кадр (если его длина меньше 512 байт) с использованием техники расширения носителя. Если этот пакет передается без коллизий, то все последующие пакеты поочередно отсылаются в течение времени, необходимого для передачи блока длиной 1500 байт. Если станция не успеет полностью переслать какой-либо из пакетов, она это сделает по истечении данного периода (рисунок 7.16).

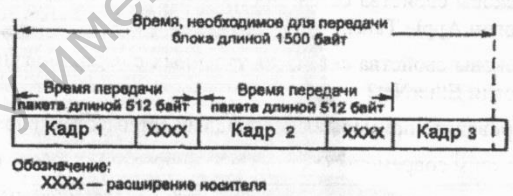


Рисунок 7.16 – Технология передачи кадров блоками

Если вы применяете сеть Gigabit Ethernet с целью соединения двух коммутаторов ЛВС или с целью соединения рабочих станций и серверов непосредственно с портами коммутаторов ЛВС, то коллизий в таком соединении не будет. Другими словами, для гарантии того, что коллизии будут обнаружены в течение заранее определенного периода времени, нет необходимости расширять кадр, то есть применять технику передачи блока пакетов не требуется.

Хотя сеть Gigabit Ethernet и не использовала все свои возможности, уже реализована технология 10 Gigabit Ethernet (IEEE 802.3ae, 10 GBase-LW или 10 GBase-ER). Этот стандарт утвержден в июне 2002 года и в случае использования для построения региональных каналов соответствует спецификациям OC-192c/SDH VC-4-46c (WAN). В протоколе 10 Gigabit Ethernet предусмотрен интерфейс chip-to-chip (802.3ae-XAUI – буквы **ae** означают здесь Ethernet Alliance – www.10gea.org).

Вопросы для самоконтроля

1 Что такое сетевые технологии и зачем они применяются?

2 Каковы свойства сетей, построенных с использованием сетевой технологии ArcNet?

3 Каковы свойства сетей, построенных с использованием сетевой технологии DECnet?

4 Каковы свойства сетей, построенных с использованием сетевой технологии TokenRing?

5 Каковы свойства сетей, построенных с использованием сетевой технологии FDDI?

6 Каковы свойства сетей, построенных с использованием сетевой технологии Apple Talk?

7 Каковы свойства сетей, построенных с использованием сетевой технологии EtherNet?

8 Приведите примеры беспроводных сетевых технологий.

9 Каковы современные стандарты скоростей сетевого обмена?

10 Какие перспективы роста скоростей передачи данных?

11 Как оценить эффективность использования сетевой технологией среды передачи данных?

12 Возможно ли увеличение скоростных характеристик сети без изменения структуры кабельной системы?

13 Какие способы существуют для объединения сетевых технологий в рамках одной сети?

14 Какие ошибки могут возникать при передаче данных в различных сетевых технологиях?

15 Какие способы для повышения надежности передачи данных применяются в различных сетевых технологиях?

8 Адресация в компьютерных сетях

8.1 Общие положения адресации

Адресация в сети – это процесс, состоящий из нескольких этапов преобразования адресной информации для установления однозначного соответствия адреса приемника приемнику, а адреса источника – источнику. Еще одно название – отображение или разрешение имен. Процесс делится на три этапа, соответствующие трем логическим уровням адресации: прикладному, транспортному и сетевому, что хорошо соотносится с эталонной моделью OSI.

На верхнем уровне адресации используются специальные имена, например, идентификаторы процессов, рабочих станций или символьные доменные имена. [4] Они предназначены для конкретных процессов, программ ими управляющих, а также для пользователей. Дополнительное назначение адресов верхнего уровня – удобство работы программистов и/или пользователей при обращении к сетевым ресурсам, что помогает существенно увеличить скорость при использовании сетевых ресурсов и управлении ими.

Примером могут служить имена NetBIOS в сетях MicroSoft, которые могут включать до 16 символов. Первые 15 символов можно использовать для указания понятного имени компьютера, а шестнадцатый символ зарезервирован для указания службы компьютера, которая передает информацию. Чаще всего NetBIOS-адресация в сетях MicroSoft используется поверх протокола TCP/IP.

Адреса сетевого уровня назначаются и используются операционной системой и программами управления сетевых устройств. Здесь решаются вопросы маршрутизации, что накладывает свои требования на структуру адресных конструкций. У работающей операционной системы может быть один и более сетевых адресов. При этом, если используется несколько интерфейсных карт, то операционная система должна назначить однозначное соответствие каждого сетевого адреса конкретному порту сетевого обмена, например, сетевому адаптеру. Для этого в самой нижней части адресного стека применяются физические адреса устройств (MAC-адреса).

Передача информационных импульсов по любой среде передачи может и должна быть принята любым другим сетевым устройством, которое подключено к этой среде. Таким образом, именно MAC-адреса позволяют перенаправить пакет конкретному сетевому адаптеру или модему, или любому другому активному сетевому оборудованию.

В общем случае к адресу сетевого интерфейса и схеме его назначения можно предъявить несколько требований:

– адрес должен уникально идентифицировать сетевой интерфейс в сети любого масштаба;

– схема назначения адресов должна сводить к минимуму ручной труд администратора и вероятность дублирования адресов;

– желательно, чтобы адрес имел иерархическую структуру, удобную для построения больших сетей;

– адрес должен быть удобен для пользователей сети, то есть он должен допускать символьное представление;

– адрес должен быть по возможности компактным, чтобы не перегружать память коммуникационной аппаратуры.

Можно перечислить следующие примеры подходов к решению задачи распределения адресов:

– уникальные статические адреса;

– выбор из фиксированного подмножества статических адресов;

– статические адреса, назначаемые администратором;

– динамические адресные системы:

– централизованные;

– децентрализованные;

– случайные адресные системы.

Адреса могут использоваться для идентификации:

– отдельных интерфейсов;

– групп интерфейсов;

– сразу всех сетевых интерфейсов сети (широковещательные).

Одна из классических систем адресации сводится к тому, что при установке сети каждому абоненту присваивается индивидуальный адрес по порядку, к примеру, от 0 до 30 или от 0 до 254. Присваивание адресов производится программно или с помощью переключателей на плате адаптера. При этом требуемое количество разрядов адреса определяется из неравенства:

$$2^n > N_{max},$$

где n – количество разрядов адреса, а N_{max} – максимально возможное количество абонентов в сети. Например, восемь разрядов адреса достаточно для сети из 255 абонентов. Один адрес отводится для широковещательной передачи, то есть он используется для пакетов, адресованных всем абонентам одновременно. К примеру, механизм, аналогичный этому, применяется в сети ArcNet.

8.2 Система адресации на уровне MAC

Подуровень MAC канального уровня модели OSI работает с физическими адресами, которые называются MAC-адресами. Они применяются в сетях Ethernet, Fast Ethernet, Token-Ring, FDDI, 100 VG-AnyLAN и представляют собой 12 шестнадцатеричных цифр (48 бит), записанных в микросхему сетевого адаптера (например, 17:A4:2C:43:2F:09).

Эти 48 бит имеют жесткую структуру (рисунок 8.1), при этом два старших разряда адреса управляющие, они определяют тип адреса и способ использования остальных 46 разрядов.

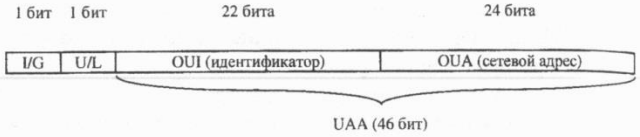


Рисунок 8.1 – Структура MAC-адреса

Старший бит I/G (Individual/Group) указывает на тип адреса. Если он установлен в 0, то индивидуальный, если в 1, то групповой (многопунктовый или функциональный). Пакеты с групповым адресом получат все имеющие этот групповой адрес сетевые адаптеры. Причем групповой адрес определяется 46 младшими разрядами.

Второй управляющий бит U/L (Universal/Local) называется флажком универсального/местного управления и определяет то, как был присвоен адрес данному сетевому адаптеру. Обычно он установлен в 0. Установка бита U/L в 1 означает, что адрес задан не производителем сетевого адаптера, а организацией, использующей данную сеть. Это случается довольно редко.

Для широковещательной передачи (всем абонентам сети одновременно) применяется специально выделенный сетевой адрес, все 48 битов которого установлены в единицу. Его принимают все абоненты сети независимо от их индивидуальных и групповых адресов.

Следующие 22 разряда адреса называются OUI (Organizationally Unique Identifier) – уникальный идентификатор, выделяемый организации.

IEEE присваивает один или несколько OUI каждому производителю сетевых устройств. Это позволяет исключить совпадения адресов адаптеров от разных производителей. Всего возможно свыше

4 миллионов разных OUI, это означает, что теоретически может быть зарегистрировано 4 миллиона производителей.

Также за этим полем закрепилось второе название «адресный диапазон». Фактически любая организация может приобрести любое количество адресных диапазонов.

Младшие 24 разряда называются OUA (Organizationally Unique Address) – уникальный адрес, назначаемый организацией.

Именно это поле заполняет каждый из зарегистрированных производителей сетевых устройств. Всего возможно свыше 16 миллионов комбинаций, то есть каждый изготовитель может адресовать 16 миллионов сетевых интерфейсов на каждый OUI.

Вместе OUA и OUI называются UAA (Universally Administered Address) – универсально управляемый адрес или IEEE-адрес.

Недостатком MAC-адресации считается сложность структуры сетевых адаптеров, а также большая доля служебной информации в передаваемом пакете (адреса источника и приемника вместе требуют уже 96 бит пакета или 12 байт).

Во многих сетевых адаптерах предусмотрен так называемый циркулярный режим. В этом режиме адаптер принимает все пакеты, приходящие к нему, независимо от значения поля адреса приемника. При этом один компьютер принимает и контролирует все пакеты, проходящие по сети, но сам ничего не передает. В данном режиме работают сетевые адаптеры мостов и коммутаторы, которые должны обрабатывать перед ретрансляцией все пакеты, приходящие к ним.

Данная система адресации используется в таких сетях как: Ethernet, Fast Ethernet, Token Ring, FDDI, 100 VG-AnyLAN.

Теоретически во всем мире не должно быть двух сетевых адаптеров с одинаковыми MAC-адресами. Однако на практике иногда происходят ошибки у производителей, присваивающих адаптерам уже использованные адреса. Кроме того, некоторые производители исчерпали выделенные им номера и начали нумерацию сначала. Повторяющиеся MAC-адреса вызывают проблемы, если два сетевых адаптера с одинаковым MAC-адресом принадлежат одной и той же сети.

Для собственных целей администраторы сетей часто меняют MAC-адрес как динамический параметр «перезаписываемой» микросхемы. Например, сетевые адаптеры, интегрированные в материнские платы отдельных производителей, имеют ручную настройку этого параметра в CMOS-настройках BIOS материнской платы.

8.3 Система адресации IPX

Протоколы IPX/SPX, разработанные компанией Novell, образуют набор (стек), используемый в сетевых программных средствах довольно широко распространенных локальных сетей Novell (NetWare). Это сравнительно небольшой и быстрый протокол, поддерживающий маршрутизацию.

Прикладные программы могут обращаться непосредственно к уровню IPX, например, для посылки широковещательных сообщений, но значительно чаще работают с уровнем SPX, гарантирующим быструю и надежную доставку пакетов.

Компанией Microsoft предложена своя реализация протокола IPX/SPX, называемая NWLink. Протоколы IPX/SPX и NWLink поддерживаются операционными системами NetWare и Windows. Выбор этих протоколов обеспечивает совместимость по сети любых абонентов с данными операционными системами.

Таким образом, в сетях IPX реализуется быстрая передача данных между узлами различных сетей. Недостатком механизма передачи является лавинообразный рост широковещательных сообщений, препятствующий организации сложных сетей с большим количеством узлов.

Протокол IPX является низкоуровневым (относительно уровней модели OSI), поэтому он непосредственно инкапсулирует свою информацию, называемую дейтаграммой, в поле данных кадра, передаваемого по сети (рисунок 8.2).

Рисунок 8.2 — Инкапсуляция данных

При этом в заголовок дейтаграммы входят адреса абонентов (отправителя и получателя) более высокого уровня, чем MAC-адреса, – это IPX-адреса для протокола IPX или IP-адреса (для сетей Microsoft). Эти адреса включают номера сети и узла, хоста (индивидуальный идентификатор абонента). При этом IPX-адреса довольно просты и имеют единственный формат (рисунок 8.3).

4 байта	6 байт
номер сети	идентификатор станции (MAC-адрес абонента)

Рисунок 8.3 — Формат IPX-адреса

Номер сети – это код, присвоенный каждой конкретной сети, то есть каждой широковещательной области единой сети.

Под широковещательной областью понимается часть сети, которая прозрачна для широковещательных пакетов, пропускает их беспрепятственно.

Для маршрутизации пакетов в объединенных сетях IPX использует протокол динамической маршрутизации, называемый RIP (Routing Information Protocol – протокол маршрутной информации). В настоящее время RIP является наиболее часто используемым протоколом для внутренних роутеров (interior gateway protocol-IGP) в сообществе Internet. По протоколу RIP все сети имеют номера (способ образования номера зависит от используемого в сети протокола сетевого уровня), а все маршрутизаторы – идентификаторы. Протокол RIP широко использует понятие «вектор расстояний». Вектор расстояний представляет собой набор пар чисел, являющихся номерами сетей и расстояниями до них в *хопах*.

Вектора расстояний итерационно распространяются маршрутизаторами по сети, и через несколько шагов каждый маршрутизатор имеет данные о достижимых для него сетях и о расстояниях до них. Если связь с какой-либо сетью обрывается, то маршрутизатор отмечает этот факт тем, что присваивает элементу вектора, соответствующему расстоянию до этой сети, максимальное значение, которое имеет специальный смысл – «связи нет». Таким значением в протоколе RIP является число 16.

При использовании протокола RIP работает эвристический алгоритм динамического программирования Беллмана-Форда, и решение, найденное с его помощью, является не оптимальным, а близким к оптимальному.

8.4 Система адресации AppleTalk

Для обеспечения минимальных затрат, связанных с работой администратора сети, адреса узлов AppleTalk назначаются динамично. Когда компьютер Macintosh начинает работу в сети AppleTalk, он выбирает случайный адрес протокола (сетевого уровня) и проверяет его, чтобы убедиться, что этот адрес не используется в данный момент. Если адрес свободен, то новый узел присваивает себе выбранный адрес. Если выбранный адрес используется, то узел, владеющий адресом, отправляет сообщение, указывающее на наличие проблемы. Новый узел выбирает другой адрес, повторяет процесс проверки и так до тех пор, пока он не найдет свободный адрес.

На рисунке 8.4 представлен процесс выбора новым узлом сетевого адреса в среде AppleTalk.

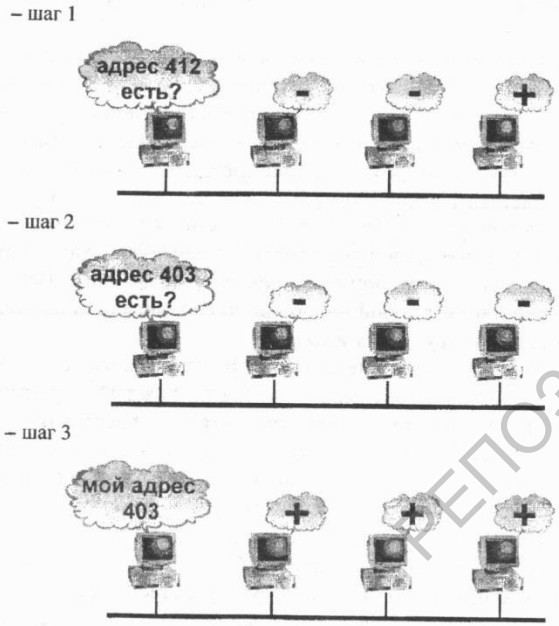


Рисунок 8.4 – Выбор адреса клиентом сети AppleTalk

AppleTalk идентифицирует несколько сетевых объектов. Самым простым является узел (node), который является просто любым устройством, соединенным с сетью AppleTalk. Следующим объектом является сеть. Сеть AppleTalk представляет собой просто отдельный логический кабель. Хотя этот логический кабель часто является отдельным физическим кабелем, некоторые вычислительные центры используют мосты для объединения нескольких физических кабелей. И, наконец, зона (zone) AppleTalk является логической группой из нескольких сетей. Объекты AppleTalk изображены на рисунке 8.5.

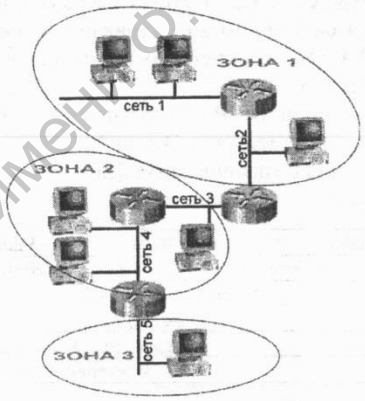


Рисунок 8.5 – Объекты AppleTalk

Основным протоколом сетевого уровня AppleTalk является протокол DDP. Адреса AppleTalk, назначаемые DDP, состоят из двух компонентов: 16-битового номера сети (network number) и 8-битового номера узла (node number). Эти два компонента обычно записываются в виде десятичных номеров, разделенных точкой (например, 10.1 означает сеть 10, узел 1). Если номер сети и номер узла дополнены 8-битовым гнездом (socket), обозначающим какой-нибудь особый процесс, то это означает, что в сети задан уникальный процесс.

AppleTalk Phase II делает различие между нерасширенными (nonextended или сетями AppleTalk Phase I) и расширенными (extended) сетями. В нерасширенных сетях, таких как LocalTalk, номер каждого узла AppleTalk уникален. В расширенных сетях (EtherTalk, TokenTalk), уникальной является комбинация: номер каждой сети/номер узла.

8.5 Система адресации IP v.4

IP-адресация – это адресация сетевого уровня. На этом уровне реализуется функция управления маршрутом продвижения данных по сети. IP-адресация эффективно объединяет сети любого масштаба и при этом позволяет снизить число широковещательных сообщений в сетях.

IP-адреса назначаются и используются операционной системой. У работающей операционной системы может быть один и более IP-адресов. При этом, если используется несколько интерфейсных карт, то операционная система должна назначить однозначное соответствие каждого IP-адреса конкретному порту сетевого обмена, например, сетевому адаптеру.

Механизм адресации IP v.4 предполагает деление адреса на 2 части: номер сети и номер узла. Эта информация занимает 4 байта и обычно разделяется по границе байта. [2]

Спецификации IP v.4 адреса разделяют на 5 классов (рисунок 8.6).

	1 байт		2 байт	3 байт	4 байт
A	0	№ сети	№ узла		
B	10	№ сети		№ узла	
C	110	№ сети			№ узла
D	1110	Адрес группы Multicast			
E	11110	Зарезервирован			

Рисунок 8.6 – Классы адресов IP v.4

Классу **A** соответствует диапазон адресов 1.0.0.0 – 127.255.255.255.
Классу **B** соответствует диапазон адресов 128.0.0.0 – 191.255.255.255.
Классу **C** соответствует диапазон адресов 192.0.0.0 – 223.255.255.255.
Классу **D** соответствует диапазон адресов 224.0.0.0 – 239.255.255.255.
Классу **E** соответствует диапазон адресов 240.0.0.0 – 247.255.255.255.

Класс **A** используется для самых крупных сетей, насчитывающих до 16 677 216 узлов. Таких сетей не может быть больше 126.

В классе **B** максимально – 65 536 узлов, количество сетей – 2 142.

Класс **C** оперирует количеством адресов, не превышающим 254 узла. Это наиболее распространенный и эффективный класс адресов.

Требования к распределению адресного пространства излагаются в стандартах ripe-185, ripe-127, RFC 1918, RFC 1112. Исключительным случаем применения этих механизмов является использование бесклассовой адресации.

Бесклассовая адресация (Classless InterDomain Routing – CIDR) – метод IP-адресации, позволяющий гибко управлять пространством IP-адресов, не используя жёсткие рамки классовой адресации.[6] Способ основывается на переменной длине маски подсети (Variable Lenght Subnet Mask – VLSM) в то время, как в классовой адресации длина маски строго фиксирована 0, 1, 2 или 3 установленными байтами.

Вот пример записи IP-адреса с применением бесклассовой адресации: 10.1.2.33/27 (рисунок 8.7). В таком случае длина маски подсети 27 бит.

октеты IP-адреса	10	1	2	33
биты IP-адреса	00001010	00000001	00000010	00100001
биты маски подсети	11111111	11111111	11111111	11100000
октеты маски подсети	255	255	255	224

Рисунок 8.7 – Организация отдельной подсети для 32 узлов

Особые IP-адреса. Для технических нужд система адресации IP v.4 использует адреса, которые по синтаксису одинаковые для всех типов сети:

– если весь IP-адрес состоит из двоичных нулей – это адрес того узла, который сгенерировал этот пакет;

– если нулевым является только номер сети по умолчанию, то считается, что узел назначения принадлежит той же сети, что и узел, отправивший пакет;

– если адрес состоит из одних единиц, то это ограниченное широковещательное сообщение BroadCast. Пакет доставляется всем узлам, принадлежащим к той же сети, что и передатчик;

– если поле номера узла состоит из одних единиц, пакет доставляется всем узлам, находящимся в сети с заданным номером.

Помимо этих адресов существует набор специализированных (отладочных) адресов. Например: 127.0.0.0, 127.0.0.1 и др. Такие адреса принято называть Loopback. Данные не передаются по сети, а воспринимаются узлом-отправителем как только что принятые.

Локальные адреса. В соответствии со стандартом RFC 1918 несколько диапазонов адресов класса A, B и C были зарезервированы. В диапазон локальных адресов входит одна сеть класса A (10.0.0.0/8), 16 сетей класса B (172.16.0.0/16 – 172.31.0.0/16) и 256 сетей класса C (192.168.0.0/24 – 192.168.255.0/24). Таким образом, сетевые администраторы получили определенную степень свободы в плане предоставления внутренних адресов для локальных адресных пространств.

8.6 Система адресации IP v.6

Система адресации IP v.4 – прозрачная, но малоэффективная и практически исчерпала свои возможности. Для продолжения ее использования системному администратору необходим определенный базовый набор знаний и серьезный опыт работы. Но поскольку число IP-сетей быстро растет, подготовка квалифицированного персонала отстает, что создает проблемы с управляемостью.

Есть и другие недостатки адресации IP v.4. В частности, динамический уровень агрегирования адреса не позволяет снизить временные затраты на маршрутизацию пакетов на уровне оборудования.

Под агрегированием адреса понимается процедура выбора сети назначения пакета на основе анализа не всего адреса целиком, а лишь его фиксированной части (рисунок 8.9).

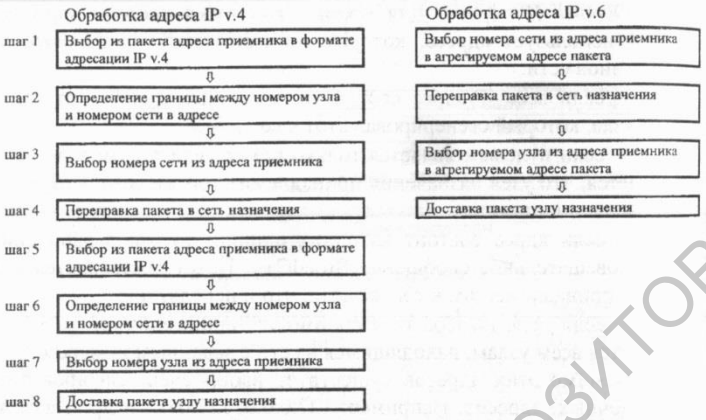


Рисунок 8.9 – Маршрутизация IP v.4 и с агрегированного адреса

Прогнозы аналитиков выявили угрозу дефицита IP-адресов формата IP v.4. Поэтому в середине 90-х годов начался процесс разработки новой версии IP-адресации – IP v.6 (RFC 1883).

Свойства адресации IP v.6:

- связь одного адреса с несколькими интерфейсами;
- автоматическое назначение адреса и CIDR-адресация.

Размер поля адреса в 128 разрядов описывает пространство для 340 289 366 920 938 463 463 374 607 431 762 211 456 узлов сети [1].

В IP v.6 определяется несколько типов адресов: AnyCast, UniCast, MultiCast. Они отличаются по префиксу формата (10, 110, 1110, …):

- UniCast – уникальный адрес (рисунок 8.10);
- MultiCast – групповой адрес;
- AnyCast (в некоторых источниках – Claster) – это тип адреса, при котором пакет доставляется ближайшему узлу из группы интерфейсов, имеющих этот адрес.

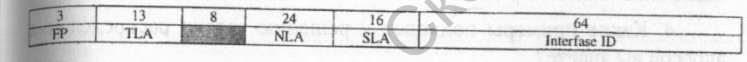


Рисунок 8.10 – Структура агрегированного уникального адреса IP v.6

Поле префикса формата FP назначено для определения типа адреса и для глобального агрегированного уникального адреса имеет значение 001.

TLA-префикс верхнего уровня предназначен для агрегирования верхнего уровня, который используют при назначении сети провайдеры самого верхнего уровня (.by, .com, .ru).

Поле 8 бит – предназначено в дальнейшем для расширения TLA, если 8196 сетей будет исчерпано.

NLA-префикс следующего уровня предназначен для размещения номеров сетей средних и мелких провайдеров. Значительный размер поля (24 бита) позволяет построить сложную структуру номеров сетей, т. е. использует технологию SIDR в пределах данного поля.

SLA-префикс местного уровня, предназначен для адресации подсетей отдельного компонента, например, подсетей корпоративной сети. Размер в 16 бит позволяет агрегировать адресное подпространство этого поля в своих пределах.

Идентификатор интерфейса Interface ID (64 бита) позволяет использовать в качестве адреса узла:

- MAC-адрес сетевого адаптера (48 бит);
- адрес X.25 (60 бит);
- адрес конечного узла ATM (48 бит);
- IP-адрес в системе IP v.4.

На момент издания пособия внедрение системы адресации IP v.6 поддержано на уровне операционных систем и является стандартом для международных организаций. В практике управления локальными сетями по-прежнему лидирующее место занимает адресация IP v.4.

Вопросы для самоконтроля

1 Зачем нужна адресация в компьютерных сетях?

2 Какие способы адресации вы знаете?

3 Какие требования к адресу сетевого интерфейса и схеме его назначения можно предъявить?

4 Какие примеры подходов к решению задачи распределения адресов вы знаете?

5 Что такое размер адресного пространства?

6 Каковы свойства системы адресации на уровне MAC?

7 Что такое адресный диапазон?

8 Каковы свойства системы адресации в сетях IPX?

9 Как осуществляется маршрутизация в сетях IPX?

10 Каковы свойства системы адресации в сетях Apple Talk?

11 Каковы свойства системы адресации в IP-сетях?

12 Что такое классы адресации?

13 Что такое бесклассовая адресация?

14 Какие бывают специальные адреса в IP-сетях?

15 В чем суть процесса «агрегирование адреса»?

16 Какие типы адресов применяются в системе адресации IP v.6?

17 Каковы перспективы применения и развития современных систем адресации?

18 Как влияет уровень подготовки персонала, обслуживающего сеть, на выбор системы адресации?

19 Как влияет выбор активного сетевого оборудования на систему адресации в сети?

20 Какие ошибки в сети возникают по причине нарушений требований системы адресации?

21 Как организовать широковещательную рассылку в различных системах адресации?

9 Управление компонентами сети

9.1 Одноранговые сети и сети на основе сервера

Различают два варианта организации управления компонентами сети – одноранговые сети и сети на основе сервера, что соответствует децентрализованной и централизованной системе управления.

Одноранговые или *пиринговые* сети (*peer-to-peer, P2P – равный с равным*) – это компьютерные сети, основанные на равноправии участников. В таких сетях отсутствуют выделенные серверы, а каждый узел (peer) является как клиентом, так и сервером.

В качестве клиента (потребителя ресурсов) каждая из машин может посылать запросы на предоставление каких-либо ресурсов другим машинам в пределах этой сети и получать их. Как сервер, каждая машина должна обрабатывать запросы от других машин в сети, отсылать то, что было запрошено, а также выполнять некоторые вспомогательные и административные функции.

Любой узел данной сети не дает гарантии своей постоянной работы в режиме on-line. Он может подключаться к сети и выходить из нее в любой момент времени, вынуждая подключенных клиентов искать узел, предлагающий аналогичный сетевой ресурс или сервис.

При достижении определённого критического размера сети наступает такой момент, когда в сети могут дублироваться функции и некоторые виды ресурсов, что приводит к путанице при определении исполнителя запроса.

Помимо чистых P2P-сетей, существуют так называемые гибридные сети, в которых существует по крайней мере один сервер, используемый для координации работы (в сетях Bittorrent, eDonkey) или для предоставления информации о существующих машинах сети, а также их статусе: on-line, off-line и т. д. (например, в сети ICQ).

Сейчас одноранговые сети условно разделяют на следующие два подмножества: *пиринговые файлообменные сети* и *пиринговые сети распределённых вычислений*.

Сети *клиент-сервер* (*Client/Server*) – это сетевая архитектура, в которой устройства являются либо клиентами, либо серверами на постоянной основе.

Клиентом (*front end*) является запрашивающая машина (обычно ПК), сервером (*back end*) – машина, которая отвечает на запрос. Оба термина (клиент и сервер) могут применяться как к физическим устройствам, так и к программному обеспечению.

Сети *с выделенным сервером* (*Client/Server network*) – сети, в которых сетевые устройства централизованы и управляются одним или несколькими серверами. Индивидуальные рабочие станции или клиенты должны обращаться к ресурсам сети через сервер (рисунок 9.1).

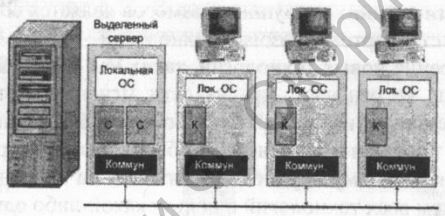


Рисунок 9.1 – Работа в сети с выделенным сервером

Этот принцип распространяется и на взаимодействие программ и информационных сред. Программа (среда), выполняющая предоставление соответствующего набора услуг – «сервер», а программа (среда), пользующаяся этими услугами – «клиент». Технология традиционной модели «клиент-сервер» модернизируется и совершенствуется.

Аналогично вариантам организации управления компонентами сети, так же можно разделить и сетевые модели:

- разбиение сети на рабочие группы;
- построение сети на базе доменной архитектуры;
- группировка сетевых устройств по другим признакам.

Сетевая модель обслуживания пользователей в первую очередь зависит от того, какая операционная система установлена на каждом из узлов сети, а также, какая операционная система управляет сетевыми потоками.

Примерами одноранговых сетевых операционных систем являются LANtastic, Personal Ware, Windows for Workgroups, Windows 9X.

Для централизованного управления многие компании выпускают две или более версии (комплектации) одной операционной системы. Полная версия предназначена для работы в качестве *серверной* операционной системы, а *облегченная* – для работы на клиентской машине. Эти версии часто основаны на одном и том же базовом коде ядра, но отличаются набором служб и утилит, а также параметрами конфигурации, в том числе устанавливаемыми по умолчанию и не поддающимися изменению. Например, Windows 2000 Professional или Vista (client) – Windows 2003 Server.

9.2 Гетерогенные сети

Построение крупной сети на основе одной сетевой платформы – это большая редкость. Обычным состоянием для любой вычислительной сети средних и крупных размеров является сосуществование различных стандартов и базовых технологий.

Внедрение новых технологий, таких как Fast Ethernet или Gigabit Ethernet, не означает, что из сети мгновенно вытесняются их предшественники, например, 10-Мегабитный Ethernet, Token Ring или FDDI, так как в эти технологии были сделаны огромные капиталовложения. Поэтому трудно рассчитывать на вытеснение в обозримом будущем всех технологий в пользу какой-либо одной.

Под *гетерогенностью* (неоднородностью) сети понимают несовместимость двух узлов, принадлежащих к одной сети, либо к смежным сегментам сети по одному или нескольким логическим признакам:

- формату кадра сети;
- способу шифрования;
- типу операционной системы;
- используемой модели безопасности и пр.

Гетерогенность является непременным атрибутом любой сложной и крупномасштабной сети, поскольку нельзя удовлетворить потребности тысяч пользователей с помощью однотипных программных и аппаратных средств. В такой сети обязательно будут использоваться различные типы компьютеров – от мэйнфреймов до персоналок, несколько типов операционных систем и множество различных приложений.

Например, при объединении в сеть нескольких архитектурных поколений и платформ вычислительной техники «букет» операционных систем в пределах одной сети может достигать 10–15 единиц.

Самым распространенным средством объединения разнородных транспортных технологий является использование единого сетевого протокола во всех узлах корпоративной сети. Единый сетевой протокол работает поверх протоколов базовых технологий и является тем общим стержнем, который их объединяет. Именно на основе общего сетевого протокола маршрутизаторы осуществляют передачу данных между сетями, даже в случае очень существенных различий между их базовыми сетевыми технологиями.

При нарушении условия единства протоколов для обмена информацией требуется применение посредника, чтобы организовать обмен на прикладном, представительском, сеансовом, транспортном, а иногда и сетевом уровне (согласно модели ISO) между участниками соединения (рисунок 6.1). В качестве такого посредника может использоваться специализированное устройство, выполняющее функции шлюза (рисунок 9.2).

Рисунок 9.2 – Сервер сети в роли посредника между разнородными клиентами

Взаимодействие разнородных сегментов в таких сетях осуществляется по схеме замещения запросов одной природы, поступающих от передатчика, в запросы другой природы, распознаваемых второй стороной сетевого обмена. В этом случае оба участника сетевого обмена не знают о гетерогенной природе второго абонента и обращаются с ним как с себе подобным.

При использовании шлюзов на базе современных сетевых операционных систем следует знать, что активация всех возможных видов и служб для этой цели нецелесообразна, т. к. это весьма ресурсоемко. Следует задействовать лишь те из них, которые необходимы. Тем более, что отключение «лишних» служб повышает уровень информационной безопасности сети.

Некоторая проблема появляется в гетерогенных сетях при распределении пользовательских прав доступа к сетевым ресурсам. Иногда невозможно связать в автоматическом режиме даже такие операционные системы компании Microsoft с ядром NT, как Windows 4.0 и Windows 2000.

Степень неоднородности сетевых технологий существенно возрастает при необходимости объединения локальных и глобальных сетей, имеющих, как правило, различные стеки протоколов.

9.3 Понятие рабочей группы

Рабочая группа (*workgroup*) – это способ реализации совместной работы нескольких связанных между собой общими информационными ресурсами компьютеров, объединенных для решения какой-либо общей задачи. Это исторически первый, основной и весьма эффективный способ управления сетевыми ресурсами в одноранговой сети. Каждому из компьютеров сети присваивается символьное имя, под которым он может быть зарегистрирован в любой рабочей группе сети. Имена компьютеров-участников в составе рабочей группы не могут повторяться.

Одно из важных свойств рабочей группы – *концентрация всего комплекта оборудования*, принадлежащего рабочей группе, на ограниченной территории. Выполнение данного условия улучшает качество обслуживания членов рабочей группы, каждый из которых может сам воспользоваться любым из устройств.

Но данное требование может не учитываться при реализации другого свойства рабочих групп – *оперативной настройки на задачу*. Рабочая группа может создаваться на короткий срок – для работы над конкретным проектом в пределах определенного промежутка времени.

Например, можно организовать рабочую группу «Презентация фирмы», которая состоит из компьютеров сотрудников фирмы, подготавливающих презентацию, или рабочую группу «Годовой отчет» – для подготовки годового финансового отчета фирмы. Все эти люди могут работать в разных отделах, но они составляют временную рабочую группу, чтобы было легко обмениваться информацией общего доступа при работе над одним проектом.

Следующее свойство рабочих групп – *независимость*. Каждая из рабочих групп самодостаточна для организации своей работы. Все службы прикладного уровня действуют только среди участников рабочей группы.

Например, при работе в Windows3.11 For Work Groups все компьютеры одной сети, независимо от их объединения в рабочие группы, имеют доступ к общим принтерам и общим файлам, а такие приложения как Mail (Электронная почта) и Shedule+ (Ежедневник), работают только в пределах одной рабочей группы.

Таким образом, обмен информацией между участниками разных рабочих групп может происходить только через общие информационные ресурсы.

Как правило, все пользователи рабочей группы могут иметь либо равный уровень доступа к ресурсам, либо он может регулироваться с помощью системы паролей. Предполагается максимум два вида доступа: «только для чтения» и «полный доступ». В Microsoft Windows такая модель использования сетевых ресурсов называется «распределение прав доступа на уровне ресурсов» (рисунок 9.3).

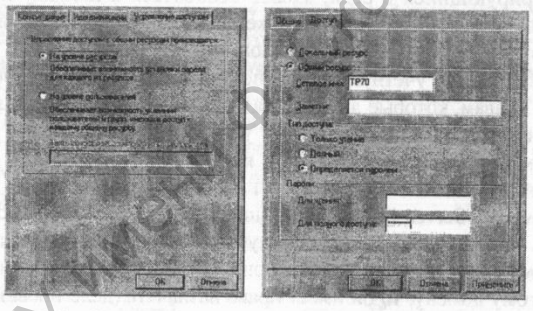


Рисунок 9.3 – Настройка модели доступа «на уровне ресурсов»

Для поддержки сетевого обмена операционная система каждого из членов рабочей группы обязана время от времени напоминать о себе и своих ресурсах другим участникам соединения. Собирая эти данные, каждая рабочая станция составляет карту сетевых ресурсов рабочей группы. Эту задачу удобно решать с применением широковещательных протоколов канального уровня.

Недостатком метода являются существенные задержки между моментом организации (инициализации) сетевого ресурса и моментом его появления в списках доступа конкретной рабочей станции. А если у машины нет сетевых ресурсов – ее вообще не видно в сети.

Характерные примеры операционных систем для работы в составе рабочей группы – Novell NetWare, OS/2 Lan Manager 2.0 Warp Connect, Windows 95, Windows 98 и Windows3.11 For Work Groups (в качестве расширения MS-DOS). Современные сетевые операционные системы также широко используют свойства рабочих групп.

Сети Novell NetWare также реализуют работу группы терминалов под управлением выделенного сервера. Данный метод является актуальным и на текущий момент. Он реализован в технологии обслуживания «тонких» клиентов.

9.4 Понятие домена

Если рабочая группа часто ориентирована на небольшое число компьютеров в пределах одной сети, то при разработке доменной архитектуры число компьютеров может быть больше, а также закладывается принцип централизованного управления: любой компьютер, регистрирующийся в сети, может относиться к любому из доменов вне зависимости от его расположения (территориально) или принадлежности к какому-либо из отделов.

На каждую учетную запись пользователя ведется отдельный учет по тем правам, которые для него назначены в домене. База данных SAM (Security Accounts Management – управление безопасными учетными записями) – это главная служба каталога для нескольких вариантов систем Microsoft Windows NT (например, Windows NT 3.5 и Windows NT Server 4) [9]. База данных SAM масштабируется намного лучше, чем предыдущая архитектура службы каталога из-за введения междоменных доверительных отношений. Если текущий домен доверяет другому домену, то он имеет право назначать (делегировать) любому пользователю или группе пользователей из этого домена права доступа к своим внутридоменным сетевым ресурсам. Управление осуществляется при помощи сервера. Сервер может нести несколько функциональных нагрузок – файл-сервер, принт-сервер, mail-сервер, сервер баз данных и прочие. Но для организации домена необходимо, чтобы он выполнял функцию «контролера домена».

В пределах домена все администраторы имеют полный контроль над серверами и службами, которые на них выполняются. По мере роста количества доменов в организации обеспечение уверенности относительно доверительных отношений, которые делают возможным пользовательскую идентификацию для доступа к ресурсам внешних доменов, приводит к росту накладных расходов. Чтобы справиться с этой растущей сложностью доменов и доверительных отношений, сетевые администраторы реализуют одну из четырех доменных моделей (рисунок 9.4): отдельный домен (single domain), домен с одним хозяином (master domain), домен с несколькими хозяевами (multiple master domain) и отношения полного доверия (complete trust).

При поддержке этих моделей самая большая сложность состоит в необходимости создания и сопровождения большого количества доверительных отношений. При этом все доверительные отношения между доменами Windows NT 4 должны создаваться с двух сторон, т. е. в обоих доменах.

База SAM является самым «узким» местом при такой системе управления сетевыми ресурсами, и все ее ограничения являются ограничениями системы администрирования в целом.

Во-первых, SAM одного домена имеет ограничение размера в 40 Мбайт. В результате количество объектов учетных записей (пользователи, их группы и узлы сети) не может превышать 40 000.

Второе ограничение на базу данных SAM состоит в возможностях доступа. Единственным методом доступа для взаимодействия с SAM является Windows NT Server. Этот метод ограничивает программируемый доступ и не обеспечивает конечным пользователям легкого доступа для поиска объектов.

В-третьих, функция контроллера домена, связанная с обновлением SAM, достаточно сложна и имеет собственную иерархию отношений.

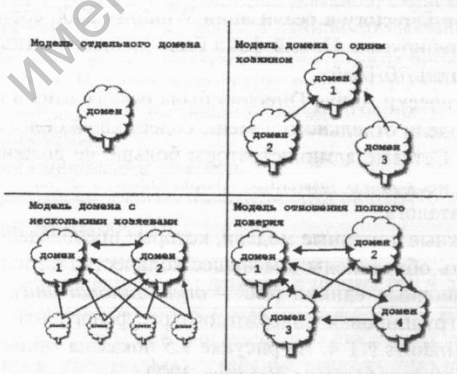


Рисунок 9.4 – Четыре доменные модели в Windows NT 4

Первичный контроллер домена (Primary Domain Controller – PDC) обладает в сети правами единственного автора изменений SAM, то есть регистрация любого сетевого объекта должна осуществляться на PDC. Для поддержки работоспособности сетевых сегментов, территориально удаленных от PDC, в сети устанавливают дополнительные или вторичные контроллеры домена (Secondary Domain Controller – SDC), которые обслуживают запросы пользователей на авторизацию в случае отсутствия отклика от PDC.

Для выполнения своих функций SDC хранит копию SAM, внесение изменений в которую запрещено, разрешена только синхронизация этой копии с основной базой SAM, хранящейся на PDC.

9.5 Модель доменов и Active Directory

Так как база данных SAM не подходит для поддержки сетевых приложений типа Exchange Server, то, когда была выпущена четвертая версия Exchange Server, она имела свою собственную службу каталога – Exchange Directory, которая была предназначена для поддержки вычислительной среды больших предприятий, в более поздних версиях она основывалась на открытых стандартах Internet. Например, она удовлетворяет спецификации облегченного протокола службы каталогов (LDAP) TCP/IP и имеет легкий программный доступ. [9]

Служба Active Directory заменила базу данных SAM в качестве службы каталога для сетевых сред от Microsoft. Она направлена на преодоление ограничений службы Windows NT 4 SAM и обеспечивает дополнительные выгоды сетевым администраторам. Главная выгода Active Directory в реализации Windows 2000 состоит в том, что она масштабируема. Новый файл базы данных учетных записей может достигать 70 Тбайт.

Фактически Active Directory была реализована в испытательной среде в модели отдельного домена, содержащей более ста миллионов объектов. Сетевые администраторы больше не должны делить свои среды на несколько доменов, чтобы обойти ограничения размеров службы каталога.

Сложные доменные модели, которые преобладали ранее, теперь могут быть объединены в меньшее количество доменов с помощью организационных единиц (*OU – organizational unit*), предназначенных для группировки содержимого ресурсного или регионального домена Windows NT 4. На рисунке 9.5 показана типичная модель отдельного домена системы Windows 2000.

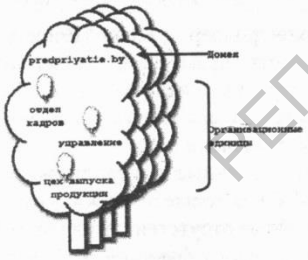


Рисунок 9.5 – Модель отдельного домена («лес») системы Windows 2000

Любые изменения в инфраструктуре Active Directory должны быть тщательно реализованы в соответствии с проектом Active Directory, который предусматривает такой рост.

В Active Directory изменен механизм реализации функции контроллера домена. Здесь нет деления на первичный и вторичный контроллеры домена, изменения могут вноситься на любом из серверов, а их синхронизация осуществляется в обоюдном направлении. Этот процесс часто занимает много времени.

Физическое проявление службы Active Directory состоит в наличии отдельного файла данных, расположенного на каждом контроллере домена в домене. Физическая реализация службы Active Directory описывается местоположением контроллеров домена, на которых расположена служба. При реализации службы Active Directory можно добавлять столько контроллеров доменов, сколько необходимо для поддержания служб каталога в данной организации. Имеется пять определенных ролей, которые может играть каждый из контроллеров домена. Все они выполняют роли FSMO (Flexible Single Master Operations – гибкие операции с одним хозяином):

- хозяин схемы;
- хозяин именования доменов;
- хозяин относительных идентификаторов RID;
- хозяин эмулятора PDC;
- хозяин инфраструктуры.

Одно из ограничений базы данных Windows NT 4 SAM состояло в том, что административные права были доступны только в виде «все или ничего». Чтобы дать пользователю любую степень административных прав, требовалось, чтобы вы сделали пользователя членом группы Domain Admins. Этот уровень административных прав давал пользователю безграничную власть в пределах домена, включая право удалять других пользователей из группы Domain Admins.

Active Directory предоставляет администраторам возможность *делегировать* административные права. Используя мастер Delegation Of Control Wizard (Делегирование управления) или устанавливая определенные разрешения на объекты Active Directory, администраторы могут предлагать тонко настроенные административные права. Например, можно назначить определенной учетной записи пользователя административное право сбрасывать пароли в домене, но не создавать, удалять или как-либо изменять пользовательский объект.

9.6 Разграничение прав доступа к сетевым ресурсам

В сетевых операционных системах при управлении сетевыми ресурсами должна быть реализована модель системы безопасности с разграничением прав доступа на разных уровнях. В том числе:

- полный доступ для всех пользователей на все виды действий;
- ограничения на уровне пользователей;
- ограничения на уровне узлов сети;
- ограничения на уровне анализа содержимого запросов;
- полный запрет для всех пользователей на все виды действий.

Управление доступом к сетевым ресурсам может быть реализовано:

- на уровне пользователей;
- на уровне ресурсов;
- на уровне физического доступа (локальный узел).

Если доступ к сетевым ресурсам регламентируется на уровне пользователей – это означает, что пользователь сможет получить доступ к объектам системы только после того, как он будет аутентифицирован и авторизован. В процессе аутентификации система удостоверяет личность пользователя (идентифицирует его) на основании факта знания пароля либо наличия биометрических характеристик, соответствующих его учетной записи. Авторизация подразумевает назначение пользователю прав доступа к объектам системы, на основании его членства в различных группах.

Примером реализации доступа на уровне пользователей является совместное использование файлов, т. е. предоставление файлов, находящихся на компьютере, в общий доступ так, что другие пользователи могут получить к ним доступ.

Если доступ к сетевым ресурсам регламентируется на уровне оборудования – это означает, что система аутентификации использует уникальные характеристики оборудования (например, MAC-адрес).

Если доступ к сетевым ресурсам регламентируется на уровне физического доступа – это означает, что подключение пользователей осуществляется на время организации сеанса сетевого обмена. Запрет физического доступа означает невозможность подключения к сети.

Примером организации такого доступа являются сети с коммутируемыми каналами связи. На практике в локальных сетях ограничение физического доступа применяется и как штрафная санкция, и как средство защиты от внешних воздействий.

Сетевые операционные системы могут оперировать одновременно несколькими сетевыми политиками и сложными видами прав доступа. Например, согласно сетевой политике Microsoft, виды прав доступа к файловой системе могут быть такие, как указано на рисунке 9.6.

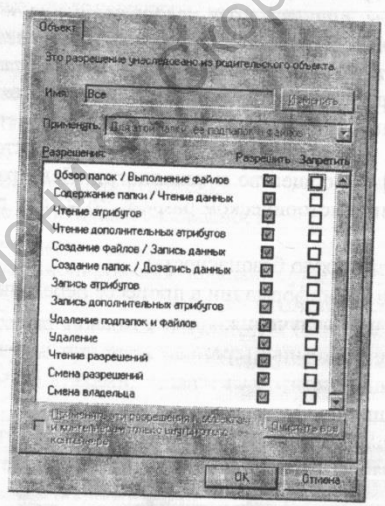


Рисунок 9.6 — Виды назначаемых прав в Windows 2000

В файловой системе NTFS у пользователя (владельца) есть возможность индивидуально назначать права доступа созданным папкам и файлам.

Пользователь, который состоит одновременно в нескольких группах, получает доступ ко всем видам ресурсов, разрешенных для каждой из групп пользователей. Но одновременно на него распространяются и запреты каждой из групп.

Успешная работа пользователя в таком случае зависит от того, насколько правильно разработана сетевая политика системным администратором и насколько корректно она применяется.

Для автоматизации управления сетевой политикой используются различные скриптовые конструкции. В этом случае на вход программного скрипта подается перечень объектов, к которым его необходимо применить.

9.7 Угрозы информационной безопасности в сетях

Защиту компьютерных сетей и систем принято связывать с информационной безопасностью.

Популярное определение информационной безопасности звучит так: *«…меры, принятые для предотвращения несанкционированного использования, злоупотребления, изменения сведений, фактов, данных или аппаратных средств либо отказа в доступе к ним…»*.

Информационная безопасность не является залогом безопасности компании, информации и компьютерных сетей и систем. Способы защиты информации и других ресурсов постоянно меняются, как меняется наше общество и технологии. Если рассматривать защиту информации в историческом разрезе, то можно выделить следующие ее виды:

- физическую безопасность;
- защиту информации в процессе передачи;
- защиту излучения;
- защиту компьютера;
- защиту сети;
- защиту информации.

В реальной жизни надежная защита – это объединение всех способов защиты (рисунок 9.7).

Рисунок 9.7 – Пример объединения некоторых аспектов безопасности

К сожалению, многие разработчики претендуют на то, что их продукт может справиться с этой задачей организации всеобъемлющего способа защиты данных для компьютеров и сетей. На самом деле это не так.

Для всесторонней защиты информационных ресурсов требуется комплекс различных средств защиты, таких как:

- антивирусное программное обеспечение;
- системы управления доступом;
- межсетевые экраны (firewall);
- смарт-карты;
- биометрия;
- системы обнаружения вторжения;
- управление политиками безопасности;
- шифрование и др.

Во время функционирования компьютерных сетей и систем часто возникают различные проблемы. Некоторые – по чьей-то оплошности, а некоторые являются результатом злоумышленных действий. В любом случае при этом наносится ущерб. Поэтому можно назвать такие события атаками, независимо от причин их возникновения. Существуют четыре основные категории атак:

- атаки доступа;
- атаки модификации;
- атаки на отказ в обслуживании;
- атаки на отказ от обязательств.

В свою очередь, каждая категория атак делится на множество различных видов. Все эти атаки связаны с различными хакерскими методами. К этим методам относятся:

- социальный инжиниринг;
- централизованные и распределенные DoS-атаки;
- прослушивание коммутируемых сетей;
- перенаправление трафика;
- имитация IP-адреса;
- вредоносные программы («Вирусы», «Троянские кони», «Черви»).

Без понимания угроз безопасности по отношению к информационным активам организации может быть использовано либо слишком много, либо слишком мало ресурсов, или они не будут использоваться должным образом.

9.8 Применение брандмауэров

Брандмауэр представляет собой барьер между двумя сетями – в большинстве случаев между внутренней сетью, часто называемой *защищенной* (trusted network), и внешней, *незащищенной* сетью (untrusted network), в данном случае Internet [9]. В брандмауэре входящие и исходящие пакеты проверяются на соответствие комплексу правил, определенных администратором, а затем в зависимости от результатов проверки они либо пересылаются по назначению, либо блокируются.

В большинстве современных брандмауэров используется один или более способов проверки пакетов, которых всего три.

Во многих маршрутизаторах применяется распространенный в брандмауэрах метод, называемый *фильтрацией пакетов*, который основан на анализе адресов источника и приемника, а также портов входящих пакетов TCP и UDP; решение о пересылке или блокировании сообщений принимается на основе набора заранее определенных правил. Фильтры пакетов довольно дешевы и прозрачны для пользователей, а их влияние на пропускную способность сети пренебрежимо мало. Однако, настройка конфигурации пакетных фильтров представляет собой относительно сложную процедуру. Еще одна проблема, связанная с фильтрами пакетов, это их уязвимость для *IP-спуфинга* (IP spoofing) – приема, применяемого хакерами для получения доступа к корпоративным сетям путем замены адресов IP (Internet Protocol) в заголовках пакетов на допустимые.

Более совершенный и надежный тип брандмауэра – *шлюз прикладного уровня*. В большинстве таких систем, в том числе в популярном семействе продуктов Eagle фирмы Raptor и изделии Gauntlet компании Trusted Information Systems, используются программы-посредники (proxies) прикладного уровня, называемые агентами. Эти программы, составленные для конкретных служб Internet, таких, как HTTP, FTP и TELNET, работают на сервере с двумя сетевыми соединениями и выполняют роль сервера для клиента и роль клиента для сервера приложений.

Поскольку программы-посредники прикладного уровня служат для проверки сетевых пакетов на наличие достоверных данных, специфических для конкретной программы, они считаются в целом более надежным средством защиты, нежели фильтры пакетов.

В большинстве брандмауэров – шлюзов прикладного уровня – имеется функция, получившая название трансляции сетевых адресов (network address translation), которая скрывает внутренние IP-адреса от пользователей, находящихся за пределами защищенной сети.

Один из основных недостатков шлюзов прикладного уровня – снижение уровня производительности из-за повторной обработки в программе-посреднике. Второй недостаток заключается в том, что, возможно, придется в течение нескольких месяцев ждать от поставщика брандмауэра выпуска программы-посредника прикладного уровня для новой службы Internet, такой, как RealAudio. Но, как правило, возможности внешнего канала связи будут исчерпаны прежде, чем ресурсы брандмауэра.

При использовании программ-посредников прикладного уровня внутри учреждения следует обратить внимание на быстродействующие аппаратные решения, например, PIX Firewall фирмы Cisco или Seattle Software компании Firebox. В качестве альтернативы можно рассмотреть возможность инсталляции программы-брандмауэра на многопроцессорной системе.

Третий тип технологии брандмауэров, названный компанией Check Point Software Technologies *комбинированным* (stateful inspection), реализован в пакетах Firewall-1 компании Check Point, PIX Firewall фирмы Cisco, ON Guard фирмы ON Technology и Firewall/Plus фирмы Network-1. Как и при использовании метода фильтрации пакетов, сначала происходит перехват пакетов на сетевом уровне, однако затем пакеты анализируются целиком, их содержимое сравнивается с известными последовательностями битов (состояниями) проверенных пакетов. Комбинированный метод, как правило, имеет немного более высокую производительность, чем у программ-посредников прикладного уровня, однако вопрос о том, обеспечивает ли он такую же степень безопасности или чуть менее надежен, остается открытым.

Крупные поставщики брандмауэров применяют в своих продуктах дополнительные методы защиты информации и заключают партнерские соглашения с другими поставщиками средств защиты, с тем чтобы предложить потребителям исчерпывающее решение проблемы безопасности в Internet. Большинство таких функциональных средств обсуждается ниже. Среди них шифрование данных, аутентификация, защита от вирусов и плохо отлаженных апплетов Java и ActiveX, загружаемых из сети, и даже равномерное распределение нагрузки между серверами.

9.9 Применение командного режима

Консоль командной строки присутствует во всех версиях операционных систем Windows и во многих других современных операционных системах, в том числе операционных системах специализированного сетевого оборудования. Ранние версии ОС поддерживали режим MS-DOS напрямую, что позволяло выполнять простые команды прямо из консоли. Представители же семейства NT, такие как Windows 2000 или Windows Server 2003, работают уже совсем по другим принципам, однако командный режим в них тоже поддерживается. В качестве интерпретатора командного режима выступает программа cmd.exe, запуск которой осуществляется через меню «Start -> Run». Кроме того, для запуска консоли можно воспользоваться элементом меню «Start -> All Programs -> Accessories -> Command Prompt». Альтернативные платформы операционных систем (например, Linux) ориентированы и оптимизированы на работу в командном режиме. Примеры данного интерфейса представлены на рисунке 9.8.

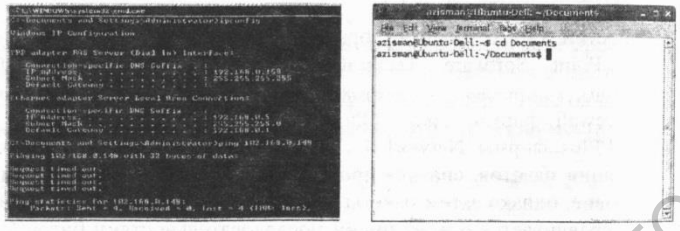


Рисунок 9.8 – Окно терминала в Windows и Linux

Запустив консоль командного режима, пользователь с правами администратора может управлять ресурсами как локальной системы, так и ресурсами удаленной машины. Существуют команды, выполняющие мониторинг системы и выявляющие критические места в настройках сервера. Отличием работы из командной строки является полное отсутствие больших и громоздких графических утилит. Программы командной строки позволяют более тонкую настройку в виде параметров-ключей, указанных справа от самой команды.

С помощью специальных файлов-скриптов (наборов команд, выполняющихся последовательно или в запрограммированном порядке) администратор может свести к минимуму выполнение рутинных ежедневных операций.

Для управления удаленными устройствами с помощью командного режима чаще всего используется протокол TELNET. Для пользователей Windows привычнее работать в среде Microsoft Hyper Terminal (рисунок 9.9).

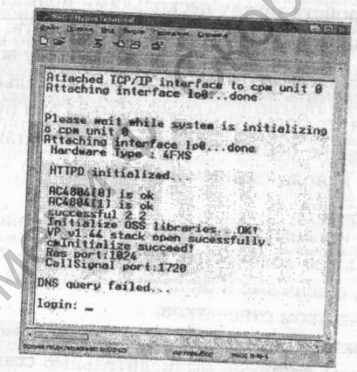


Рисунок 9.9 – Окно программы HyperTerminal

Сам администратор может выполнять как одиночные команды, так и список команд, используя специальные управляющие символы (&, |).

Например:

Команда 1 & Команда 2 – выполняется Команда 1, затем Команда 2;

Команда 1 && Команда 2 – только после успеха Команды 1 – Команда 2.

Существует возможность перенаправить выводимый программой поток напрямую в текстовый файл для дальнейшей обработки. Для этого необходимо использовать управляющий символ «>» и имя текстового файла.

Администратор может запустить несколько копий консоли, вызвав в командной строке программу cmd.exe. Использование вложенной консоли позволяет работать с переменными окружения операционной системы без каких-либо последствий для всей системы в целом, так как после закрытия вложенной консоли изменения переменных окружения не сохраняются.

9.10 Организация сетевой печати

Сетевая печать – это частный случай распределенной печати. Организация распределенной печати, т. е. распределение ресурсов печатающих устройств между несколькими пользователями является наиболее популярным сервисом в локальной сети. Основной причиной этого можно считать следующую постановку вопроса:

– если обеспечить всех клиентов сети локальными печатающими устройствами, то большую часть времени они будут простаивать;

– обслуживание большого количества печатающих устройств и контроль за их использованием по назначению – дорогостоящая и очень сложная задача;

– скорость и качество печати на этих устройствах будут низкими, так как большое количество дорогостоящих устройств приобретаться не будет, а дешевые и бюджетные решения обладают низкими скоростью и качеством отпечатков.

Таким образом, для любой организации, применяющей в своем производственном процессе вычислительные сети, будет выгодным приобрести оптимальное количество качественных печатающих устройств и организовать обслуживание пользователей.

Разделенную печать можно реализовать следующими способами:

– *применением несетевых специализированных промежуточных устройств подключения к принтеру* (Switcher – переключатель). Такие устройства являются наиболее дешевым и простым с точки зрения пользователя решением данной проблемы. Компьютеры пользователей подключаются к Switcher-у с помощью стандартных портов: COM, LPT, USB (рисунок 9.10).

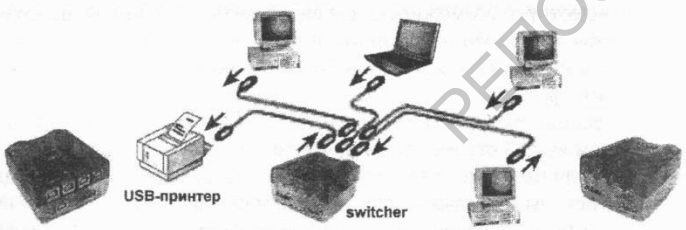


Рисунок 9.10 – Схема подключения к принтеру через Switcher

Switcher является «прозрачным» для запросов пользователя и, таким образом, принтер как бы локально подключен к компьютеру. Очередность доступа к принтеру передается последовательно между всеми портами Switcher-а. Если одно из устройств начало печатать, для остальных принтер переходит в состояние «занят». Очередь печати управляется операционной системой клиента;

– *использованием аппаратных принт-серверных средств* (принтер подключается к сети непосредственно или через специализированное устройство). Если в предыдущем случае уровень физического доступа к печати был ограничен числом портов Switcher-а, то здесь все клиенты сети физически подключены к печатающему устройству потому что оно, в свою очередь, подключено к сети (рисунок 9.11). Ограничение доступа к таким устройствам осуществляется назначением прав сетевой политики;

а) б)

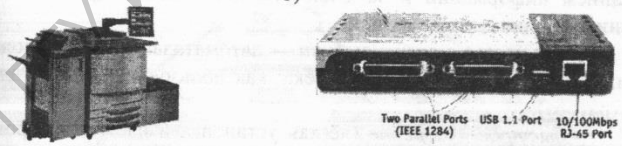


Рисунок 9.11 – Примеры аппаратных «print-server» устройств:
а) специализированный комплекс Konica Minolta Bizhub PRO C5500;
б) устройство сетевого расширения D-Link с 2 LPT и 1 USB выходами

– *с помощью программно-эмулируемых принт-серверных устройств*. Самый медленный способ организации сетевой печати. В этом случае часть производительной мощности сервера выделяется на обслуживание заданий печати. Очередь на печать строится в пределах операционной системы сервера. Управление заданиями печати возлагается на сервер и его администратора, но часть прав по управлению этой очередью можно передать и клиентам сети.

Права доступа к принтеру определяются двумя способами:

– авторизовано (на уровне пользователей);

– на уровне ресурсов (общий пароль доступа).

Управление правами доступа, как правило, осуществляется с помощью специализированного ПО, поставляемого вместе с аппаратным принт-сервером, либо посредством протокола удаленного управления (например, TELNET).

9.11 Резервное копирование данных

Резервное копирование (англ. *backup*) – процесс создания копии данных на носителе (жёстком диске, дискете и т. д.), предназначенном для восстановления данных в оригинальном месте их расположения в случае их повреждения или разрушения.

Резервное копирование необходимо для возможности быстрого и недорогого восстановления информации (документов, программ, настроек и т. д.) в случае утери рабочей копии информации по какой-либо причине.

Кроме этого решаются смежные проблемы:

- дублирование данных;
- передача данных и работа с общими документами.

Требования к системе резервного копирования:

- *надёжность* хранения информации. Обеспечивается дублированием информации и заменой утерянной копии другой в случае уничтожения одной из копий;
- *простота в эксплуатации* — автоматизация (по возможности минимизировать участие человека: как пользователя, так и администратора);
- *быстрое внедрение* (лёгкая установка и настройка программ, создание скриптов, краткое обучение пользователей).

Виды резервного копирования:

- полное резервирование (*Full Backup);*
- дифференциальное резервирование *(Differential Backup)*;
- добавочное резервирование *(Incremental Backup);*
- пофайловый метод.

Для резервного копирования очень важным вопросом является выбор подходящей схемы ротации носителей (например, магнитных лент, DVD дисков). Наиболее часто используют следующие схемы:

- одноразовое копирование;
- простая ротация;
- «дед, отец, сын»;
- «ханойская башня»;
- «10 наборов».

Схемы «ханойская башня» и «10 наборов» используются нечасто, так как многие системы резервирования их не поддерживают.

Хранение резервной копии можно осуществлять при использовании различных технологий:

– лента стримера – запись данных на магнитную ленту;
– DVD или CD – запись резервных данных на компактные диски;
– HDD – запись резервных данных на жёсткий диск компьютера;
– LAN – запись резервных данных на любую машину локальной сети;
– FTP – запись резервных данных на FTP-серверы;
– USB – запись резервных данных на любое USB-совместимое устройство (такое, как флэш-карта или внешний жёсткий диск);
– ZIP, JAZ, MO – копирование данных на дискеты ZIP, JAZ, MO.

В некоторых случаях для увеличения вероятности сохранности данных комбинируются локальные и глобальные технологии передачи данных. Тогда схема общей системы резервного копирования данных может стать такой же сложной, как показано на рисунке 9.12.

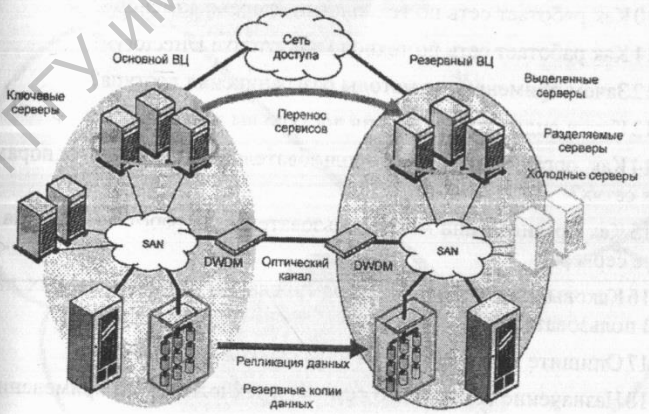


Рисунок 9.12 – Пример схемы резервного копирования

Самыми важными свойствами резервных копий являются: их наличие и защита от несанкционированного доступа. В случае потери основной копии данных – резервная дает возможность минимизировать финансовые убытки, которые вызовет остановка производственного цикла, либо полномерная ревизия текущей обстановки. Наличие механизмов защиты в резервных копиях снижает вероятность убытков от промышленного шпионажа.

Вопросы для самоконтроля

1 Как производится управление компонентами сети?

2 Какие виды компонентов сети вы знаете?

3 Как организовано управление в одноранговых сетях?

4 Какие виды «пиринговых» сетей вы знаете?

5 Как организовано управление в сетях на основе сервера?

6 Как работают сетевые операционные системы в сетях с различными системами управления?

7 Как объясняется термин – гетерогенность сети?

8 Как организовать управление в гетерогенных сетях?

9 Как работает сеть по технологии «рабочая группа»?

10 Как работает сеть по технологии «дерево доменов»?

11 Как работает сеть по технологии «Active Directory»?

12 Зачем применяются методы разграничения доступа?

13 Какие виды разграничения доступа вы знаете?

14 Как организована многопользовательская работа в одноранговых сетях?

15 Как организована многопользовательская работа в сетях на основе сервера?

16 Каковы требования при формировании индивидуальных паролей пользователей?

17 Опишите назначение и методы работы брандмауэров.

18 Назначение командного режима и технология его применения.

19 Каковы методы организации сетевой печати?

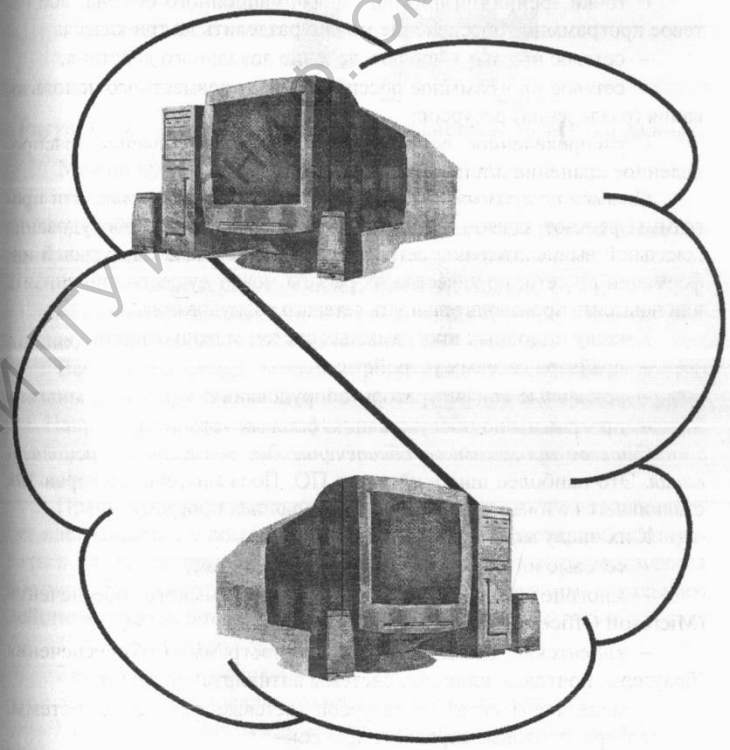
20 Какие средства защиты информации вы знаете?

21 Какие четыре основные категории атак вы знаете?

22 Назначение резервного копирования данных.

23 Оборудование и технологии организации резервного копирования данных.

10 Сетевые вычислительные среды



10.1 Классификация сетевого программного обеспечения

К понятию сетевого программного обеспечения следует относить все виды исполняемых программных кодов, служебных библиотек, наборов баз данных и приложений, используемых для управления, настройки сетевого оборудования, эмуляции виртуальных сетевых устройств, серверов и т. д.

С точки зрения организации информационного обмена, все сетевое программное обеспечение можно разделить на три класса:

– сетевое программное обеспечение локального действия;

– сетевое программное обеспечение для совместного использования (разделения) ресурсов;

– распределенное сетевое программное обеспечение (распределенное хранение и/или обработка данных).

Сетевое программное обеспечение локального действия. Эти программы решают задачи в пределах узла или активного оборудования локальной вычислительной сети. Их работа не связана с передачей информации по сети, но качество их работы может существенно снизить или повысить производительность сетевого оборудования.

К числу подобных программных систем можно отнести:

– драйвера сетевых устройств;

– локальные конфигураторы оборудования;

– программы по обслуживанию сетевых устройств.

Сетевое программное обеспечение для совместного использования. Это наиболее широкий класс ПО. Пользователь, как правило, сталкивается с ними и работает в среде данных программ.

К их числу можно отнести:

– сетевые интерфейсы операционных систем;

– многопользовательские версии программного обеспечения (Microsoft Office, базы данных SQL);

– клиентские оболочки сетевого программного обеспечения (браузеры, почтовые клиенты, системы антивирусной защиты);

– менеджеры сетевых ресурсов (сетевые файловые системы, web-сервера, почтовые сервера и прочее);

– протоколы сетевого обмена и т. д.

Распределенное сетевое программное обеспечение. Данный вид программного обеспечения подразумевает распределенную обработку и/или хранение информации (рисунок 10.1).

В общем случае для распределенной системы географическое положение сервера относительно клиентов не имеет значения.

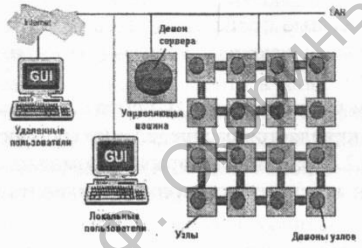


Рисунок 10.1 – Пример распределенной системы обработки данных

Можно привести такие примеры:

– чат-сервера (ICQ, MAIL.RU);

– игровые сервера (спортивные симуляторы, виртуальные казино, виртуальные пространства боевых состязаний и пр.);

– поисковые сервера (Yandex, Rambler, Google, TYT);

– системы распределенного вычисления (распределенный рендеринг, расчет графической или научной информации).

Все эти три класса сетевого программного обеспечения жестко связаны друг с другом, либо используют друг друга в процессе работы. Например, локальные конфигураторы могут получать параметры для изменения режима работы устройств методом взаимодействия с сетевыми протоколами.

Права пользовательского доступа в каждом из этих классов могут настраиваться с помощью индивидуальных средств, либо базироваться на общесистемных алгоритмах авторизации и разграничения доступа. Т. е. системы авторизации доступа программ локального действия могут работать по следующему алгоритму:

1) локальный ввод данных;

2) удаленная проверка;

3) разрешение локального и/или удаленного допуска.

По вышеупомянутым и некоторым другим причинам любую из анализируемых программ бывает довольно трудно однозначно отнести к тому или иному классу. Взаимодействие с локально установленным программным обеспечением, как правило, еще больше усложняет картину, а иногда и вообще делает бессмысленным сетевое взаимодействие.

10.2 Организации вычислительного процесса в сетевой структуре

Вычислительные процессы в сетевых структурах можно разделить на три класса: *централизованные, децентрализованные* и *распределенные*.

Основным различием между централизованной и децентрализованной моделью является распределение функций между сторонами. На рисунке 10.2 отражены некоторые возможные варианты архитектур программных систем с «тонкими клиентами» разного уровня «толщины».

Рисунок 10.2 – Четыре уровня толщины «тонкого клиента»

Многоуровневая web-архитектура, тонкий клиент и ультратонкий клиент являются примерами централизованной модели обслуживания.

Ультратонкий клиент (терминал) может только отображать растровое изображение и передавать на сервер информацию с устройств ввода. Оконная система реализуется за счет ресурсов сервера, к которому подключаются терминалы. Такая архитектура обеспечивает высокую нагрузку на процессор сервера, что ограничивает число одновременно обслуживаемых клиентов. Для снижения нагрузки на сервер запросы от терминалов группируются и обрабатываются параллельно.

Тонкие клиенты – устройства, способные поддерживать оконную систему (например, X-Window). В этом случае объем передаваемой клиенту информации значительно снижается по сравнению с предыдущей архитектурой.

На следующем уровне располагаются Java-станции, сочетающие интерфейс на основе Интернет-навигатора с возможностью загрузки и выполнения Java-аплетов и самостоятельных Java-приложений. Здесь к функциям ввода/вывода добавляются возможности загрузки программ по сети и их локального (на клиенте) выполнения.

Перераспределение функций клиента в любом из рассмотренных вариантов архитектур увеличивает сетевой трафик и нагрузку на ресурсы сервера. Решение этой проблемы было найдено в применении для типовых сетевых сервисов специализированных устройств и приближение этих устройств к клиентам.

Современное сетевое оборудование рассчитано на выполнение функций обработки программных систем (рисунок 10.2).

Рисунок 10.3 – Четыре уровня перераспределения серверных функций

Число функций прикладных программ, переносимых на передающее оборудование в большей мере зависит от совместимости встроенных операционных систем выбранных устройств с операционной системой сервера.

В заключение можно сказать, что выбор сетевой операционной системы – это поиск компромисса. Пользователь ищет наиболее подходящую для работы среду. Администрация предприятия ищет способ снижения стоимости владения сети. Персонал, обслуживающий сеть, ищет программную платформу, позволяющую максимально эффективно реализовать управление вычислительным процессом, а также обеспечить достаточные уровни информационной безопасности и производительности.

10.3 Серверные операционные системы

Назначение серверной операционной системы следующее: под управлением этих операционных систем выполняются приложения, обслуживающие всех пользователей корпоративной сети, а нередко и внешних пользователей. К таким приложениям относятся современные системы управления базами данных, средства управления сетями и анализа событий в сети, службы каталогов, средства обмена сообщениями и групповой работы, Web-серверы, почтовые серверы, корпоративные брандмауэры, серверы приложений разнообразного назначения. Требования к производительности и надежности указанных операционных систем намного выше, нежели в случае клиентских операционных систем. В последнее время от серверных операционных систем порой требуются такие средства обеспечения надежности и доступности, как поддержка кластеров (набора ряда однотипных компьютеров, выполняющих одну и ту же задачу и делящих между собой нагрузку), возможности дублирования и резервирования, переконфигурации программного и аппаратного обеспечения без перезагрузки операционной системы.

Иными словами, выбор серверной операционной системы и аппаратной платформы для нее в первую очередь определяется тем, какие приложения под ее управлением должны выполняться и каковы требования к ее производительности, надежности и доступности. Такие факторы, как удобный пользовательский интерфейс, возможность выполнения клиентских приложений и иные «пользовательские» потребности, хотя и присутствуют в современных версиях многих подобных операционных систем, но в данном случае не играют решающей роли – нередко управление сервером может осуществляться удаленно с клиентского компьютера.

Серверные версии Windows (Microsoft). Статистически Windows установлена на более чем 90 % персональных компьютеров, но в случае серверов картина выглядит намного более разнообразной и доминирования какого-то одного производителя на рынке серверных операционных систем пока не наблюдается. Тем не менее серверные версии Windows сейчас применяются довольно широко. Windows NT, первая полностью 32-разрядная операционная система этого семейства, появилась вскоре после выпуска Windows 95 и ознаменовала собой первый шаг на пути завоевания компанией Microsoft части рынка серверных операционных систем. В настоящее время происходит дальнейшее развитие линейки MS Windows NT: Windows NT Server 4.0, Windows Server

2000, Windows 2000 Datacenter Server, Windows 2000 Advanced Server, Windows Server 2003, Windows Server 2008.

Операционная система UNIX относится к «долгожителям» рынка серверных операционных систем – она была создана в конце 60-х годов в Bell Laboratories фирмы AT&T. Отличительной особенностью этой ОС, обусловившей ее «живучесть» и популярность, было то, что ядро операционной системы, написанной на ассемблере, было невелико, тогда как вся оставшаяся часть операционной системы была написана на С – языке высокого уровня, созданном сотрудником Bell Laboratories Деннисом Ритчи специально для этой цели. Такой подход к созданию операционных систем, с одной стороны, позволял легко добавлять к ОС новые возможности и адаптировать ее в соответствии с теми или иными потребностями (в частности, именно для этой операционной системы появилась реализация протокола TCP/IP, лежащего в основе Интернета), а с другой — делал легко переносимыми и собственно операционную систему, и созданные для нее приложения на самые разнообразные аппаратные платформы. Благодаря бесплатному предоставлению данного продукта университетам вместе с исходными текстами, а также наличию большого количества компиляторов С, популярность этой операционной системы в 70-80-х годах еще более возросла. Даже Microsoft в начале 80-х производила совместно с компанией Santa Crus Operations версию UNIX, носившую название Xenix и бывшую в течение какого-то времени весьма популярной на рынке UNIX-систем. Еще одним достоинством UNIX является ее открытость, то есть публичная доступность спецификаций интерфейсов, протоколов и алгоритмов работы операционной системы. Открытость UNIX позволила одновременно существовать как коммерческим версиям UNIX, производимым компаниями Sun Microsystems, IBM, Hewlett-Packard и др., так и некоммерческим версиям, вроде FreeBSD и Linux.

NetWare (Novell) – в начале и середине 90-х годов Novell NetWare была доминирующей сетевой операционной системой и пользовалась заслуженной популярностью благодаря своей надежности. В то время для нее создавались СУБД, серверы приложений, средства групповой работы, Web- и почтовые серверы. В настоящее время доля серверов, управляемых NetWare, заметно снизилась.

Наряду с вышеперечисленными серверными ОС существует и ряд других специализированных ОС, не получивших широкого распространения.

10.4 Операционные системы сетевых клиентов

На текущий момент актуальным является утверждение, что *«любая версия операционной системы на стороне клиента должна обеспечить работоспособность при взаимодействии с любой серверной платформой»*. Выбор операционной системы пользователем может быть обусловлен *изначальным* решением решать свои задачи в конкретной программной среде. Современная тенденция в разработке операционных систем состоит в перенесении значительной части системного кода на уровень пользователя и одновременной минимизации ядра (рисунок 10.5). Дополнительно, при разработке современной операционной системы следует учитывать принцип организации взаимодействия с оператором (интерфейс), поэтому многие образцы современных операционных систем имеют признаки внешнего подобия, а также общность структуры.

Рисунок 10.5 – Модель клиент-сервер в микроядерной архитектуре

Схема на рисунке соответствует принципу работы операционной системы Windows. Программные продукты для этой системы наиболее распространены, что обуславливает ее популярность в современных сетях. Большинство альтернативных Windows операционных систем для увеличения конкурентоспособности предлагают не только интерфейс, но и широкий спектр предустановленного полнофункционального программного обеспечения.

Linux. Прототипом для первого ядра Linux была совместимая с UNIX операционная система MINIX. Это требовало поддержки стандарта POSIX. POSIX – это функциональная модель, в которой описано, как должна вести себя система в той или иной ситуации, но не приводится никаких указаний, как это следует реализовать программными средствами. Поэтому проект Linux развивается одновременно в нескольких версиях ядра: Red Hat Linux, Mandrake Linux, SuSE Linux, Debian GNU/Linux, ASPLinux, ALT Linux, Slackware Linux и пр.

BeOS (компания Be Inc.). Поначалу BeOS не была отдельным продуктом, она поставлялась с компьютером BeBox. BeBox был ориентирован на домашний сектор и мультимедийные приложения. Основные требования, предъявляемые к системе были таковы: поддержка нескольких процессоров; файловая система, подходящая для работы с большими мультимедийными файлами; стабильность; удобство и доступность для рядовых пользователей. 64-битная файловая система, примененная уже в конце 90-х снимает ограничения по размеру обрабатываемых файлов.

На текущий момент BeOS считается мультиплатформенной системой. Реализована поддержка процессоров и чипсетов различных производителей. При этом в состав установочного пакета их включать не обязательно. Система сохраняет ограниченный функционал и позволяет подключиться к сети для поиска необходимых библиотек.

Недостатком системы является ограниченный рынок дополнительных программ и, в первую очередь, офисных приложений.

FreeBSD – UNIX-подобная операционная система, работающая на платформах Intel x86 и Alpha. FreeBSD представляет собой прекрасную основу для создания Internet или Intranet сервера. Качество FreeBSD превосходно комбинируется с дешевыми аппаратными средствами, что делает FreeBSD отличной альтернативой коммерческим рабочим станциям под управлением UNIX или Microsoft. Приложения подходят для использования как на настольной системе, так и в высокопроизводительных серверах. FreeBSD распространяется бесплатно и поставляется вместе с исходными текстами.

QNX (компания QNX Software System Ltd.) – POSIX-совместимая операционная система реального времени, предназначенная преимущественно для встраиваемых систем. Как микроядерная операционная система, QNX основана на идее работы основной части своих компонентов, как небольших задач, называемых сервисами. QNX Neutrino, выпущенная в 2001 году, перенесена на многие платформы, и сейчас способна работать практически на любом современном процессоре, используемом на рынке встраиваемых систем. Среди этих платформ присутствуют семейства x86, MIPS, PowerPC, а также специализированные семейства процессоров: SH-4, ARM, StrongARM и xScale.

Помимо упомянутых операционных систем, которые в большей или меньшей степени ориентированы на архитектуру IBM-совместимых вычислительных систем, существуют и другие. Самая известная из них – MacOS.

10.5 Операционные оболочки тонких клиентов

Конфигурации оборудования современных тонких клиентов предоставляют пользователю хорошую вычислительную мощность. К примеру, тонкий клиент Jack-PC Chip (рисунок 10.6) обладает ресурсами на уровне офисного компьютера в очень компактном исполнении. Применение твердотельных накопителей даже дает возможность выбора операционной оболочки для подключения к различным терминальным серверам.

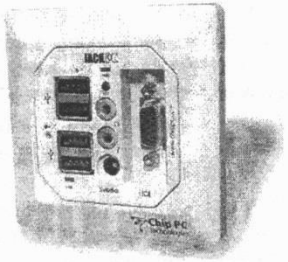


Рисунок 10.6 – Тонкий клиент Jack-PC Chip PC Technologies

Для подключения тонкого клиента к удаленному серверу он должен удовлетворять двум условиям: поддержке протокола связи между клиентом и сервером и поддержке функционального уровня взаимодействия (интерфейс, объекты, схемы сжатия) между клиентом и сервером.

Перечислим протоколы, используемые тонкими клиентами:

- X11 – используется в Unix;
- Telnet – мультиплатформенный;
- SSH – мультиплатформенный защищённый аналог Telnet;
- NX technology – протокол X11 со сжатием данных;
- Virtual Network Computing;
- Citrix ICA;
- Remote Desktop Protocol (RDP), протокол для удалённой работы с использованием графического интерфейса пользователя для Windows.

Поскольку «тонкий клиент» в большинстве случаев обладает минимальной аппаратной конфигурацией, иногда – без жесткого диска, то в некоторых конфигурациях системы тонкий клиент загружает операционную систему по сети с сервера, используя протоколы PXE, BOOTP, DHCP, TFTP и Remote Installation Services (RIS).

Среди операционных оболочек «тонких клиентов» выделяются следующие:

Thinstation – дистрибутив GNU/Linux, разработанный специально для создания тонких клиентов. Может быть загружен с CD, по сети, с USB или IDE flash. Имеет модульную структуру. Не использует менеджера пакетов. Размер бинарного файла – около 8 Mb, что позволяет использовать для загрузки компьютеры с 8 – 16 Mb оперативной памяти.

LTSP (англ. Linux Terminal Server Project) – пакет дополнений для GNU/Linux, позволяющий подключить большое количество низкопроизводительных тонких клиентов к Linux-серверу. LTSP доступен как набор пакетов для установки на Linux-системе. Также он доступен как часть уже готового дистрибутива, например Edubuntu и Debian .

Windows Embedded. Этим термином обозначается семейство встраиваемых операционных систем для интеллектуальных, легко подключаемых, компактных устройств. В семейство Windows Embedded входит серия продуктов, основанных на платформах Windows CE и Windows XP Embedded.

Windows CE – это вариант операционной системы Microsoft Windows для наладонных компьютеров, мобильных телефонов и встраиваемых систем. Windows CE не является «урезанной» версией Windows для стационарных систем и основана на совершенно другом ядре. Поддерживаются архитектуры x86, MIPS, ARM и процессоры Hitachi SuperH.

Windows CE оптимизирована для устройств, имеющих минимальный объём памяти – для ядра достаточно 32 Кб. С графическим интерфейсом (GWES) понадобится от 5 Мб. Устройства часто не имеют дисковой памяти и могут быть сконструированы как «закрытые» устройства, без возможности расширения пользователем.

На базе Windows CE основано множество платформ, включая Handheld PC, Pocket PC, Pocket PC 2002, Pocket PC 2003, Pocket PC 2003 SE, Smartphone 2002, Smartphone 2003, Windows Mobile, а также множество промышленных устройств и встроенных систем.

Система Windows XP Embedded реализует возможности Microsoft Windows XP в компонентной форме и обеспечивает быстрое создание встраиваемых устройств на базе процессора x86 и аппаратной архитектуры ПК. Примерами устройств Windows XP Embedded служат кассовые терминалы розничной торговли, банкоматы, некоторые модели телеприставок и, наконец, тонкие клиенты. В отличие от тонких клиентов под управлением Windows CE пользователь не заметит серьёзных отличий от обычной «десктопной» Windows XP.

10.6 Операционные оболочки WEB-OS

Идея разработки этих программных систем возникла достаточно давно. Основным положением web-OS является решение вопроса организации единственного защищенного рабочего пространства для пользователя независимо от его географического положения, типа операционной системы, которой он пользуется во время сеанса работы и даже аппаратной платформы оборудования, на котором ему приходится работать.

Вариант решения – использовать в качестве основы интерфейса такой операционной оболочки браузер, а сам сервис защищенного рабочего пространства разместить на web-сервере. Сдерживающим фактором долгое время была низкая пропускная способность каналов связи. Сейчас этот вопрос практически решен, поэтому число таких систем резко возросло.

В данном секторе отмечены серьезные продукты разработки компаний: Adobe, Microsoft, Google и многих других. Такие программы универсальны и одинаково легко применяются как для обычной вычислительной техники, так и для мобильных устройств (рисунок 10.7).

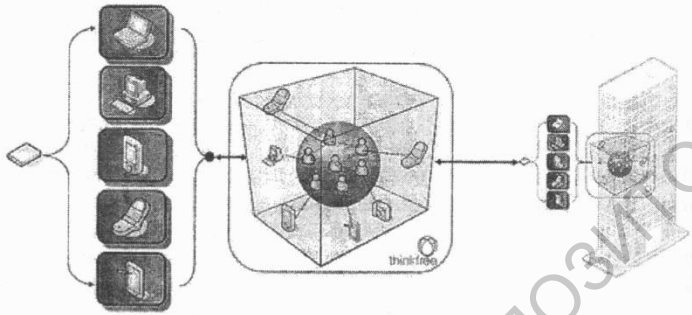


Рисунок 10.7 – Возможности работы с Web-OS

Среди особенностей, называемых разработчиками – безопасность, мобильность данных, отсутствие привязки к «железу» и платформам, встроенные инструменты совместной разработки и высокая производительность при создании приложений. Под безопасностью, в первую очередь, подразумевается то, что программы будут работать в виртуальной машине, изолированной от системы, в так называемом «песочном ящике» (sandbox), как Java-апплеты.

Изначально для работы в среде web-оболочек применялись отдельные web-программные системы (рисунок 10.8). Примером могут служить текстовые on-line редакторы: J2E.com (http://www.j2e.com), AjaxWrite (http://us.ajax13.com/en/ajaxwrite), Peepel.com (http://peepel.com), Solodox.com (http://www.solodox.com), FlySuite.com (http://www.flysuite.com), Buzzword (http://about.buzzword.com), iNetWord.com (http://www.inetword.com), Nevercode Docs (http://www.nevrocode.com/docs), Writeboard (http://www.writeboard.com).

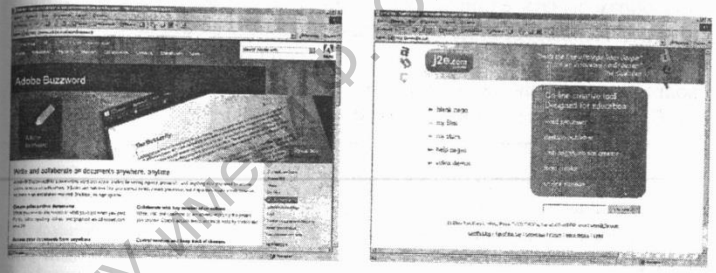


Рисунок 10.8 – Примеры текстовых on-line редакторов

Вторым шагом развития этих программ стали онлайновые офисные пакеты (рисунок 10.9). Например: ThinkFree (www.thinkfree.com), Live Documents (www.live-documents.com), Google Docs (docs.google.com), Zoho (www.zoho.com), Office Live (www.officelive.com), Ulteo (www.ulteo.com).

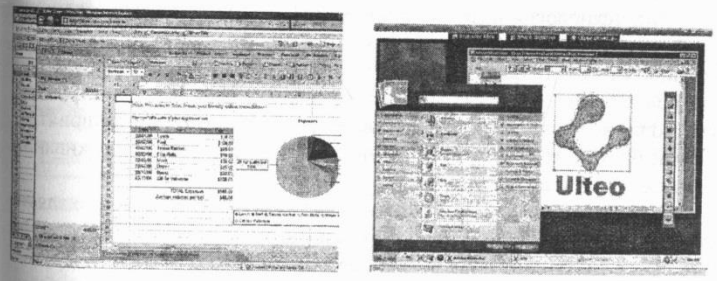


Рисунок 10.9 – Примеры работы в среде on-line офисов

10.7 Применение браузеров в локальных и глобальных сетях

Основным поставщиком информации и средством взаимодействия (в том числе, управления) постепенно становится среда веб (web). Средством взаимодействия пользователя с этой средой являются программы – браузеры. Браузер (обозреватель, навигатор – от английского *browser* – человек, перелистывающий книги) – программа для отображения текста, графических объектов и мультимедиа файлов [7]. Такие объекты могут образовывать единый информационный объект, например, web-страницу. Первые браузеры обладали вполне достаточной функциональностью. Благодаря тому, что многие сетевые протоколы появились задолго до рождения собственно Internet.

Среди реализованных сервисов были:

– просмотр локальных и удалённых файлов;
– обмен данными по протоколу FTP;
– передача запросов и команд по протоколу HTTP;
– просмотр информации, размещённой на web-серверах.

Первым средством автоматизации работы с браузером стали гиперссылки, позволяющие переходить с одной страницы на другую не занимаясь утомительным вводом прямого адреса.

Любой современный браузер способен передавать файлы и в обратном направлении – с локального диска посетителя на сервер. Возможность передачи файлов на web-сервер предусмотрена протоколом RFC1867 с названием Form-based file Upload in HTML (типовой файл на HTML для переписи на Web-сервер).

Эта технология позволила применять браузер в качестве клиентской части почтовых веб-серверов. Популярность сервиса послужила причиной того, что большинство почтовых систем имеют параллельную веб-консоль. Затем браузеры стали широко применять как инструмент контроля и управления производственным процессом предприятия. Сейчас браузер стал ключевым звеном новой технологии обслуживания пользователей Web-OS (Internet – операционных систем).

Использование пользователями сети различных браузеров является серьезной проблемой для web-разработчиков. Если писать web-интерфейс только под один из браузеров, то нет гарантии, что на других программах-обозревателях страница будет отображаться так, как была задумана. Следствием решения проблемы является многократно дублированная система навигации, а иногда и отказ от некоторых элементов оформления. Некоторые из браузеров описаны в таблице 10.1.

Таблица 10.1 – Сводная таблица браузеров

Название	Производитель	Дата первой публичной версии	Последний релиз	Лицензия	Операционная система
Amaya	W3C, INRIA	Ноябрь 1996	10.0	W3C	Windows, BSD, GNU/Linux, Mac OS X, Unix
Camino	Mozilla Foundation	Февраль 2002	1.5.4	MPL, тройная лицензия MPL/GPL/LGPL	Mac OS X
Dillo	Arellano Cid, Geerken, Rota и др.	Декабрь 1999	0.8.6	GPL	Mac OS X, GNU/Linux, BSD, Unix
Elinks	Baudis, Fonseca и др.	Декабрь 2001	0.11.3	GPL	Windows, BSD, GNU/Linux, Mac OS X, Unix
Epiphany	GNOME	Декабрь 2002	2.20.1	GPL	Mac OS X, GNU/Linux, BSD, Unix
Galeon	GNOME	Июнь 2000	2.0.3	GPL	Mac OS X, GNU/Linux, BSD, Unix
ICab	iCab Company	1998	3.0.3	Закрытая	Mac OS X
Internet Explorer	Microsoft Spyglass, Inc.	Август 1995	7.0 5.2.3 (Mac)	Закрытая	Windows
K-Meleon	Doozan, Erikson, Vallet и др.	Ноябрь 2000	1.1.2	GPL	Windows
Konqueror	KDE	Октябрь 2000	3.5.8	GPL	Mac OS X, GNU/Linux, BSD, Unix
Links	Patocka и др.	Ноябрь 1999	0.99	GPL	Windows, BSD, GNU/Linux, Mac OS X, Unix
Lynx	Montulli, Grobe, Rezac и др.	Июль 1993	2.8.6	GPL	Windows, BSD, GNU/Linux, Mac OS X, Unix
Mosaic	Marc Andreessen и Eric Bina, NCSA	Апрель 1993	2.6	Закрытая	Windows, BSD, GNU/Linux, Mac OS X, Unix
Muzilla Suite	Mozilla Foundation	Декабрь 1998	1.7.13	MPL	Windows, BSD, GNU/Linux, Mac OS X, Unix
Mozilla Firefox	Mozilla Foundation	Сентябрь 2002	3.0.4	MPL / GNU LGPL / GNU GPL	Windows, BSD, GNU/Linux, Mac OS X, Unix
Netscape Navigator	Netscape Communications, Mozilla Foundation (с 2000), Mercurial Communications (с 2004)	Октябрь 1994	9.0.0.6	NPL	Windows, Mac OS X, GNU/Linux, BSD, Unix
OmniWeb	Omni Group	Март 1995	5.5.4	Закрытая, LGPL	Mac OS X
Opera	Opera Software	Сентябрь 1996	9.62	Закрытая	Windows, BSD, GNU/Linux, Mac OS X, Unix
e-Capsule Private Browser	Eisst	2005	2.1.0.611	Закрытая	Windows, Mac OS X
Safari	Apple Computer	Июнь 2003	3.1.2	Закрытая, LGPL	
SeaMonkey	Mozilla Foundation, SeaMonkey Council	Сентябрь 2005	1.1.9	MPL / GNU LGPL / GNU GPL	OS/2
WorldWideWeb	Tim Berners-Lee	Август 1991	0.18	общественное достояние	Встроен в NeXTSTEP

Примечание – приведена информация сайта http://ru.wikipedia.org.

10.8 Публикация информации в Internet

Браузеры, рассмотренные выше, работают на стороне клиента. Сервером, предоставляющим ресурсы для работы браузера в сетях Internet и Intranet, является web-сервер.

Сервер WWW (Word-Wide-Web), именуемый также *web-сервером*, является информационным хранилищем, в котором на основе технологии гиперсреды хранятся и предоставляются пользователям страницы WWW, содержащие взаимосвязанные сведения по определенным направлениям науки, культуры, политики, техники, торговли.

Работа с документами web-сервера осуществляется при помощи редактора просмотра и гипертекстового протокола передачи. Серверы связываются как друг с другом, так и с клиентами. В поисках необходимых сведений пользователи осуществляют навигацию по web-серверам.

Создание web-серверов привело к созданию индустрии, специализирующейся на предоставлении услуг пользователям глобальной сети. Тематика информации, предоставляемой web-серверами, чрезвычайно разнообразна. Благодаря этим серверам появился даже термин электронная политика. Базой этой индустрии являются многие тысячи взаимосвязанных web-серверов. Они могут опираться на различные платформы и позволяют работать с большим числом баз данных. При этом должна быть обеспечена высокая степень безопасности данных. Для обеспечения последней используются брандмауэры.

При разработке программного обеспечения:

– используют интерактивные средства доступа к данным, включая электронную рекламу, почтовые автоответчики и технологию гиперсреды;

– создают удобную справочную систему, предоставляющую пользователям исчерпывающую информацию;

– как можно чаще обновляют содержимое адресуемых страниц, добавляют новые страницы.

Web-серверы по предоставляемой ими информации, являются: *универсальными* либо *специализированными*. Каждая организация, желающая разместить информацию, создает на сервере web-сайт, которая представляет собой перечень сведений, выдаваемых на экран. По своим функциям адресная страница очень напоминает оглавление книги. При желании пользователь может передать нужные ему данные в свою абонентскую систему и распечатать на принтере. Для нахождения информации используются поисковые серверы.

Для публикации информации в Интернет необходимо в первую очередь само подключение к сети, которое осуществляется через провайдера. Обычно каждая фирма-провайдер доступа к Интернет, предоставляет своим клиентам возможность размещения своих web-страничек. Однако немаловажный фактор, по которому следует выбирать, где же расположить свой сайт – это Internet-адрес.

Размещение информации в Интернет, подразумевает два этапа:

– собственно подготовка файлов с информацией в необходимом формате у себя на компьютере;

– копирование этих файлов на web-сервер, либо отсылка этих файлов на электронную почту администратора web-сайта с просьбой их разместить.

В Интернете размещают информацию в одном из следующих форматов HTML (Hyper Text Marking Language), PHP, APS, JSP и другие. Для создания Web-страниц можно использовать: Microsoft Word, Microsoft FrontPage Express, Microsoft FrontPage, Macromedia DreamWeaver. Хотя лучше не использовать Microsoft Word, а создавать все в специализированных редакторах. Потому, что Microsoft Word, дает излишне «тяжелый» и перегруженный код.

После того, как подготовлен сайт, проверьте его, открыв его в одном из браузеров. И, убедившись в правильности работы сайта, можно приступать к размещению файлов в Internet. Если у вас небольшой сайт (до 1 Мб) и вам лень возиться с самостоятельным размещением, то можно заархивировать файлы вашего сайта и отослать архив администратору сайта с просьбой разместить. В дальнейшем вы также будете по мере изменения данных присылать архивы обновления своего сайта. Данный метод обновления не годится, если вы планируете обновлять свой сайт очень часто. В этом случае вам необходимо получить доступ к возможности самостоятельного размещения данных на вашем сайте. Получить такой доступ можно сразу в момент заключения договора с фирмой-провайдером на подключение к Internet или позже. Обычно для обновления используется FTP. Для копирования обновлений сайта используют FTP-клиент. Например, CuteFTP или FAR manager.

Важно знать! Когда web-страничка размещается в Internet – никто о ней не знает. Для того, чтобы на вашей web-страничке появились посетители, нужно приложить некоторые усилия. Например, посетить поисковые сервера и прописать ее адрес в разделы с соответствующей тематикой.

10.9 Применение баз данных в сетевой среде

В мире существует масса информационных источников, владельцы которых готовы предоставить их в пользование человечества, но не могут этого сделать. Прежде всего, это относится к научным базам данных. Имеется множество баз данных, подключенных к Internet в режиме свободного доступа. Конечно, этими базами данных можно пользоваться. Но основная проблема состоит в том, что интерфейсы доступа к разным базам данных абсолютно различаются, также, как и способы подключения баз данных к Internet. Имеются трудности как у тех, кто хочет пользоваться базами данных, так и у тех, кто хотел бы передать свою информацию в использование в режиме «on-line».

Отправной точкой разработки технологии является желание потребителей информации получить к ней доступ и стремление поставщиков информации обеспечить ее, а также отсутствие стимула в Internet для предоставления соответствующих возможностей.

В Web все же имеется одна возможность, которую, в принципе, можно использовать для доступа к базам данных. Это *формы*. При навигации по страницам Web можно наткнуться на пометки, при остановке на которых вы получаете не готовую информацию, а некоторую форму, необходимую заполнить. Форма, заполненная в клиентской части системы, поступает на обработку соответствующей программе (программному сценарию), связанной с данной формой. Именно формы являются наиболее близким пользователям интерфейсом для непосредственного доступа к базам данных. Формы разрабатываются на специализированных языках описания форм или с использованием интегрированных языков четвертого поколения. Применяются и средства автоматизированного построения (простых) форм на основе соответствующей схемы базы данных.

Этот простой подход, который не требует привлечения современных технологий Internet, ориентированных на обеспечение доступа к мультимедийной информации, может оказаться вполне достаточным для решения удобного доступа к традиционным реляционным научным базам данных. Если ограничиться SQL-ориентированными базами данных, то несложный инструментальный пакет, который облегчает создание программ, связанных, с одной стороны, с формами, управляемыми сервером Web, а с другой стороны, обеспечивающих стыковку с базами данных.

База Данных (БД) – структурированный организованный набор данных, описывающих характеристики каких-либо физических или виртуальных систем.

Структура БД формируется из следующих соображений:

– адекватность описываемому объекту/системе – на уровне концептуальной и логической модели;

– удобство использования для ведения учёта и анализа данных – на уровне так называемой физической модели.

По модели представления данных БД классифицируются: *картотеки, иерархические, сетевые, реляционные, многомерные, объектно-ориентированные, дедуктивные*.

На уровне физической модели электронная БД представляет собой файл или их набор в формате TXT, CSV, Excel, DBF, XML и пр. Системы управления базами данных в понятие физической модели могут включать виртуальные понятия, существующие в их среде – таблицу, табличное пространство, сегмент, куб, кластер и т. д.

В настоящее время наибольшее распространение получили реляционные БД. Картотеками пользовались до появления электронных БД. Сетевые и иерархические БД данных считаются устаревшими, хотя последние активно применяются после распространения XML. Объектно-ориентированные БД пока никак не стандартизированы и не получили широкого распространения.

Распределённые базы данных (РБД) – совокупность логически связанных баз данных, распределённых в компьютерной сети. РБД состоит из набора узлов, связанных коммуникационной сетью. Узлы взаимодействуют между собой таким образом, что пользователь любого из них может получить доступ к любым данным в сети так, как будто они находятся на его собственном узле. Для пользователя распределённая система должна выглядеть так же, как нераспределённая система. Дополнительные требования к РБД:

- локальная независимость;
- отсутствие опоры на центральный узел;
- непрерывное функционирование;
- независимость от расположения;
- независимость от фрагментации;
- независимость от репликации;
- обработка распределённых запросов;
- управление распределёнными транзакциями;
- аппаратная независимость;
- независимость от операционной системы;
- независимость от типа сети и программной платформы.

10.10 Применение поисковых систем

Практика показывает, что в настоящий момент эффективно и правильно использовать поисковые системы умеют не более 8 % пользователей. В основном люди слишком полагаются на отнюдь несовершенные возможности автоматики и в результате на запрос из 1–2 слов получают совершенно бесполезную для себя информацию.

Современные поисковые системы Интернет не обладают искусственным интеллектом, они построены на принципах, заложенных австрийским ученым Ципфом. Согласно определению *поисковая система* или *поисковая машина* – комплекс программ, предназначенный для поиска информации. Основными критериями качества ее работы являются релевантность (степень соответствия запроса и найденного результата), полнота базы, учёт морфологии языка.

Поисковые системы обычно состоят из трех компонент: агента (паука или кроулера), который перемещается по сети и собирает информацию; базы данных, которая содержит всю информацию, собираемую пауками; поискового механизма, используемого как интерфейс взаимодействия с базой данных.

Средства поиска типа агентов, пауков, кроулеров и роботов – это специальные программы, занимающиеся поиском страниц в сети, извлекают гипертекстовые ссылки на этих страницах и автоматически индексируют информацию, которую они находят для построения базы данных. Каждый тип имеет собственный набор правил, определяющих, как собирать документы (следуют по каждой ссылке на каждой найденной странице; игнорируют или не игнорируют ссылки, ведущие к графическим и звуковым файлам и т. д.).

Агенты – самые «интеллектуальные» из поисковых средств, они могут выполнять даже транзакции от Вашего имени, могут искать сайты специфической тематики и возвращать списки сайтов, отсортированных по их посещаемости и т. д.

Пауки сообщают о содержании найденного документа, индексируют его и извлекают итоговую информацию. Также они просматривают заголовки, некоторые ссылки и посылают проиндексированную информацию базе данных поискового механизма.

Кроулеры просматривают заголовки и возвращают только первую ссылку.

Роботы могут быть запрограммированы так, чтобы переходить по ссылкам различной глубины вложенности, выполнять индексацию и даже проверять ссылки в документе.

База данных отыскивает предмет запроса, согласно информации, указанной в заполненной форме, и выводит соответствующие документы, подготовленные базой данных. Чтобы определить порядок, в котором список документов будет показан, база данных применяет алгоритм ранжирования. Например, *время* (как долго страница находится в базе поискового сервера) или *индекс цитируемости* (как много ссылок на данную страницу ведет с других страниц, зарегистрированных в базе поисковика.)

Классификация поисковых машин. По области поиска делятся (условно) на: локальные и глобальные.

Локальные поисковые машины предназначены для поиска информации по какой-либо части всемирной сети, например по одному или нескольким сайтам, либо по локальной сети.

Глобальные предназначены для поиска информации по всей сети Интернет либо по значительной её части. Представителями таких поисковых машин являются поисковые машины поисковых систем Google, Yahoo, Yandex и т. д.

В последнее время появился тип поисковых движков, основанных на технологии RSS, а также среди XML-данных разного типа.

В идеале процесс поиска должен выглядеть примерно так. Сначала делается общий запрос. На запрос получается ответ с результатами поиска, в котором нужно выделить описания более-менее подходящих ссылок. Затем необходимо добавить к запросу общие ключевые слова, которые есть в описании нужных ссылок и повторить процесс.

Корректировка запроса осуществляется изменением состава и вариантов ключевых слов в виде простой текстовой строки, либо с использованием специального языка операторов, поддерживаемого поисковой машиной. Вот операторы, общие для поисковых систем:

Первый оператор, которого нужно отметить – оператор строгого соответствия, как правило, в современных поисковых системах это кавычки "". Сочетание слов, которые вы укажете в кавычках, будет учитываться системой как единое целое, то есть, таким образом вы задаете порядок следования слов друг за другом. Следующие очень важные операторы – это операторы обязательного наличия слова «+» и оператор обязательного отсутствия слова «–». С языками запросов конкретной поисковой системы можно ознакомиться в разделе помощи. При этом нужно отметить, что многие из них обладают собственными дополнительными операторами, которые могут помочь опытным пользователям.

10.11 Системы обмена сообщениями в сетях разного масштаба

Ускорение и автоматизация пересылки корреспонденции (сообщений) между пользователями – актуальная задача, которая по утверждению некоторых авторов [4,6] дала толчок к самому появлению компьютерных сетей.

По своей сути, платформа обмена сообщениями – это технология, позволяющая двум разнесенным объектам обмениваться любыми видами информации. Остановимся подробнее на тех видах систем обмена сообщениями, которые реализуют информационный обмен между пользователями.

Мгновенный обмен сообщениями. В данном случае используется режим on-line обмена. В сети выделяется сервер, который доставляет данные между узлами, участвующими в текущем соединении. Сервер кэширует сообщения на случай перерывов в сеансах связи, которые часто случаются в глобальной сети. Некоторые сравнивают эту модель общения с моделью виртуального пространства. В локальных и корпоративных сетях могут использоваться бессерверные многопользовательские on-line соединения (chat-системы). В этом случае кэширование данных осуществляется средствами самого узла. А каналы связи считаются абсолютно надежными.

Обмен почтовыми сообщениями. Служба электронной почты предназначена для обеспечения возможности обмена персональными сообщениями между пользователями информационных сетей. Данная служба состоит из объектов клиентов службы (клиентских программ доступа) и серверов электронной почты. Серверы электронной почты, взаимодействуя друг с другом, образуют сеть электронной почты. Каждый пользователь сети зарегистрирован на одном из почтовых серверов. Сервер хранит банк сообщений пользователя (почтовый ящик) под определенным именем. Для отправки сообщения достаточно передать его в определенном формате на свой почтовый сервер с указанием адреса получателя. Почтовый сервер, проанализировав адрес получателя, отправит сообщение через сеть почтовых серверов другому почтовому серверу, содержащему почтовый ящик получателя, куда это сообщение и будет положено. Для получения своих сообщений достаточно обратиться к своему почтовому серверу и считать из почтового ящика все свои сообщения. Существует несколько типов служб электронной почты, базирующихся на различных протоколах обмена, однако наибольшее распространение получила сетевая служба, используемая в сети Internet, базирующаяся на протоколе SMTP.

Служба обмена новостями. Internet-сообщество уже много лет пользуется системой тиражирования объявлений, рекламы, сообщений и другой информации. Всю подобным образом тиражируемую информацию называют новостями – «news». Новости делятся на группы новостей – «newsgroups». Группы новостей организованы в определенном порядке, основанном на распределении дискуссий по темам, например, отдых, спорт, новости, информация, религия и др. Внутри каждой из этих групп может быть до нескольких тысяч подгрупп, которые, в свою очередь, обладают такой же иерархической структурой. Принцип этой организации подобен структуре размещения каталогов и подкаталогов на жестком диске.

Механизм передачи статей пользователю заключается в следующем. Предположим, что какое-либо сообщение попадает в конференцию на одной машине, например, оно поступило от пользователя. Это сообщение принимается данным хостом в локальную базу данных и передается всем его соседям, которые «подписаны» по крайней мере на одну из конференций, к которой относится данная статья. Этот процесс будет продолжаться до тех пор, пока все хосты подсети данной конференции не будут располагать этой статьей.

Для небольшого количества пользователей идеальной схемой построения обмена новостями была бы структура, состоящая из одного News-сервера и пользователей, обращающихся к нему для отправки или получения новых статей. В системах с большим количеством клиентов, например, масштаба университета или крупного предприятия, необходимо использовать так называемые промежуточные серверы новостей – intermediate news server.

Для обмена сообщениями между серверами новостей используется протокол NNTP (Network News Transfer Protocol).

Подписки на рассылку. Метод получения актуальной информации по электронной почте. Сообщение содержит краткое описание обновлений и непосредственные адреса (url-link) обновленных страниц. Это позволяет сократить время поиска обновлений сайта Internet.

Форумы и Блоги. Интерактивные банки сообщений, оставляемые посетителями на каком-либо сайте в Internet. Допускается промежуточный отбор входящих сообщений, либо четко выраженное авторское наполнение.

Также здесь следует упомянуть о современных технологиях обмена сообщениями, применяемых компаниями сотовой связи. Например, SMS, EMS, MMS и прочие.

Вопросы для самоконтроля

1 Что представляет собой компьютерная программа?

2 На какие виды можно разделить программное обеспечение?

3 Для чего применяются операционные оболочки?

4 Опишите взаимодействие программных компонентов при работе двух сетевых операционных систем.

5 Опишите различие между видами операционных систем.

6 Что такое «тонкий клиент»?

7 Опишите место Web-OS в современном вычислительном процессе.

8 Как работает серверная операционная система?

9 Приведите примеры операционных систем для сетевых клиентов.

10 Перечислите функции сервера в сетевой среде.

11 Для чего предназначены браузеры?

12 Как организован доступ к информации в Интернет и Интранет?

13 Дайте определения следующим понятиям: Web-сервер, база данных, поисковая система.

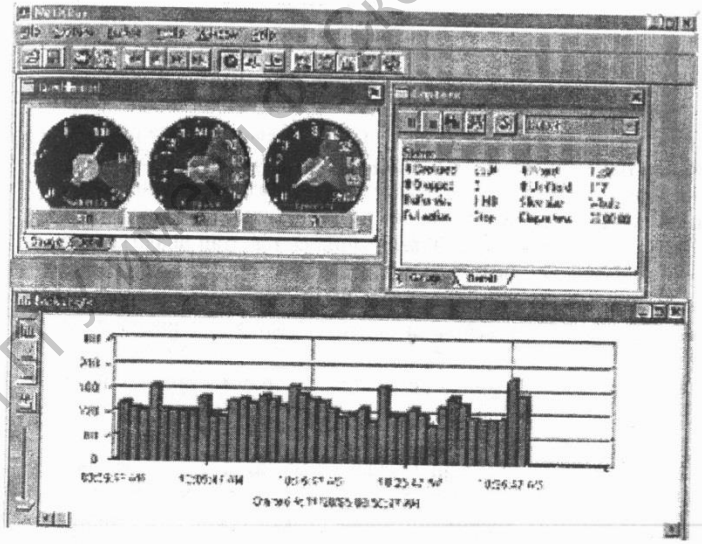
14 Для чего применяются базы данных в сетевых средах?

15 Как найти нужные данные в сети?

16 Что представляют собой системы обмена сообщениями?

17 Назовите наиболее популярные технологии обмена сообщениями и их свойства.

11 Средства мониторинга и анализа сетей



11.1 Контроль состояния сетевой среды

Постоянный контроль за работой локальной сети, составляющей основу любой корпоративной сети, необходим для поддержания ее в работоспособном состоянии. Контроль – это необходимый первый этап, который должен выполняться при управлении сетью. Ввиду важности этой функции ее часто отделяют от других функций систем управления и реализуют специальными средствами. Использование автономных средств контроля помогает администратору сети выявить проблемные участки и устройства сети.

Процесс контроля работы сети обычно делят на два этапа – мониторинг и анализ. На этапе мониторинга выполняется более простая процедура – процедура сбора первичных данных о работе сети: статистики о количестве циркулирующих в сети кадров и пакетов различных протоколов, состоянии портов концентраторов, коммутаторов и маршрутизаторов. Далее выполняется этап анализа, под которым понимается более сложный и интеллектуальный процесс осмысления собранной на этапе мониторинга информации, сопоставления ее с данными, полученными ранее, и выработки предположений о возможных причинах замедленной или ненадежной работы сети.

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

Отдельной функцией контроля сети, связанной с профилактикой потенциального роста паразитного трафика, является организация работы антивирусной системы. Например, когда вирус типа «червь» (worm) поражает операционную систему, он начинает искать пути для распространения. С этой целью он рассылает по сети служебные запросы от имени системы. В сети большого масштаба такой паразитный трафик может быть значительным. Автономную систему можно защитить локальным брандмауэром, действующим совместно с антивирусным монитором, но блокировать паразитный трафик от зараженных систем без централизованной политики безопасности – практически невозможно.

В действующих вычислительных сетях хорошо зарекомендовали себя следующие антивирусные решения: Dr.Web Enterprise Suite, ESET Enterprise Security (NOD32), Kaspersky Open Space Security, McAfee Total Protection for Endpoint, Symantec AntiVirus и некоторые другие.

Еще одной важной частью системы контроля в вычислительных сетях являются системы биллинга – детализированный авторизованный учет сетевого трафика по типу запроса и объему сервиса.

Существуют комплексные решения биллинга и антивирусной защиты. Например: Kaspersky Gate Antivirus / Traffic Inspector или Panda Gate Antivirus / Traffic Inspector.

Типовой вариант схемы размещения контрольных средств в сети может выглядеть следующим образом (рисунок 11.1).

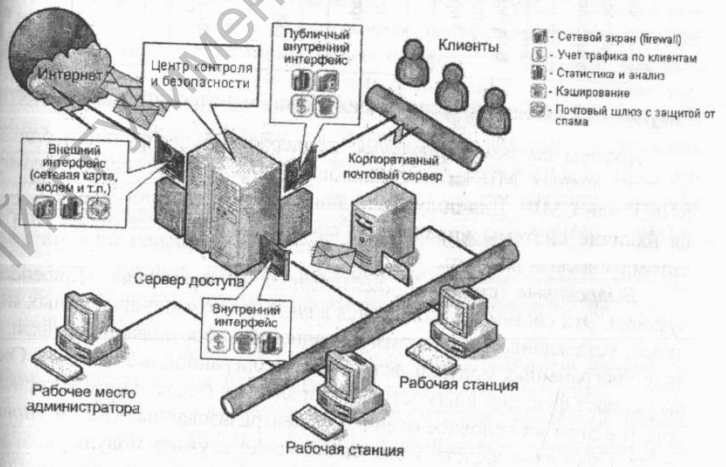


Рисунок 11.1 – Работа системы контроля сетевого трафика

При выборе программных средств сетевого контроля важно учитывать, что любое средство контроля и управления само является источником порождения дополнительного трафика и нагрузки на вычислительные мощности серверов сети. Учитывая данный факт, необходимо найти точку баланса настроек текущей версии защитных систем, либо лучший вариант соотношения качества/цены при покупки альтернативной системы.

11.2 Классификация средств мониторинга и анализа сети

Все многообразие средств, применяемых для анализа и диагностики сетей, можно разделить на несколько классов (рисунок 11.2).

Рисунок 11.2 – Общая классификация средств мониторинга и анализа сети

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

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

Анализаторы протоколов (Protocol analyzers). Представляют собой программные или аппаратно-программные системы, которые ограничиваются в отличие от систем управления лишь функциями

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

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

Оборудование для диагностики и сертификации кабельных систем. Условно это оборудование можно поделить на четыре основные группы:

– *сетевые мониторы* (называемые также сетевыми анализаторами) предназначены для тестирования кабелей различных категорий. Эти устройства являются наиболее интеллектуальными устройствами, так как работают не только на физическом, канальном и сетевом уровнях. Они также данные о среднестатистических показателях трафика;

– *устройства для сертификации кабельных систем* выполняют сертификацию в соответствии с требованиями одного из международных стандартов на кабельные системы;

– *кабельные сканеры* используются для диагностики медных кабельных систем;

– *тестеры* предназначены для проверки кабелей на отсутствие физического разрыва.

11.3 Анализаторы протоколов

Анализатор протоколов представляет собой либо специализированное устройство, либо персональный компьютер, обычно переносной, класса Notebook, оснащенный специальной сетевой картой и соответствующим программным обеспечением. Применяемые сетевая карта и программное обеспечение должны соответствовать технологии анализируемой сети (Token Ring, FDDI, Fast Ethernet). Анализатор подключается к сети точно так же, как и обычный узел. Отличие состоит в том, что анализатор может принимать все пакеты данных, передаваемые по сети, в то время как обычная станция – только адресованные ей. Для этого сетевой адаптер анализатора протоколов переводится в режим «беспорядочного» захвата – promiscuous mode.

Все множество анализаторов можно условно разделить на два вида. К первому относятся автономные продукты, устанавливаемые на мобильном компьютере. Второй вид анализаторов является частью более широкой категории аппаратного и программного обеспечения, предназначенного для мониторинга сети и позволяющего организациям контролировать свои локальные и глобальные сетевые службы, в том числе Web. Эти программы дают администраторам целостное представление о состоянии сети. Например, с помощью таких продуктов можно определить, какие из приложений выполняются в данный момент, какие пользователи зарегистрировались в сети и кто генерирует основной объем трафика.

Вместо того чтобы выявлять низкоуровневые характеристики сети, скажем источник пакетов и пункт их назначения, современные анализаторы декодируют полученные сведения на всех уровнях модели OSI и зачастую выдают рекомендации по устранению проблем.

Программное обеспечение анализатора состоит из ядра, поддерживающего работу сетевого адаптера и программного обеспечения, декодирующего протокол канального уровня, с которым работает сетевой адаптер, а также наиболее распространенные протоколы верхних уровней, например IP, TCP, FTP, TELNET, HTTP, IPX, NCP, NetBEUI, DECnet и др. В состав некоторых анализаторов может входить также экспертная система, которая позволяет выдавать пользователю рекомендации о том, какие эксперименты следует проводить в данной ситуации, что могут означать те или иные результаты измерений, как устранить некоторые виды неисправности сети.

Перечислим общие свойства анализаторов протоколов:

– возможность (кроме захвата пакетов) измерения среднестатистических показателей трафика в сегменте локальной сети, в котором установлен сетевой адаптер анализатора. Обычно измеряется коэффициент использования сегмента, матрицы перекрестного трафика узлов, количество хороших и плохих кадров, прошедших через сегмент;

– возможность работы с несколькими агентами, поставляющими захваченные пакеты из разных сегментов локальной сети. Эти агенты чаще всего взаимодействуют с анализатором протоколов по собственному протоколу прикладного уровня, отличному от SNMP или CMIP;

– наличие развитого графического интерфейса, позволяющего представить результаты декодирования пакетов с разной степенью детализации;

– фильтрация захватываемых и отображаемых пакетов. Условия фильтрации задаются в зависимости от значения адресов назначения и источника, типа протокола или значения определенных полей пакета. Пакет либо игнорируется, либо записывается в буфер захвата. Использование фильтров значительно ускоряет анализ, так как исключает захват или просмотр ненужных в данный момент пакетов;

– использование триггеров. Триггеры – это задаваемые администратором некоторые условия начала и прекращения процесса захвата данных из сети. Такими условиями могут быть: время суток, продолжительность процесса захвата, появление определенных значений в кадрах данных. Триггеры могут использоваться совместно с фильтрами, позволяя более детально и тонко проводить анализ, а также продуктивнее расходовать ограниченный объем буфера захвата;

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

11.4 Кабельные сканеры и тестеры

Кабельные сканеры – это портативные приборы, которые обслуживающий персонал может постоянно носить с собой. Основное назначение кабельных сканеров – измерение электрических и механических параметров кабелей: длины кабеля, параметра NEXT, затухания, импеданса, схемы разводки пар проводников, уровня электрических шумов в кабеле. Точность измерений, произведенных этими устройствами, ниже, чем у сетевых анализаторов, но вполне достаточна для оценки соответствия кабеля стандарту.

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

Точность измерения расстояния зависит от того, насколько точно известна скорость распространения электромагнитных волн в кабеле. В различных кабелях она будет разной. Скорость распространения электромагнитных волн в кабеле (Nominal Velocity of Propagation, NVP) обычно задается в процентах от скорости света в вакууме. Современные сканеры содержат в себе электронную таблицу данных о NVP для всех основных типов кабелей, что дает возможность пользователю устанавливать эти параметры самостоятельно после предварительной калибровки. Они также позволяют идентифицировать все существующие ошибки в схеме разводки кабеля, включая определение расщепленных пар (Split pair), и измерить расстояние до неисправности, определить скорость соединения, выполнить команду Ping, подать сигнал для трассировки, идентифицировать порт ближайшего коммутатора, провести аутентификацию в сетях со стандартом 802.1x, протестировать питание через Ethernet (PoE). Вся информация отображается на большом высококонтрастном дисплее.

Кабельные тестеры – наиболее простые и дешевые приборы для диагностики кабеля. Они позволяют определить непрерывность кабеля, однако, в отличие от кабельных сканеров, не дают ответа на

вопрос о том, в каком месте произошел сбой. Тестеры кабельных линий предназначены для экспресс-контроля, проведения комплексных испытаний, выявления различных видов неисправностей локальных компьютерных сетей, телевизионных и телефонных линий, использующих в соединении кабели различных стандартов. Типичным представителем является тестер LAN-PRO-L (рисунок 11.3), предназначенный для тестирования линий связи, построенных на основе медных пар, телефонных и коаксиальных кабелей. Прибор позволяет выявить дефекты линии (перепутанные пары, обрыв и замыкание) и измерить длину каждой пары. В комплект поставки LAN-PRO-L входят специальные адаптеры:

– RJ45-BNC – для тестирования коаксиальных кабелей, оконцованных коннекторами типа BNC;

– RJ45-крокодил, 1 пара – для тестирования отдельных пар или неоконцованных кабелей.

Для удобства работы с тестером LAN-PRO-L, при наличии физического контакта хотя бы по одному проводнику динамик ответной части издает звуковой сигнал. Свидетельством об окончании тестирования служит изменение звукового сигнала. С целью экономии батареи, тестер, после 30 минут бездействия, переключается в «спящий режим».

Рисунок 11.3 – Консоль управления кабельного тестера LAN-PRO-L

11.5 Программные системы моделирования сетевых структур

Перед тем как внедрять сетевое решение в программной части или при замене оборудования, удобнее апробировать его работу в среде программного симулятора.

Один из лидеров в области телекоммуникационных технологий Cisco Systems предлагает использовать программные системы моделирования сетевых структур. Системы моделирования компьютерных сетей, разработанные специалистами данной компании, позволяют быстро сконструировать сеть, настроить программную часть имитационной модели, увидеть, какие процессы происходят в созданной сети и правильно ли она функционирует.

Cisco System Inc предлагает использовать бесплатный программный пакет Packet Tracer (рисунок 11.4) для симулирования работы сети, построенной по сетевым технологиям Cisco в рамках программы Cisco Networking Academy.

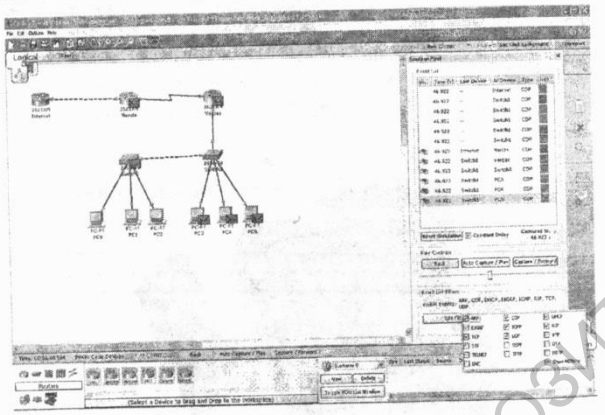


Рисунок 11.4 – Рабочее окно программы Packet Tracer

Медиатор Packet Tracer (система отслеживания пакетов) позволяет имитировать функции сетей любого размера и тем самым расширяет возможности обкатки сети на модели. Как показала практика использования данного продукта, минусом является весьма ограниченный список моделей коммутаторов и маршрутизаторов фирмы Cisco, а также отсутствие поддержки многих функций реального оборудования.

Еще одна программная система моделирования сетевых структур – *Boson Network simulator* – имеет расширенные возможности по сравнению с Packet Tracer. Данная программа позволяет получить практические знания по работе с сетевыми устройствами, начиная от обычных управляемых свичей и заканчивая роутерами 7-го поколения. В поставку включена утилита для моделирования сети. В ней можно смоделировать любой тип сети или выбрать готовый образец.

Еще один программный эмулятор маршрутизаторов Cisco – *Dynamips* (рисунок 11.5) разработанный Christophe Fillot работает на большинстве Linux-систем, Mac OS X и Windows, при этом позволяет эмулировать аппаратную часть маршрутизаторов, непосредственно загружая и взаимодействуя с реальными образами Cisco IOS. На данный момент Dynamips поддерживает различные платформы, в их числе 1700, 2600, 3600, 3700, 7200, а также большое количество модулей для интерфейсов типа Ethernet, Serial, ATM и других.

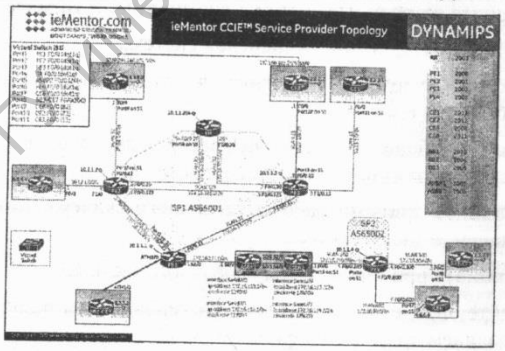


Рисунок 11.5 – Работа в среде программы Dynamips

Все же, как показывает практика, реальное оборудование никакая программа моделирования не может заменить.

Ограничение на применение программ-эмуляторов:

– эмуляция работы операционной системы сетевого устройства требует значительных вычислительных ресурсов, а в рамках одной модели должно взаимодействовать несколько устройств;

– библиотеки моделей сетевых устройств не поставляются;

– виртуальное оборудование не дает эффекта полноценной поддержки всех модулей и функций реальных устройств.

Вопросы для самоконтроля

1 Опишите назначение систем контроля за состоянием сети.

2 Как организовать работу системы антивирусного контроля в сети?

3 Что такое агенты систем управления?

4 Каким образом можно провести сертификацию кабельных линий сети?

5 Какие характеристики позволяет измерить кабельный сканер?

6 Перечислите основные задачи мониторинга.

7 Дайте краткую классификацию средств мониторинга.

8 Опишите встроенные системы диагностики и управления.

9 Дайте характеристику экспертной системы.

10 Какое оборудование применяется для диагностики и сертификации кабельных систем?

11 Опишите общие свойства анализаторов протоколов. Что подразумевается под понятием многоканальности?

12 Опишите принцип работы кабельного сканера. Каково основное назначение кабельного сканера?

13 Опишите принцип работы кабельного тестера.

14 Дайте определение понятию триггеров. В чем разница между использованием тригтеров и фильтрацией?

15 На каких уровнях модели OSI работает анализатор протокола?

16 Дайте определение анализатора протокола.

17 Зачем нужны программы моделирования сетевых структур и сетевых устройств?

Словарь терминов

ADPCM (Adaptive Differential Pulse Code Modulation, адаптивная разностная (дифференциальная) импульсно-кодовая модуляция) – стандартизованный ITU-TSS метод преобразования аналогового речевого сигнала в цифровую форму, когда по каналу связи передается разность между текущим значением сигнала и предыдущим.

Apple Talk (AppleTalk network) – тип локальной сети, созданная корпорацией Apple Computer локальная сеть, предназначенная для совместного использования серверов, клиентов и принтеров.

ArcNet (Attached Resource Computer Network, вычислительная сеть соединенных ресурсов) – широковещательная локальная сеть с использованием маркера (IEEE 802.4).

ARP (Address Resolution Protocol, протокол разрешения адресов) – сетевой протокол канального уровня, предназначенный для преобразования IP-адресов (адресов сетевого уровня) в MAC-адреса (адреса канального уровня) в сетях TCP/IP. Он определён в RFC 826.

ARPAnet – исследовательская сеть с коммутацией пакетов Агентства перспективных исследовательских проектов министерства обороны США. Сеть ARPANET явилась основой для построения Internet.

ASCII (American Standard Code for Information Interchange) – американский стандартный код для информационного обмена.

ATM (Asynchronous Transfer Mode, асинхронный способ передачи) – пакетно-ориентированный метод скоростной коммутации данных, позволяющий передавать данные по одним и тем же физическим каналам, работать с постоянными и переменными потоками данных, интегрировать тексты, речь, изображения и видеофильмы, поддерживать соединения разных типов.

AUI (Attachment Unit Interface, интерфейс модуля присоединения) – 15-штырьковый разъём для соединения между сетевой платой компьютера (NIC) и коаксиальным кабелем Ethernet типа 10Base5 («толстый»).

BISYNC – протокол двоичной синхронизированной связи. Синхронная связь используется в основном на выделенных цифровых линиях, и в домашних условиях, как правило, не применяется.

Blade-system – это комплекс из шасси, процессорных модулей, дополнительных функциональных модулей, плат внутренней коммутации, системы подачи и распределения электропитания, а также программного обеспечения, которое позволяет эффективно использовать весь этот набор.

Bluetooth – производственная спецификация беспроводных персональных сетей (WPAN – Wireless Personal Area Network). Bluetooth обеспечивает обмен информацией между портативными устройствами на повсеместно доступной радиочастоте для ближней связи (2,4–2,48 ГГц).

BootP – протокол Internet, используемый для обеспечения сетевых адаптеров конфигурационной информацией. Особенно полезен данный протокол для выбора конфигурации сетевых адаптеров дистанционно.

CAN (Campus Area Network) – кампусные сети, объединяют локальные сети близко расположенных зданий.

Carrier (несущая) – синусоидальный сигнал определенной частоты с низким коэффициентом затухания для данной среды передачи, модулируемый полезным сигналом.

CATV (Community Antenna Television, телевидение с общей антенной) – модель телевизионного вещания (а также иногда и FM-радиовещания), в которой сигнал распространяется посредством высокочастотных сигналов, передаваемых через проложенный к потребителю кабель.

CDMA (Code Division Multiple Access, множественный доступ с кодовым разделением) – множественный доступ, основанный на присвоении каждому пользователю отдельного числового кода.

CIDR (Classless Inter-Domain Routing, бесклассовая междудоменная маршрутизация) – метод маршрутизации, используемый для увеличения количества подсетей, соответствующих заданной длине адреса.

Cisco IOS (Internetwork Operating System – Межсетевая Операционная Система) – это многозадачная операционная система, выполняющая функции сетевой организации, маршрутизации, коммутации и передачи данных. IOS – программное обеспечение, используемое в маршрутизаторах Cisco и некоторых сетевых коммутаторах, является не бесплатным – это продукт, который надо покупать.

CLI (Command Line Interface) – режим командного интерфейса. Пользователь вводит текстовые команды для управления системой. Результат система выдает в виде текстовых сообщений.

COM – двунаправленный последовательный интерфейс, предназначенный для обмена байтовой информацией. Информация передаётся последовательно по одному биту.

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) – метод множественного доступа с контролем несущей и предотвращением коллизий.

CSMA/CD (Carrier Sense Multiple Access with Collision Detection) – метод множественного доступа к среде с контролем несущей и обнаружением коллизий.

DDP – протокол сетевого уровня в сетях AppleTalk. Обеспечивает обслуживание без установления соединения между сетевыми гнездами.

DECNet – набор протоколов корпорации Digital Equipment Corporation для одноименных сетей.

DECT (Digital Enhanced Cordless Telecommunication) – технология беспроводной связи на частотах 1880—1900 МГц с модуляцией GMSK, разработанный Европейским институтом стандартов (ETSI).

Demand Priority (обработка запросов по приоритету) – высокоскоростной метод доступа к каналу, используемый сетями 100VG–AnyLAN в топологии активных концентраторов («звезда»). Спецификация IEEE 802.12.

DMA channel (Direct memory access channel, канал прямого доступа к памяти) – канал для прямого доступа к памяти, в котором не участвует процессор.

DNS (Domain Name System, система доменных имён) – распределённая система (база данных), способная по запросу, содержащему доменное имя хоста (компьютера или другого сетевого устройства), сообщить его IP адрес или другую информацию.

DoD (Department of Defense, Министерство обороны США) – четырехуровневая модель организации взаимодействия сетевых устройств, соответствующая стеку протоколов TCP/IP.

EIGRP (Enhanced Interior Gateway Routing Protocol) – протокол маршрутизации, разработанный фирмой Cisco на основе протокола IGRP той же фирмы.

EISA (Extended Industry Standard Architecture, архитектура расширенного индустриального стандарта) – открытая 32-разрядная архитектура шины, совместимая с 8 и 16-разрядными платами расширения для шины ISA.

E–mail (Electronic mail, электронная почта) – сетевая служба, позволяющая пользователям обмениваться сообщениями или документами без применения бумажных носителей.

Ethernet (от англ. Ether – эфир + Net – сеть) – технология построения локальной вычислительной сети на основе кабеля. В Ethernet каждый узел может принимать все сообщения. Топология Ethernet – линейная или звездообразная.

EWN – корпоративная сеть.

FDDI (Fiber Distributed Data Interface, оптоволоконный распределенный интерфейс передачи данных) – сетевая архитектура высокоскоростной передачи данных по оптоволоконным линиям, основанная на топологии резервированного двойного кольца с подсоединяемыми деревьями.

FDMA (Frequency Division Multiple Access, множественный доступ с разделением частоты, WDMA, Wave Division Multiple Access, множественный доступ с разделением волны) – множественный доступ с разделением частоты – множественный доступ, основанный на разделении полосы пропускания физического канала на группу (узких) полос, образующих логические каналы.

FireWire (IEEE 1394, i–Link) – последовательная высокоскоростная шина, предназначенная для обмена цифровой информацией между компьютером и другими электронными устройствами.

FSK (frequency shift keying, частотная манипуляция) – вид модуляции, при которой дискретная информация заложена в переменной частоте сигнала несущей.

FTP (File transfer protocol, протокол передачи файлов) – протокол, предназначенный для обеспечения передачи и приема файлов между серверами и клиентами, работающими в сетях, поддерживающих протокол TCP/IP.

GAN (Global Area Network, WAN Wide/World Area Network) – глобальная сеть. Сетью сетей в наше время называют глобальную сеть – Internet .

Gigabit Ethernet – стандарт объединения компьютеров в вычислительную сеть со скоростью передачи данных 1 Гбит/с.

Gopher – протокол доступа клиентов к файлам и каталогам в сети Internet . Протокол Gopher предоставляет доступ к текстовой информации и удобен для передачи больших документов, не содержащих форматирования или иллюстраций.

HDLC (High Level Data Link Control, высший уровень управления каналом данных) – протокол канального уровня, определяющий функции управления каналом для синхронной, независимой от выбранных кодов передачи данных между смежными системами.

HDTV (High–Definition Television) — телевидение высокой чёткости — набор стандартов телевизионного вещания повышенного качества посредством цифровых каналов связи (кабельные, спутниковые сети, цифровые носители).

HiperLAN (High PErformance Radio LAN) – европейский стандарт беспроводных локальных сетей.

HomeRF – беспроводная технология, которая использует безлицензионный ISM диапазон 2.4 ГГц. Она основана на протоколе совместного беспроводного доступа (Shared Wireless Access Protocol – SWAP), который определяет общий интерфейс, поддерживающий беспроводные сети для передачи голоса и данных в пределах дома.

HTML (HyperText Markup Language, язык гипертекстовой разметки HTML) – язык разметки исходного текста веб-документа, включающий специальные символы (теги), которые позволяют веб-браузеру сконструировать из текста дизайн.

HUB – многопортовый повторитель или концентратор, служащий узлом кабельных систем в сетях с древовидной и звездообразной топологиями.

ICMP (Internet Control Message Protocol, межсетевой протокол управления сообщениями) – служебный протокол стека протокола TCP/IP, поддерживающий пакеты, содержащие сообщения об ошибках, тестирующие пакеты и информационные сообщения.

IEC (International Electrotechnical Commission, международная комиссия по электротехнике) – занимается стандартизацией в области электротехники и электроники. В 1967 году IEC заключила соглашение с ISO о совместной разработке стандартов и спецификаций.

IEEE (Institute of Electrical and Electronics Engineers, институт инженеров по электротехнике и электронике) – занимается содействием обмену информацией и разработкой стандартов и специфика-

ций для нижних уровней сетевых технологий (т. е. физического и канального).

IETF (Internet Engineering Task Force) входит в состав IAB, который, в свою очередь, является технической консультативной группой в составе ISOC (Internet Society). Основной задачей групп IETF является разработка и подача проектов Internet, которые затем преобразуются в официальные документы RFC.

IMAP (Internet Message Access Protocol, протокол доступа к электронной почте Internet) – протокол прикладного уровня для доступа к электронной почте.

IP (Internet Protocol, межсетевой протокол) – часть стека протоколов TCP/IP, определяющая процесс маршрутизации пакетов.

IPX (Internetwork Packet Exchange, межсетевой обмен пакетами) – в сетях NetWare – пятиуровневый протокол, регламентирующий обмен данными между сервером и рабочими станциями.

ISA (Industry Standard Architecture, архитектура индустриального стандарта) – открытая 16-разрядная архитектура шины, принятая в IBM-совместимых компьютерах.

ISO (International Standardization Organization, всемирная федерация национальных органов стандартизации) – занимается разработкой международных стандартов.

ITU (International Telecommunications Union, международный союз телекоммуникаций) – занимается финансированием конференций, публикацией документов и учреждением стандартов на продукты и услуги в области телекоммуникации.

LAN (Local Area Network, ЛВС, локальная сеть) – компьютерная сеть, покрывающая обычно относительно небольшую территорию или небольшую группу зданий.

LDP (Label Distribution Protocol, протокол распределения меток) – протокол маршрутизации. Служит для организации процедуры «раздачи» и согласования меток маршрутизаторами MPLS.

LLC (Logical Link Control sublayer, подуровень управления логической связью) – по стандарту IEEE 802 – верхний подуровень канального уровня модели OSI, управляющий передачей данных и обеспечивающий проверку и правильность передачи информации по соединению.

LPT (IEEE 1284, порт принтера, параллельный порт) – международный стандарт параллельного интерфейса для подключения периферийных устройств персонального компьютера.

MAC (Media Access Control sublayer, подуровень управления доступом к среде) – по стандарту IEEE 802 – нижний подуровень канального уровня модели OSI, взаимодействующий с платой сетевого адаптера и отвечающий за безошибочную передачу данных между двумя компьютерами в сети.

MAN (Metropolitan area network, «сеть крупного города») – тип сети, применяемый для объединения в одну сеть группы сетей, расположенных в разных зданиях. В диаметре такая сеть может составлять от 5 до 50 километров.

MAU (Multiple Access Unit) – активный или пассивный концентратор, используемый для реализации топологии кольца на кабельной системе с физической топологией звезды.

MCA (Micro Channel Architecture, микроканальная архитектура) – шина, предназначенная для соединения внешних устройств с компьютерами, разработанная корпорацией IBM.

NetBIOS (Network Basic Input/Output System, сетевая базовая система ввода/вывода) – интерфейс сеансового уровня, обеспечивающий связь между сетевыми приложениями, выполняющимися на компьютерах типа IBM PC, и протоколами транспортного и сетевого уровней эталонной модели OSI.

NFS (Network File System) – протокол сетевого доступа к файловым системам. Позволяет подключать (монтировать) удалённые файловые системы через сеть. Описан в RFC 1094, RFC 1813, и RFC 3530.

NIC (Network Interface Card, сетевой адаптер) – устройство, служащее для подключения компьютера к локальной сети. Сетевой адаптер контролирует доступ к среде передачи данных и обмен данными между единицами сети.

NLSP (NetWare Link Services Protocol) – протокол маршрутизации базирующийся на определении состояния линии связи. Используется маршрутизаторами в сетях IPX для разделения информации об обеспечиваемых ими маршрутах с другими устройствами сети.

NVP (Nominal Velocity of Propagation) – скорость распространения электромагнитных волн в кабеле, задается в процентах от скорости света в вакууме.

OFDM (Orthogonal Frequency Division Multiplexing, ортогональное мультплексирование с разделением частот) – метод высокоскоростной передачи данных, при котором входной поток разби-

вается на группы по n символов в каждой. После преобразования в параллельный поток длительность символов T увеличивается в n раз, т.е. $T = n * To$. Все символы одной группы передаются параллельно, каждый на своей поднесущей. Это позволяет снизить до минимума или полностью исключить символьные искажения в радиоканале.

OSI (Open System Interconnection, взаимодействие открытых систем) – семиуровневая модель организации взаимодействия сетевых устройств, разработанная ISO.

OSPF (Open Shortest Path First) – протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала (link–state technology) и использующий для нахождения кратчайшего пути – алгоритм Дейкстры (Dijkstra's algorithm).

PCI (Peripheral Component Interconnect) – шина, предназначенная для соединения внешних устройств с компьютерами. Стандарт PCI предусматривает использование вспомогательного контроллера, который берет на себя разделение сигналов процессора и шины и осуществляет разрешение конфликтов.

PCMCIA – спецификация на модули расширения для ноутбуков, разработанная ассоциацией PCMCIA (Personal Computer Memory Card International Association).

POP (Post Office Protocol, протокол почтового отделения) – протокол прикладного уровня для доступа к электронной почте, используется почтовым клиентом для получения сообщений электронной почты с сервера. Обычно используется в паре с протоколом SMTP.

RADIUS (Remote Authentication in Dial–In User Service) — протокол AAA (Authentication, Authorization и Accounting), разработанный для передачи сведений между центральной платформой AAA и оборудованием Dial–Up доступа (NAS, Network Access Server) и системой биллинга.

RAID (Redundant Array of Independent Disks, избыточный массив независимых дисков) – архитектура массива жестких дисков, обеспечивающая отказоустойчивость накопителей. Уровни спецификации различаются по производительности, надежности и цене.

RARP (Reverse Address Resolution Protocol, обратный протокол преобразования адресов) – протокол третьего (сетевого) уровня модели OSI, выполняет обратное отображение адресов, то есть преобразует аппаратный адрес в IP–адрес. Описан в RFC 903.

RFC (Requests for Comments, запросы на комментарии) – серия документов, публикуемая сообществом исследователей и разработчиков, в которой описывается набор протоколов Internet и обобщается опыт функционирования Internet .

RIP (Routing Information Protocol) – дистанционный векторный протокол маршрутизации для небольших компьютерных сетей, который позволяет маршрутизаторам динамически обновлять маршрутную информацию, получая ее от соседних маршрутизаторов.

RPC (Remote procedure call, удаленный вызов процедур) – протокол сеансового уровня, предназначенный для отображения результатов выполнения процедуры на удаленном хосте.

RTS (Request to Send, запрос на передачу) – посылается модему терминалом, когда последний имеет данные для передачи.

SMTP (Simple Mail Transfer Protocol, простой протокол передачи почты) – сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP.

SNMP (Simple Network Management Protocol, простой протокол управления сетью) – протокол управления сетями связи на основе архитектуры TCP/IP. SNMP определяет сеть как совокупность сетевых управляющих станций и элементов сети, которые совместно обеспечивают административные связи между сетевыми управляющими станциями и сетевыми агентами.

SNMP (Simple Network Management Protocol, простой протокол управления сетью) – группа стандартов прикладного уровня, определяющих функционирование ассоциации локальных сетей.

SOHO (Small Office Home Office) – организация производственного процесса, при котором сотрудники распределяются по филиалам (малым офисам) или выполняют свои служебные обязанности на дому. Управление производственным процессом осуществляется с использованием сетевых технологий.

Sonet (Synchronous Optical Network, синхронная оптическая сеть) – международный стандарт передачи сигналов через оптические каналы. Физический уровень SONET основывается на иерархии асинхронных линий T–1.

STDM (Statistical Time Division Multiplexing, статистическое временное мультиплексирование) – метод мультиплексирования, при котором канал представляется по очереди только тем системам, которые способны немедленно начать передачу данных.

STP (Shielded Twisted Pair, экранированная витая пара) – витая пара, окруженная заземленной металлической фольгой, которая служит экраном и обеспечивает защиту от электромагнитных помех.

STP (Spanning Tree Protocol) – протокол автоматического исправления петлевых связей между коммутаторами.

T–1 – магистральные линии аналоговой связи, обеспечивающие повышенную пропускную способность и снижающие стоимость телекоммуникационной инфраструктуры методом мультиплексирования.

TCP (Transmission Control Protocol, протокол управления передачей) – протокол управления передачей данных, использующий автоматическую повторную передачу пакетов, содержащих ошибки. Протокол TCP отвечает за разбиение передаваемой информации на пакеты и правильное восстановление информации из пакетов получателя.

TDD (time division duplex) – дуплексный канал с временным разделением.

TDMA (Time Division Multiple Access, Множественный доступ с разделением времени) – множественный доступ, основанный на использовании тактового генератора, который делит время работы канала на повторяющиеся циклы.

Telnet – TCP/IP – протокол для доступа к удаленному компьютеру и обработки данных на нем. В рамках операционной системы или оболочки организуется доступ к его функциям в виде командного интерфейса.

Token Ring (эстафетная кольцевая сеть, сеть с передачей маркера, маркерное кольцо) – кольцевая сеть, в которой передача данных основана на том, что каждый узел кольца ожидает прибытия короткой уникальной последовательности битов (маркера) из смежного предыдущего узла.

TDR (Time Domain Reflectometry) – измерение коэффициента отражения путем совмещения прямого и отраженного сигналов или с помощью индикаторной диаграммы в кабеле.

UDP (User Datagram Protocol, протокол пользовательских дейтаграмм) – протокол транспортного уровня в стеке протоколов TCP/IP, являющийся упрощенным вариантом TCP. Протокол не обеспечивает проверку на наличие ошибок и не подтверждает доставку пакета.

URL (Uniform resource locator, унифицированный указатель ресурсов) – адрес веб-страницы в сети Internet с указанием протокола, с помощью которого можно обращаться к этой странице. В URL входят: имя домена, названия файла и каталога, сетевой адрес машины и метод (протокол) доступа к файлу.

USB (Universal Serial Bus, универсальная последовательная шина) – последовательная шина, предназначенная для (шлейфового) подключения к компьютеру периферийных устройств и поддерживающая «горячее» подключение, автоматическое распознавание и настройку оборудования.

UTP (Unshielded Twisted Pair, неэкранированная витая пара) – кабель типа «витая пара», не имеющая металлического экрана.

v.11 (ANSI/TIA/EIA–422–B (бывш. RS–422), X.27) – технический стандарт направленный на обеспечение сбалансированной или дифференциальной однонаправленной нереверсируемой передачи данных по терминированным или нетерминированным линиям, с возможностью соединения «точка к точке» или для многоабонентской доставки сообщений.

VLB (VESA local bus) – шина, предназначенная для соединения внешних устройств с компьютерами, разработанная ассоциацией VESA (Video Electronics Standards Association).

WDM (Wavelength division multiplexing, мультиплексирование с разделением по длине волн) – в оптоволоконных технологиях – способ мультиплексирования, при котором свет с волнами разной длины передается по одному световоду.

WiFi (Wireless Fidelity) – беспроводной сетевой стандарт на оборудование, разработанный консорциумом Wi–Fi Alliance на базе стандартов IEEE 802.11.

WiMax (Worldwide Interoperability for Microwave Access) – телекоммуникационная технология, разработанная с целью предоставления универсальной беспроводной связи на больших расстояниях, основанная на стандарте IEEE 802.16.

WLAN (Wireless Local Area Network, беспроводная локальная вычислительная сеть) – способ построения сетей, при котором передача данных осуществляется через радиоэфир. Объединение устройств в сеть происходит без использования кабельных соединений.

WWW (World Wide Web, служба глобального соединения) – основная служба в сети Internet , позволяющая получать доступ к информации на любых серверах, подключенных к сети.

x.25 – семейство протоколов канального уровня сетевой модели OSI. Предназначалось для организации WAN на основе телефонных сетей с линиями с достаточно высокой частотой ошибок, поэтому содержит развитые механизмы коррекции ошибок.

x.400 — протокол, представляет собой набор рекомендаций по построению системы передачи электронных сообщений, не зависящей от используемых на сервере и клиенте операционных систем и аппаратных средств.

ZIGBEE – беспроводная технология, основанная на стандарте IEEE 802.15, которая предназначена для использования в системах сбора данных и управления. Она обладает малым энергопотреблением, надежностью передачи данных и защиты информации.

Волновод (Waveguide) – канал в неоднородной среде, вдоль которого может распространяться направленное электромагнитное излучение. Отличают экранированные волноводы, образованные зеркально отражающими стенками.

Гетерогенная сеть (Heterogeneous network, неоднородная сеть) – информационная сеть, в которой работают протоколы сетевого уровня различных фирм-производителей. Гетерогенная сеть может состоять из фрагментов разной топологии и разнотипных технических средств.

Грид (grid, решетка, сеть) – согласованная, открытая и стандартизированная компьютерная среда, обеспечивающая гибкое, безопасное, скоординированное разделение вычислительных ресурсов и ресурсов хранения информации, являющихся частью этой среды, в рамках одной виртуальной организации.

Грид вычисления – это форма распределённых вычислений, в которой «высокопроизводительный виртуальный компьютер» представлен в виде кластера соединенных с помощью сети, слабосвязанных компьютеров, работающих вместе для выполнения огромного количества заданий (операций, работ).

Домен (Domain) – в модели OSI – административная часть распределенной системы или домен управления службой каталогов.

Интрасеть – внутрикорпоративная сеть с Web-узлом. Такие сети могут быть изолированы от Internet или защищаются от доступа внешних пользователей Internet с помощью брандмауэров.

Информационная сеть – сеть, предназначенная для обработки, хранения и передачи данных. Информационная сеть состоит: из абонентских и административных систем, а также связывающей их коммуникационной сети.

Кабель (Cable) – группа изолированных проводников, заключенных в герметическую оболочку.

Кабельная сеть (Wire network) – сеть, системы которой взаимодействуют через кабели. Кабельные сети обеспечивают защищенность от атмосферных помех и излучений солнца и высокую степень безопасности данных.

Канал передачи данных (Data Communication Channel, DCC, channel, канал связи, канал) – часть коммуникационной сети, состоящая из технических средств передачи и приема данных, включая линию связи, а также из средств программного обеспечения и протоколов.

Кластер – группа компьютеров, объединённых высокоскоростными каналами связи и представляющая с точки зрения пользователя единый аппаратный ресурс.

Коммуникационная сеть – сеть, основной задачей которой является передача данных без ошибок и искажения. Коммуникационная сеть является ядром информационной сети, обеспечивающим передачу и некоторые виды обработки данных.

Коммутатор (Switch) – концентратор, который может одновременно устанавливать соединения между несколькими парами портов и реализует виртуальные соединения между сетевыми сегментами.

Коммутируемая сеть Ethernet – стандартная технология Ethernet, в которой вместо мостов или концентраторов используются коммутаторы, позволяющие создавать виртуальные каналы между каждой парой узлов, предоставляя каждому пользователю всю полосу пропускания.

Концентратор – устройство или функциональный блок, у которого суммарная пропускная способность входных каналов выше пропускной способности выходного канала.

Манчестерский код – самосинхронизирующийся информационный код. Логическому нулю соответствует положительный переход в центре бита. Логической единице соответствует отрицательный переход в центре бита. Обязательное наличие перехода в центре бита позволяет легко выделить синхросигнал.

Маркер (Token) – пакет с уникальной структурой, непрерывно циркулирующий в локальной сети от узла к узлу и описывающий ее текущее состояние. Узел может осуществлять передачу только тогда, когда получает право на управление маркером.

Маршрутизатор (Router) – устройство, обеспечивающее трафик между локальными сетями, имеющими разные сетевые адреса. Маршрутизатор отвечает за выбор маршрута передачи пакетов между узлами.

Модем (Modem, модулятор/демодулятор) – внешнее или внутреннее устройство, подключаемое к компьютеру для передачи и приема сигналов по телекоммуникационным (телефонным) линиям.

Мост (Bridge) – ретрансляционная система, соединяющая каналы передачи данных. Мост выполняет соединение на канальном уровне модели OSI. Мосты не имеют механизмов управления потоками блоков данных.

Мультиплексирование – технология разделения средств передачи данных между группой использующих их объектов. В результате мультиплексирования в одном физическом канале создается группа логических каналов.

Повторитель (Repeater, репитер) – устройство, которое передает электрические сигналы от одного участка кабеля к другому, предварительно усиливая эти сигналы и восстанавливая их форму. Обычно повторитель используется в локальных сетях для увеличения длины сегмента.

Рабочая группа (Workgroup) – совокупность пользователей, имеющих общие данные, периферийные устройства и другие вычислительные ресурсы, а также права их использования.

Ретрансляция кадров (Frame relay) – высокоскоростная цифровая технология передачи кадров переменной длины, использующая коммутацию кадров и технологию «точка-точка», применяющую виртуальный канал для передачи кадров переменной длины на канальном уровне модели OSI.

Световод – волновод, предназначенный для направленной передачи света. Конструктивно световод представляет собой тонкую кварцевую нить, окруженную защитной оболочкой со значительно меньшим коэффициентом преломления, чем сердцевина.

Сервер – компьютер или программная система, предоставляющие удаленный доступ к своим службам или ресурсам с целью обмена информацией. Сервер работает по заданиям клиентов. После выполнения задания сервер посылает полученные результаты клиенту, инициировавшему задание.

СКС (Structured Cabling System, структурированная кабельная система) – кабельная система, поддерживающая всевозможные информационные системы (компьютерные, телефонные и телевизионные сети, системы пожарной и охранной сигнализации) и разделенная на несколько уровней в зависимости от функционального назначения и расположения ее компонентов.

Топология (Topology) – схема соединения компьютеров, кабельной системы и других сетевых компонентов. Наиболее распространенными видами сетевых топологий являются: линейная, кольцевая, древовидная, звездообразная, ячеистая и полносвязная.

Трансивер (от англ. TRANSmitter – передатчик + receiver – приемник) – устройство предназначенное для подключения компьютера к сети, преобразующее поток параллельных данных, пересылаемый по шине компьютера, в поток последовательных данных, пересылаемый по кабелю, соединяющему компьютеры.

xDSL – семейство технологий, позволяющих значительно расширить пропускную способность абонентской линии местной телефонной сети путём использования эффективных линейных кодов и адаптивных методов коррекции искажений линии на основе современных достижений микроэлектроники и методов цифровой обработки сигнала.

Экстрасеть (extranet) – область частной сети, в которой размещены доступные через Internet ресурсы.

4b5b – способ избыточного кодирования информации в цифровых сетях, когда каждые 4 бита преобразуются в группы по 5 битов данных перед передачей с дополнительной информацией, используемой для поддержания целостности данных.

8b6t – способ избыточного кодирования информации в цифровых сетях, когда каждые 8 бит входного потока кодируются шестью троичными цифрами (0, 1 или 2).

8b10b – способ избыточного кодирования информации в цифровых сетях, когда каждые 8 битов данных перед передачей преобразуются в 10 битов с дополнительной информацией, используемой для поддержания целостности данных.

Литература

1 Олифер, В. Г. Новые технологии и оборудование IP-сетей / В. Г. Олифер, Н. А. Олифер. – СПб. : БХВ-СПб., 2000. – 512 с.

2 Компьютерные сети. Сертификация Network+.: учебный курс – официальное пособие Microsoft для самостоятельной подготовки; пер. с англ. – М. : Русская редакция, 2002. – 704 с. : ил.

3 Палмер, М. Проектирование и внедрение компьютерных сетей: учебный курс / М. Палмер, Р. Б. Синклер. – 2-е изд., перераб. и доп. – СПб. : БХВ-Петербург, 2004. – 740 с.

4 Хелд, Г. Технологии передачи данных / Г. Хелд: пер. с англ. – 7-е изд. – СПб. : Питер, 2003. – 715 с. : ил.

5 Шиндер, Д. Л. Основы компьютерных сетей: монография / Д. Л. Шиндер; пер. с англ. А. Г. Сысонюка. – М. : Вильямс, 2002. – 651 с. : ил.

6 Таненбаум, Э. Компьютерные сети: монография / Э. Таненбаум; пер. с англ. А. Леонтьев. – 3 изд. – М. : ПИТЕР, 2002. – 846 с. : ил.

7 Семенов, Ю. А. Сети Интернет. Архитектура и протоколы: монография / Ю. А. Семенов. – М. : Радио и связь, 1998. – 423 с. : ил.

8 Олифер, В. Г. Сетевые операционные системы: учебник для вузов / В. Г. Олифер, Н. А. Олифер. – СПб. : Питер, 2001. – 538 с. : ил.

9 Закер, К. Компьютерные сети. Модернизация и поиск неисправностей: К. Закер; пер. с англ. – СПб. : БХВ-Петербург, 2004. – 1008 с. : ил.

10 One Alex Сеть для дома и офиса. Создание, настройка, диагностика и защита / Alex One. – М. : Лучшие книги, 2004. – 394 с. : ил.

11 Колесниченко, Д. Н. Сделай сам компьютерную сеть. Монтаж, настройка, обслуживание / Д. Н. Колесниченко. – СПб. : Наука и Техника, 2000. – 400 с. : ил.

12 Минаев, И. Я. Локальная сеть своими руками. 100 % самоучитель: учеб. пособие / И. Я. Минаев. – М. : ТЕХНОЛОДЖИ – 3000, 2004. – 368 с. : ил.

13 Семенов, А. Б. Структурированные кабельные системы / А. Б. Семенов, С. К. Стрижаков, И. Р. Сунчелей. – М. : Компьютер Пресс, 1999. – 471 с. : ил.

Для заметок

Для заметок

Учебное издание

ДЕМИДЕНКО Олег Михайлович
ВОРУЕВ Андрей Валерьевич
КУЧЕРОВ Александр Иванович
КУЛИНЧЕНКО Владимир Николаевич

Аппаратное и программное обеспечение сетей

Учебное пособие
для студентов высших учебных заведений
по специальности
«Автоматизированные системы обработки информации»

Редактор *В. И. Шкредова*
Корректор *В. В. Калугина*

Лицензия № 02330/0133208 от 08.04.09.
Подписано в печать 26.05.09. Формат 60x84 1/16.
Бумага писчая №1. Гарнитура «Таймс». Усл. печ. л. 13,5.
Уч.-изд. л. 14,74. Тираж 100 экз. Заказ № 191

3863-00

Отпечатано с оригинала-макета на ризографе
учреждения образования
«Гомельский государственный университет
имени Франциска Скорины»
Лицензия № 02330/0150450 от 03.02.09.
246019, г. Гомель, ул. Советская, 104